GCF ANNUAL MEETING 2024

ADVANCING COLLECTIVE
ACTION IN CYBERSPACE

GLOBAL
CYBERSECURITY
FORUM

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

THE GCF RULE

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

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

TABLE OF CONTENTS

01

INTRODUCTION

INTRODUCTION

Cyberspace is closely linked to the growth of economies, the prosperity of societies, the security of individuals, and the stability of nations.
HIS ROYAL HIGHNESS PRINCE MOHAMMED BIN SALMAN BIN ABDULAZIZ AL-SAUD
CROWN PRINCE, PRIME MINISTER OF KINGDOM OF SAUDI ARABIA
Annual Meeting 2024

GCF is a global, non-profit organization, which aims to strengthen the safety and resilience of Cyberspace by advancing dialogue, pushing knowledge boundaries, driving social impact and investment, and building a unified global Cyberspace community.

This book provides an overview of GCF's activities, with a focus on the GCF Annual Meeting 2024 and the Child Protection in Cyberspace (CPC) Global Summit. As a major two-day event held in Riyadh, Saudi Arabia, the Annual Meeting brings together the international community to advance cross-border collaboration and shape the global Cyberspace agenda.

His Royal Highness Prince Mohammed bin Salman bin Abdulaziz Al-Saud, Crown Prince and Prime Minister of Saudi Arabia, welcomed participants to this year's Annual Meeting and CPC Global Summit in a statement saying that "Cyberspace is closely linked to the growth of economies, the prosperity of societies, the security of individuals, and the stability of nations. The cross-border nature of Cyberspace means that it is increasingly important to harmonize international efforts to seize the opportunities it offers, and face the challenges it presents, by investing in people."

From highlighting the action-oriented discussions that took place during the Annual Meeting, to charting GCF's efforts to complement the global conversation on cybersecurity before, during, and beyond the event, this book offers insights into how global decision makers, business leaders, and experts engaged with the 2024 theme of 'Advancing Collective Action in Cyberspace' across multiple platforms. This book also highlights the wider program of activities being delivered under the GCF umbrella, which provide sustained opportunities for collaboration on cybersecurity, beyond the Annual Meeting. This includes two global initiatives instated by His Royal Highness Prince Mohammed bin Salman – Child Protection in Cyberspace (CPC) and Women Empowerment in Cybersecurity (WEC) – both of which aim to drive tangible action on two of the most significant issues in Cyberspace today.

In conjunction with the Annual Meeting, GCF hosted its first ever Child Protection in Cyberspace (CPC) Global Summit, in collaboration with the International Telecommunication Union (ITU), United Nations Children's Fund (UNICEF), DQ Institute, and WeProtect Global Alliance. The strategic objectives of the summit were to consolidate global efforts and advance collective action, enhance the global response to pressing challenges, mitigate emerging threats facing children in Cyberspace, and ensure that child protection in Cyberspace resonates with the agenda of global decision-makers.

As set out in this book, the GCF Annual Meeting 2024, CPC Global Summit and GCF's achievements across all of its activities over the two-day event are a demonstration of the significant progress the GCF community is making in its journey – guided by a strong vision to strengthen the safety, resilience, and inclusivity of Cyberspace for the benefit of people around the world.

02

GCF ANNUAL MEETING 2024: ADVANCING COLLECTIVE ACTION IN CYBERSPACE

WELCOME STATEMENT

HRH THE CROWN PRINCE WELCOMES ATTENDEES TO THE GCF ANNUAL MEETING 2024, HELD IN RIYADH

October 2nd, 2024, SPA

The fourth edition of the Global Cybersecurity Forum (GCF) Annual Meeting kicked off today in the capital, Riyadh, under the patronage of the Custodian of the Two Holy Mosques, King Salman bin Abdulaziz Al-Saud.

The event brings together high-level international figures, including former prime ministers, government ministers, decision-makers, policymakers, thought leaders, and CEOs, from more than 125 countries, to advance multistakeholder collaboration and action on Cyberspace issues. The GCF Annual Meeting 2024 will also run in conjunction with the Child Protection in Cyberspace (CPC) Global Summit.

His Royal Highness Prince Mohammed bin Salman bin Abdulaziz Al-Saud, Crown Prince and Prime Minister – may God protect him – welcomed attendees on behalf of the Custodian of the Two Holy Mosques – may God protect him, saying: "The Kingdom of Saudi Arabia has always been a force for good for the benefit of humanity and human prosperity around the world. It has continuously worked to uphold the principle of cooperation, and strengthen international collaboration towards efforts that support development and prosperity for all nations. It has initiated several initiatives aimed at achieving these genuine goals in all sectors."

His Royal Highness added: "Cyberspace is closely linked to the growth of economies, the prosperity of societies, the security of individuals, and the stability of nations. The cross-border nature of Cyberspace means that it is increasingly important to harmonize international efforts to seize the opportunities it offers, and face the challenges it presents, by investing in people."

His Royal Highness continued: "Believing in the importance of investing in people in this vital and promising domain, in 2020 we launched two global initiatives. The first relates to protecting children in Cyberspace, and the second focuses on empowering women in the field of cybersecurity. The institute for the Global Cybersecurity Forum is entrusted with overseeing both initiatives, as well as implementing the associated projects."

His Royal Highness the Crown Prince highlighted the progress made by the two initiatives, most importantly the increased understanding of needs at the global level that has established new and inspiring visions that have enabled GCF to develop impactful initiatives and programs, publish research and studies, and formulate new frameworks and strategies. These efforts enable decision-makers around the world to develop policies and programs aimed at enhancing child protection in Cyberspace and enabling women's participation in the field of cybersecurity.

Based on these achievements, His Royal Highness the Crown Prince, also announced the launch of the Child Protection in Cyberspace Global Summit, hosted by the Kingdom as the first global summit of its kind, with the goals of unifying international efforts and enhancing the global response to the threats facing children in Cyberspace.

His Highness called on God Almighty to grant success to all participants in the Annual Meeting and the Summit, and for the efforts towards shaping a safe and reliable Cyberspace that enables growth and prosperity for all peoples of the world.

This year's edition of the Global Cybersecurity Forum Annual Meeting is held under the theme 'Advancing Collective Action in Cyberspace.' It will feature panel discussions in which decision-makers, senior officials, and international experts from various government agencies, academia, and leading global companies, will engage with five main themes: Beyond Cyber Discord, Cyber Psychology, Cyber Social Fabric, Thriving Cyber Economy, and New Cyber Frontier.

OPENING ADDRESS

HIS ROYAL HIGHNESS PRINCE MOHAMMED BIN ABDULRAHMAN BIN ABDULAZIZ, DEPUTY GOVERNOR OF RIYADH REGION

Distinguished participants and honored guests,

It is with great pleasure and gratitude that we welcome you to the fourth edition of the Global Cybersecurity Forum Annual Meeting, held under the esteemed patronage of the Custodian of the Two Holy Mosques, King Salman bin Abdulaziz Al-Saud.

We gratefully receive the welcome statement delivered by His Royal Highness Prince Mohammed bin Salman bin Abdulaziz, Crown Prince and Prime Minister. His Royal Highness extended a warm welcome to all participants and announced the launch of the Child Protection in Cyberspace Global Summit. This landmark summit, the first of its kind, aims to consolidate international efforts and enhance the global response to threats facing children in Cyberspace. His words underscore Saudi Arabia's steadfast dedication to promoting global prosperity and the well-being of humanity.

Esteemed guests,

The need for enhanced international collaboration to ensure a safe and resilient Cyberspace is greater than ever.

A secure Cyberspace is vital to fostering growth and prosperity for all nations. With the expertise gathered at this forum, we are confident that the outcomes will meet global aspirations for this vital and promising sector.

Honored guests,

I thank you for your presence and pray for success in the forum's insightful dialogues and the summit's proceedings.

Governor of the National Cybersecurity Authority, Saudi Arabia
Acting on behalf of the Board of Trustees, Global Cybersecurity Forum

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, Ladies and Gentlemen, I am pleased to welcome you to the Global Cybersecurity Forum Annual Meeting 2024.

Many of you have been part of the GCF journey from its inception in 2020. Since then, the GCF community has grown stronger and more diverse, transforming discussion into shared priorities among stakeholders from over 120 countries.

As stated this morning by His Royal Highness Prince Mohammed bin Salman bin Abdulaziz, Crown Prince and Prime Minister, welcoming all the participants to this 4th edition of GCF: "Cyberspace is closely linked to the growth of economies, the prosperity of societies, the security of individuals and the stability of nations."

Last year, a significant milestone was reached when GCF was officially established by royal decree as a global non-profit institute, committed to advancing dialogue, pushing knowledge boundaries, driving social impact and investment, and building a unified global Cyberspace community.

These objectives provide a clear path toward GCF's vision for a safer, more inclusive and resilient Cyberspace, and form the basis of our activities. From impact-driven global initiatives to thought leadership platforms, including Knowledge Communities led by Aramco, NEOM, SITE, and stc - established only one year ago, these working groups are convening more than 80 international members, whom we thank for their meaningful and impactful collaboration.

GCF's activities and partnerships embody the theme of this year's Annual Meeting – "Advancing Collective Action in Cyberspace" – building on the roadmap established in previous editions and setting the direction for the year ahead.

Over the next two days, a range of new projects will be launched under GCF's umbrella, addressing some of the key issues and opportunities in Cyberspace, from cyber economics, to closing the cybersecurity workforce and skills gap, and ensuring that Cyberspace is safe and secure for children.

Indeed, in conjunction with the Annual Meeting, the Child Protection in Cyberspace Global Summit will bring together global stakeholders to identify pathways for collective action toward safeguarding children in Cyberspace. The summit is held in collaboration with our esteemed partners, ITU, UNICEF, DQ Institute, and WeProtect Global Alliance.

As we take this next step in our journey together, we look forward to forging new partnerships, and to sharing the benefits arising from these vital discussions.

Thank you.

GCF ANNUAL MEETING 2024

Advancing Collective Action in Cyberspace

2nd-3rd October, 2024 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.

The theme for the GCF Annual Meeting 2024, which took place on 2nd-3rd October in Riyadh, was 'Advancing Collective Action in Cyberspace.' This built on the previous year's theme, 'Charting Shared Priorities in Cyberspace', which sought to spearhead strategic planning around the results of GCF 2022, 'Rethinking the Global Cyber Order'. The GCF Annual Meeting 2024 aimed to move the international cyber community to take multistakeholder actions to ensure Cyberspace is safe, secure and an enabler of prosperity for people around the world.

GCF ANNUAL MEETING 2024 – KEY FIGURES

Global Participation

126
Countries represented

51
Open Forum speakers

42
Participatory Track speakers

Action-Oriented Program

18
Open Forum sessions

13
Deep Dive sessions

3
High-level Roundtables

Cyber CxO meeting

3
Knowledge Community meetings

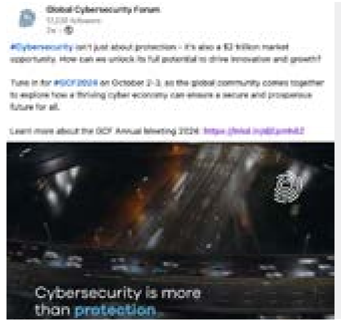
Center of Excellence meeting

Sustained Conversation

542M
Total media reach

67
Tier 1 international media interviews from the GCF Live Studio

GLOBAL BUSINESS TODAY
INCLUSIVE CYBER POLICIES: THE ROLE OF WOMEN IN DECISION-MAKING



Global Cybersecurity Forum

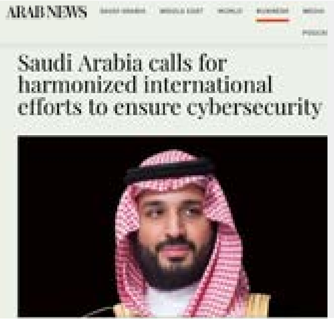
#Cybersecurity isn't just about protection – it's also a $2 trillion market opportunity. How can we unlock its full potential to drive innovation and growth?

Tune in for #GCF2024 on October 2-3, as the global community comes together to explore how a thriving cyber economy can ensure a secure and prosperous future for all.

Learn more about the GCF Annual Meeting 2024: [illegible]

Cybersecurity is more than protection

75.6M
Impressions across X and LinkedIn



ARAB NEWS

Saudi Arabia calls for harmonized international efforts to ensure cybersecurity

533
Mentions in international and regional press

PARTNERS

GCF FOUNDING PARTNERS

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Site

GCF STRATEGIC PARTNERS

aramco

NEOM نيوم

stc

GCF ANNUAL MEETING PARTNERS

Microsoft

FURTINET

CISCO

paloalto NETWORKS

GCF ANNUAL MEETING MEDIA PARTNERS

العربية alarabiya

ARAB NEWS

Bloomberg Media

CGTN

GCF KNOWLEDGE CONTRIBUTORS

Site
NEOM نيوم
stc
aramco
BCG BOSTON CONSULTING GROUP
UL
DRAGOS
KACST

IDQ
TREND MICRO
CYBER RANGES
IBM
CYBERCRYPT.
Schneider Electric
CISCO

pwc
CYBERNETICA
Chainalysis
NTIS
AXON
Cyberani by aramco digital

Deloitte.
EMERSON
KPMG
EY
FURTINET
Honeywell
جامعة الملك عبدالله للعلوم والتقنية

جامعة الملك فهد للبترول والمعادن
King Fahd University of Petroleum & Minerals
جامعة الملك سعود
King Saud University
UNSW AUSTRALIA
INSEAD
SmartCitiesWorld
European Smart Cities Association
Smart City Cluster

SWISS CYBER INSTITUTE
Cellusys
orange
AUJAS CYBERSECURITY
MOTIVA
Syracuse University
libelium

ENEA
mobileum
NETWITNESS
accenture
HUAWEI
Petroleum Development Oman
PETRONAS

Schneider Electric
Shell
SIEMENS energy
splunk>
YOKOGAWA
academy from stc
THALES
Google

ERICSSON
ORACLE
paloalto NETWORKS
NOKIA
sirar by stc
SLAC NATIONAL ACCELERATOR LABORATORY
CROWDSTRIKE

(one)
Privafy
SANS
Trellix
IMMERSIVELABS
CNTXT

GCF ANNUAL MEETING 2024

Advancing Collective Action in Cyberspace

The 2024 Annual Meeting advanced collective action across five key sub-themes, focusing on the geostrategic, economic, social, behavioral, and technical dimensions of Cyberspace.

Beyond Cyber Discord

Building trust within geopolitical competition, enabling constructive dialogue and effective collaboration on critical issues in Cyberspace.

Cyber Psychology

Leveraging psychological insights to decrypt behaviors of attackers, defenders, and users in Cyberspace.

Cyber Social Fabric

Protecting our most vulnerable communities and ensuring safety and security for all users in Cyberspace.

Thriving Cyber Economy

Unleashing the potential of the cybersecurity sector, developing stronger markets, and building resilient cyber ecosystems.

New Cyber Frontier

Maximizing the benefits from emerging technologies and mitigating potential cybersecurity risks.

PROGRAM FORMAT

As part of GCF's comprehensive program of activities, the GCF Annual Meeting gathers global stakeholders with a shared commitment to addressing the challenges and opportunities of Cyberspace, and ensuring it becomes safer and more resilient for the benefit of people around the world. It is designed to deepen multi-stakeholder engagement and to drive collective action across key strategic priorities.

To accomplish this goal, the Annual Meeting program consists of two main tracks:

OPEN FORUM

Open to all Annual Meeting participants, the Open Forum facilitates dialogue and knowledge-sharing in an accessible manner, providing new perspectives and multidisciplinary lenses across key cybersecurity issues.

Plenary Session

Panel Discussions

Fireside Chats

PARTICIPATORY TRACK

Held in a range of formats, the extensive 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

Fireside Chats

Invite-only Briefs

Solution Design Sessions

Initiative Working Sessions

Invite-only Breakfast

GCF ANNUAL MEETING PROGRAM

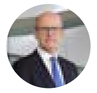
OPEN FORUM - OCTOBER 2ND, 2024 (DAY 1 - MORNING)

9:30 - 09:50 **Opening Ceremony**

9:50 **Pathways To De-Escalation:** Shared priorities for reducing tensions and advancing stability in Cyberspace | ROOM G | 45 MIN

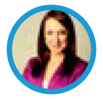
John Defterios (Moderator)
Former CNN, Emerging
Markets Editor & Anchor

Dr. Mark Esper
27th Secretary of Defense
United States


Sir Jeremy Fleming
Former Director of
GCHQ, United Kingdom

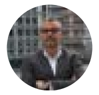
H.E. José Manuel Barroso
President of the EU
Commission (2004-2014)

10:35 **Pioneering Pathways:** Unleashing potential in the Cybersecurity sector | ROOM G | 35 MIN


Rebecca McLaughlin-Eastham (Moderator)
Independent TV Anchor
& Media Trainer

Dr.Saad Alaboodi
CEO
Saudi Information Technology
Company (SITE)

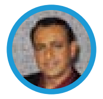
Timothy Sherman
Vice President/CTO,
Global Security Sales
Engineering, Cisco


Miguel Ángel Cañada
Head of National Coordination
Centre (NCC-ES)
Spanish National Cybersecurity
Institute (INCIBE)

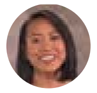
Suk-Kyoon Kang
CEO
AhnLab

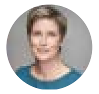
Dr. Megat Zuhairy
Chief Executive
National Cyber Security
Agency (NACSA), Malaysia

11:10 **Leadership Launchpad:** Charting paths to cyber leadership | ROOM G | 35 MIN


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

H.E. Dr. Hala Al-Tuwaijri
President, Human Rights
Commission, Saudi Arabia


Joy Chik
President, Identity and
Network Access, Microsoft


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

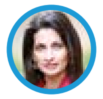
11:40-11:50 **Coffee Break**

11:50 **Cyber Statecraft:** The new chessboard of geopolitics | ROOM G | 20 MIN

Rima Maktabi (Moderator)
London Bureau Chief
Al Arabiya

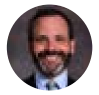
Chris Inglis
Former National Cyber
Director, U.S. Government

12:10 **The Multilateral Frontier:** Assessing the state of play and imperatives for collective action in cyber diplomacy | ROOM G | 30 MIN


Nisha Pillai (Moderator)
International Moderator
and Journalist

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

H.E. Massimo Marotti
Managing Director for
Strategies and Cooperation
National Cybersecurity
Agency (ACN), Italy


Adam Hantman
Deputy Director, Bureau of
Cyberspace and Digital Policy,
U.S. Department of State

Sub-Themes Beyond Cyber Discord | Cyber Psychology | Cyber Social Fabric | Thriving Cyber Economy | New Cyber Frontier

OPEN FORUM - OCTOBER 2ND, 2024 (DAY 1 - AFTERNOON)

14:00 **Ctrl + Invest:** Women shaping the future of cyber innovation | ROOM G | 30 MIN

Lara Habib (Moderator)
Senior Business News
Presenter, Al Arabiya

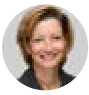
Christopher Steed
CIO and Managing Director,
Paladin Capital Group

David A. Hoffman
Steed Family Professor
of Cybersecurity Policy,
Duke University Sanford
School of Public Policy

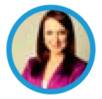
Dr. Mary Aiken
Chair & Professor of the
Cyberpsychology
Department, Capitol
Technology University

14:30 **Economic Security and Critical Infrastructure:** The imperative of building trust in an era of geopolitical competition | ROOM G | 20 MIN

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

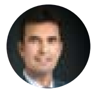

Heidi Crebo-Rediker
Senior Fellow Council on
Foreign Relations

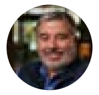
14:50 **Beyond the Firewall:** Building a cyber resilient supply chain in a hyperconnected world | ROOM G | 30 MIN


Rebecca McLaughlin-Eastham (Moderator)
Independent TV Anchor
& Media Trainer

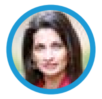
Paul Selby
CISO, U.S. Department of
Energy

Akshay Joshi
Head of Industry and
Partnerships, Centre for
Cybersecurity, World
Economic Forum (WEF)


Christophe Blassiau
SVP, Cybersecurity &
Product Security, Global
CISO & CPSO Schneider
Electric


Michael Ruiz
VP and General Manager for
Cyber Products, Honeywell

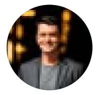
15:20 **Balancing Progress and Peril:** Understanding the challenges and opportunities of AI in Cybersecurity | ROOM G | 35 MIN

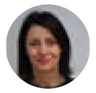

Nisha Pillai (Moderator)
International Moderator
and Journalist

Brigadier-General Edward Chen
Defence Cyber Chief
Ministry of Defense, Singapore

Ken Naumann
Chief Executive Officer
NetWitness

Dr. Helmut Reisinger
CEO for EMEA and
LATAM, Palo Alto
Networks, inc.


Adam Russell
VP of Cloud & Enterprise
Security, Oracle


Dr. Sadie Creese
Professor of Cybersecurity,
Oxford University; Director, Global
Cyber Security Capacity Centre

Sub-Themes Beyond Cyber Discord | Cyber Psychology | Cyber Social Fabric | Thriving Cyber Economy | New Cyber Frontier

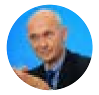
OPEN FORUM - OCTOBER 3RD, 2024 (DAY 2 - MORNING)

9:30

The History of Cyber Diplomacy Future: Drawing insights from collaborative progress on trade, nuclear and climate

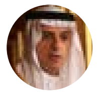
ROOM G 30 MIN

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



Pascal Lamy
Vice President, Paris Peace Forum & Former Director, General World Trade Organization

H.E. Ambassador Shyam Saran
Former Minister of Foreign Affairs, India

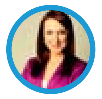


H.E. Adel Al-Jubeir
Saudi Arabia's Minister of State for Foreign Affairs, Member of the Council of Ministers & Envoy for Climate Affairs

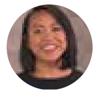
10:00

Principles of Stability: Applying the lessons of the past to the current and future challenges in Cyberspace

ROOM G 20 MIN



Rebecca McLaughlin-Eastham (Moderator)
Independent TV Anchor & Media Trainer



Joy Chik
President Identity and Network Access, Microsoft

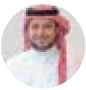
10:20

Shielding Connectivity: Safeguarding future networks

ROOM G 30 MIN

Yang Chengxi (Moderator)
International Journalist and TV host, Al Arabiya English

Bocar Alpha Ba
CEO & Board Member SAMENA Telecommunications Council



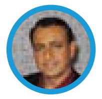
Yasser Alswailem
Group VP, Cybersecurity STC Group

Mohamed Ben Amor
Director General Arab ICT Organization

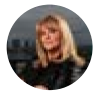
10:50

Cognitive Resilience: Building psychological defense against cyberattacks

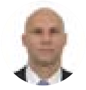
ROOM G 30 MIN



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



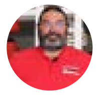
Dr. Mary Aiken
Chair & Professor of the Cyberpsychology Department Capitol Technology University



Dr. Neal Jetton
Director, Cybercrime INTERPOL

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

Major General (Rtd) Eng. Mohammad Boarki
Chief, National Cyber Security Center, Kuwait



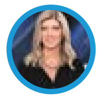
Filippo Cassini
Global Technical Officer, and Senior VP of Engineering Fortinet

11:20-11:30 **Coffee Break**

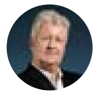
11:30

The Pulse of Security: Securing the healthcare sector amidst technological disruptions

ROOM G 30 MIN



Lara Habib (Moderator)
Senior Business News Presenter, Al Arabiya



Dr. Richard Staynings
Chief Security Strategist, Cylera & Teaching Professor, University of Denver

Prof. Junaid Nabi
Professor in Healthcare Strategy, Harvard University

Mike Fell OBE
Director, National Cyber Operations, NHS England

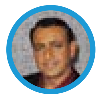
Sub-Themes Beyond Cyber Discord | Cyber Psychology | Cyber Social Fabric | Thriving Cyber Economy | New Cyber Frontier

OPEN FORUM - OCTOBER 3RD, 2024 (DAY 2 - AFTERNOON)

14:00

Navigating the Future: Advancing international cooperation to build confidence in Cyberspace

ROOM G 15 MIN



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

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

14:15

Crime Inc.: The institutionalization of organized cybercrime

ROOM G 15 MIN

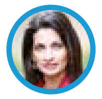
John Defterios (Moderator)
Former CNN, Emerging Markets Editor & Anchor

Josh Goldfoot
Deputy Assistant Attorney General Criminal Division, U.S. Department of Justice

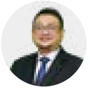
14:30

From Shortage to Strength: Closing the cybersecurity skills gap for a resilient Cyberspace

ROOM G 30 MIN



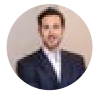
Nisha Pillai (Moderator)
International Moderator and Journalist



Dr. Haji Amirudin Abdul Wahab
Chief Executive Officer CyberSecurity Malaysia

Shaikh Salman bin Mohammed Al Khalifa
CEO, National Cyber Security Center (NCSC), Kingdom of Bahrain

Dan Cîmpean
Director, National Cybersecurity Directorate, Romania

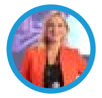


Dr. Bernd Pichlmayer
CEO and Founder, FTGG Cyber

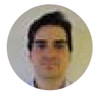
15:00

Securing the Spotlight: Cybersecurity roadmap for mega events

ROOM G 30 MIN



Laura Buckwell (Moderator)
International Moderator



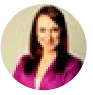
João Marcelo Azevedo Marques Mello da Silva
Advisor National Telecommunications Agency, Brazil

Dr. Hazim S. Almuhimedi
Risk & Compliance Deputy Governor, National Cybersecurity Authority (NCA), Saudi Arabia

Ahmed Mohammed Al Hammadi
Director, National Cyber Fusion, Qatar

15:30-16:00 **Closing Plenary**

John Defterios
Former CNN, Emerging Markets Editor & Anchor



Rebecca McLaughlin-Eastham
Independent TV Anchor & Media Trainer

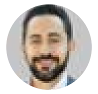
Sub-Themes Beyond Cyber Discord | Cyber Psychology | Cyber Social Fabric | Thriving Cyber Economy | New Cyber Frontier

PARTICIPATORY TRACK (1/3) - OCTOBER 2ND, 2024 (DAY 1 - MORNING)

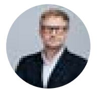
10:30 **"Securing Industrial Systems for Global Energy Supply" Knowledge Community Meeting** ROOM F 1 HOUR

11:00 **Perspective Reversal:** Cognitive strategies and orientations of attackers ROOM C2 30 MIN

Yang Chengxi (Moderator)
CGTN


Harold Rivas
CISO and Member of the Executive Leadership
Trellix

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

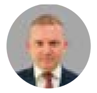

Oliver Väärtnõu
CEO
Cybernetica

Kevin Brown
Chief Operating Officer, NCC Group

11:40 **Equipping the Defenders:** What law enforcement needs to win ROOM C2 20 MIN

Rudolph Lohmeyer (Moderator)
Partner, Kearney

Pablo Muñoz de Mora
Principal Commissar, General Secretary of Operations and Digital Transformation Division Directorate General of Spanish National Police, Spain


Mustafa Ünal Erten
Chief,
UNODC Cybercrime Centre

Dr. Neal Jetton
Director, Cybercrime
INTERPOL

11:40 **Safeguarding the Cyber Heartbeat:** Insight on leveraging AI for patient data protection ROOM C1 20 MIN

Shoaib Yousuf (Moderator)
Managing Director & Partner, BCG

Prof. Junaid Nabi
Senior Fellow, The Aspen Institute

12:00 **Cyber CxO Meeting** ROOM F 1 HOUR

12:30 **Global View Series:** Korea's cybersecurity journey ROOM C1 30 MIN

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

PARTICIPATORY TRACK (1/3) - OCTOBER 2ND, 2024 (DAY 1 - AFTERNOON) - 01

13:00 **Roundtable on Active Defense** ROOM C3 1 HOUR

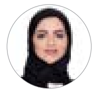
14:00 **High-Level Roundtable on Collective Action in Cyberspace** ROOM F 1 HOUR

14:00 **Cyber (S)heroes:** Breaking stereotypes, building careers ROOM C2 30 MIN

Alexandra Topalian (Moderator)
International Moderator

Almerindo Graziano
CEO, CYBER RANGES

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

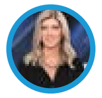

H.E. Dr. Ohoud Shehail
Director General, Department of Digital Ajman, UAE

Orhan Osmani
Head of the Cybersecurity Division, International Telecommunication Union (ITU)

14:30 **Beyond Code:** The institutional machinery of cyber diplomacy ROOM C1 20 MIN

Katherine Prizeman
Political Affairs Officer
United Nations Office for Disarmament Affairs (UNODA)

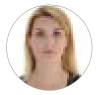
14:40 **Towards a Resilient Cyber Future:** Insight on global cyber workforce gaps and skills shortage ROOM C2 30 MIN


Lara Habib (Moderator)
Senior Business News Presenter, Al Arabiya

Eng. Abdurahman Al Hassan
Acting CEO, Global Cybersecurity Forum (GCF)

William H. Dutton
Martin Fellow, Oxford University's Global Cyber Security Capacity Centre

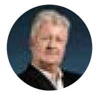
Shoaib Yousuf
Managing Director & Partner, BCG


Natasa Perucica
Lead for Capacity Building, World Economic Forum's Centre for Cybersecurity

PARTICIPATORY TRACK (1/3) - OCTOBER 2ND, 2024 (DAY 1 - AFTERNOON) - 02

15:00 **Curing the Gap:** Promoting Cybersecurity solutions for vulnerable health systems ROOM C1 20 MIN

Alexandra Topalian (Moderator)
International Moderator



Dr. Richard Staynings
Chief Security Strategist, Cylera & Teaching Professor, University of Denver

15:30 **OTC Center of Excellence** ROOM F 1 HOUR

15:30 **Code, Clicks, and Culture:** Social transformation in the technological age ROOM C1 20 MIN

Sauvik Tegta (Moderator)
Partner, Kearney

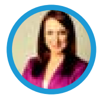
Wael Fattouh
Chief Advisory Officer, SITE

Erik Bertman
CEO, Conscia

Daren Smith
International Government Managing Director, BAE Systems Digital Intelligence

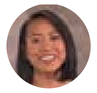
PARTICIPATORY TRACK (3/3) - OCTOBER 3RD, 2024 (DAY 2)

9:00 **Breakfast:** Launch of 'Women Leadership in Cyber' global mentoring program ROOM C2 20 MIN

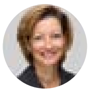


Rebecca McLaugh-lin-Eastham (Moderator)
Independent TV Anchor & Media Trainer

Doreen Bogdan-Martin
Secretary-General International Telecommunication Union



Joy Chik
President Identity and Network Access Microsoft



Heidi Crebo-Rediker
Senior Fellow
Council on Foreign Relations

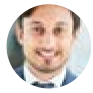
Silvana Koch-Mehrin
Founder and President
Women Political Leaders (WPL)

10:00 **"Future of Cybersecurity" Knowledge Community Meeting** ROOM F 1 HOUR

10:30 **Fortifying the Field:** Securing operational technology of oil industry in a hyperconnected world ROOM C2 20 MIN

Lara Habib (Moderator)
Senior Business News Presenter, Al Arabiya

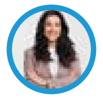
Phil Tonkin
CTO
Dragos



Filipe Beato
Lead, Centre for Cybersecurity, World Economic Forum (WEF)

Salem S. Al-Elwi
Manager of OT Cybersecurity, Saudi Aramco

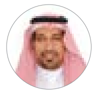
11:30 **Hacking Trust:** Cybercrime's role in transforming social norms ROOM C2 20 MIN



Alexandra Topalian (Moderator)
International Moderator

Anand Kashyap
CEO & Co-Founder
Fortanix

Dr. Moataz Bin Ali
Regional Vice President and Managing Director, MMEA, Trend Micro



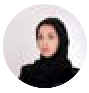
Dr. Abdulaziz Almaslukh
Senior RDI Executive
SITE

14:00 **High-Level Multi-Stakeholder Roundtable** ROOM F 1 HOUR

14:30 **Reducing Cyber Carbon Footprint:** Making Cybersecurity sustainable ROOM C2 20 MIN

Jay Bhatnagar (Moderator)
Principal, BCG

Dr. Antonio J. Jara
CSO
Libelium



Dr Manar Alohaly
Senior RDI Executive
SITE

15:30 **"Safeguarding the Future Networks & Emerging Technologies" Knowledge Community Meeting** ROOM F 1 HOUR

ANNUAL MEETING PROCEEDINGS: OPEN FORUM

OPEN FORUM

PATHWAYS TO DE-ESCALATION

Shared Priorities for Reducing Tensions and Advancing Stability in Cyberspace

- **Dr. Mark Esper**, 27th Secretary of Defense, United States
- **Sir Jeremy Fleming**, former Director of GCHQ, United Kingdom
- **José Manuel Barroso**, former President of the European Commission (2004-2014) and former Prime Minister of Portugal (2002-2004)
- **John Defterios (Moderator)**, former Emerging Markets Editor and anchor, CNN

The first open forum session of the GCF Annual Meeting 2024, 'Pathways to De-escalation: Shared Priorities for Reducing Tensions and Advancing Stability in Cyberspace', set the stage for substantive dialogue on the global cybersecurity landscape. Chaired by John Defterios, the session brought a distinguished panel together to address the multifaceted challenge of de-escalating tensions in Cyberspace amidst an increasingly fragmented geopolitical landscape.

The discussion underscored the accelerating impact of cybercrime, which is projected to cost the global economy $10.5 trillion by 2025. With the rapid advancement of technologies like AI and quantum computing, panelists explored how these innovations could both exacerbate vulnerabilities and offer new pathways for cyber defense.

72% of leaders reported that geopolitics has influenced organizations' cybersecurity strategies

(World Economic Forum)

A central theme of the session was the critical need for international cooperation, intelligence sharing, and cohesive enforcement to mitigate cyber risks. The conversation underscored the widening gap between nations acting responsibly in Cyberspace and those failing to do so, emphasizing the importance of establishing consequences for irresponsible behavior.

Panelists also emphasized the role of public-private partnerships in setting new cybersecurity norms, while stressing the urgent need for collaborative efforts to address increasing complex challenges in Cyberspace. The discussion recognized the importance of fostering global resilience, preparedness, and accountability to maintain a stable, secure Cyberspace. In conclusion, the session reinforced the need for collective action to tackle both immediate and long-term cybersecurity challenges.

To watch the full session, scan the QR code:

SCAN HERE

Panel Discussion | **Thriving Cyber Economy**

OPEN FORUM

PIONEERING PATHWAYS

Unleashing Potential in the Cybersecurity Sector

- **Dr. Saad Alaboodi**, CEO, Saudi Information Technology Company (SITE)
- **Timothy Sherman**, Vice President/CTO, Global Security Sales Engineering, Cisco
- **Miguel Ángel Cañada**, Head of National Coordination Centre (NCC-ES), Spanish National Cybersecurity Institute (INCIBE)
- **Suk-Kyoon Kang**, CEO, AhnLab
- **Dr. Megat Zuhairy**, Chief Executive, National Cyber Security Agency (NACSA), Malaysia
- **Rebecca McLaughlin-Eastham (Moderator)**, Independent TV anchor & media trainer

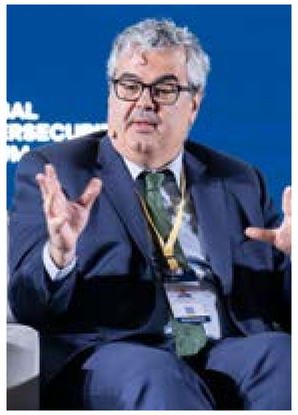
In his opening remarks, Dr. Saad Alaboodi, CEO of SITE, laid the groundwork for an in-depth discussion on the critical role of cybersecurity in ensuring economic stability and minimizing tensions in Cyberspace. He highlighted the interconnected nature of modern society, in which data, energy, and supply chains are interdependent – making cybersecurity a pressing global concern. Vulnerabilities in one sector can have widespread ramifications, underscoring the necessity of a cohesive cybersecurity strategy.

Dr. Alaboodi highlighted the staggering economic implications of cyber threats, noting that the global cost of cybercrime is projected to reach $9.5 trillion by year-end. He also stressed the importance of technological sovereignty, advocating for the localization of technology to ensure control over data and operations remains within national borders. This approach, he noted, would create opportunities for technology firms to innovate and strengthen their offerings, while reinforcing the cybersecurity landscape.

$9.5T The global cybercrime economy – a $9.5 trillion behemoth – represents the world's third-largest economy by GDP

(Source: Bloomberg)

Panelists in the 'Pioneering Pathways: Unleashing Potential in the Cybersecurity Sector' session expanded upon Dr. Alaboodi's insights, emphasizing that cybersecurity vulnerabilities extend beyond individual organizations and pose significant risks that can disrupt entire sectors and economies. With industries increasingly reliant on interconnected infrastructures, it is crucial to recognize that the impact of cyber threats is systemic, requiring a unified and proactive approach to cybersecurity.



Rebecca McLaughlin-Eastham
Independent TV Anchor
& Media Trainer
Timothy Sherman
Vice President/CTO,
Global Security Sales Engineering,
Cisco
Miguel Ángel Cañada
Head of National Coordination Centre (NCC-ES)
Spanish National Cybersecurity Institute (INCIBE)
Suk-Kyoon Kang
CEO
AhnLab

As critical systems in energy and manufacturing become more intertwined, the existing lag in Operational Technology (OT) cybersecurity presents a considerable risk, and the discussion highlighted the urgent need to bridge the gap between OT and Information Technology (IT) cybersecurity measures. The panelists asserted that it is imperative to invest in integrated cybersecurity solutions that encompass both OT and IT frameworks, ensuring comprehensive protection of vital infrastructure.

The panelists advocated for enhanced collaboration among policymakers, industry stakeholders, and technology providers to establish adaptive standards and frameworks that evolve alongside the threat landscape. By fostering partnerships that prioritize cybersecurity, organizations can strengthen their resilience against potential disruptions.

The conversation reinforced the importance of collective action, as each stakeholder has a critical role to play: policymakers facilitate international cooperation, industry players prioritize the security of economic assets, and technology firms integrate cybersecurity best practices into their products and services.

Ultimately, the panelists agreed that fostering global interconnectedness between governments, and encouraging multistakeholder forums, are essential to harmonize standards and build a resilient cybersecurity ecosystem. This collaborative approach not only safeguards individual organizations but also contributes to a broader movement towards a stable, secure Cyberspace that catalyzes opportunities and benefits for the global economy.

To watch the full session, scan the QR code:

SCAN HERE

Panel Discussion | Thriving Cyber Economy

OPEN FORUM

LEADERSHIP LAUNCHPAD

Charting Paths to Cyber Leadership

- **H.E. Dr. Hala Bint Mazyad Al-Tuwaijri**, President, Human Rights Commission, Saudi Arabia
- **Joy Chik, President**, Identity and Network Access, Microsoft
- **Silvana Koch-Mehrin**, Founder and President, Women Political Leaders (WPL)
- **Riz Khan (Moderator)**, Journalist and TV Host, Al Arabiya English

This session, 'Leadership Launchpad: Charting Paths to Cyber Leadership', explored the critical need to enhance leadership opportunities for women in cybersecurity, with a particular focus on addressing the gender talent gap in cybersecurity.

The discussion centered on developing strategies to advance women into leadership roles, emphasizing the importance of inclusivity in work environments, teams, and mentorship, and the need for corporate cultures to tap into women's unique perspectives in cybersecurity.

Speakers discussed the importance of creating clear pathways for women to enter and thrive in the cybersecurity workforce, where they remain significantly underrepresented. The conversation underscored the need for strategic investments in mentorship and peer networks, which help women navigate male-dominated industries and rise to leadership roles.

24% Women make up 24% of the global cybersecurity workforce in 2024

(Source: Global Cybersecurity Forum & Boston Consulting Group)

Moreover, the session reflected on the ongoing transformation within various sectors, where societal shifts and national reforms are enabling greater female participation. The discussion highlighted the long-term benefits of expanding the pipeline of female talent in cybersecurity and why that depends on offering women meaningful opportunities for growth in the sector.

The panelists agreed on the importance of fostering inclusive leadership pipelines, building mentorship structures, and creating opportunities for women to grow and excel in cybersecurity. Through such initiatives, they concur that the sector could harness the full potential of talented women, ensuring that cybersecurity leadership becomes more diverse, innovative, and resilient in the years to come.

To watch the full session, scan the QR code:

SCAN HERE

Fireside Chat | Beyond Cyber Discord

OPEN FORUM

CYBER STATECRAFT

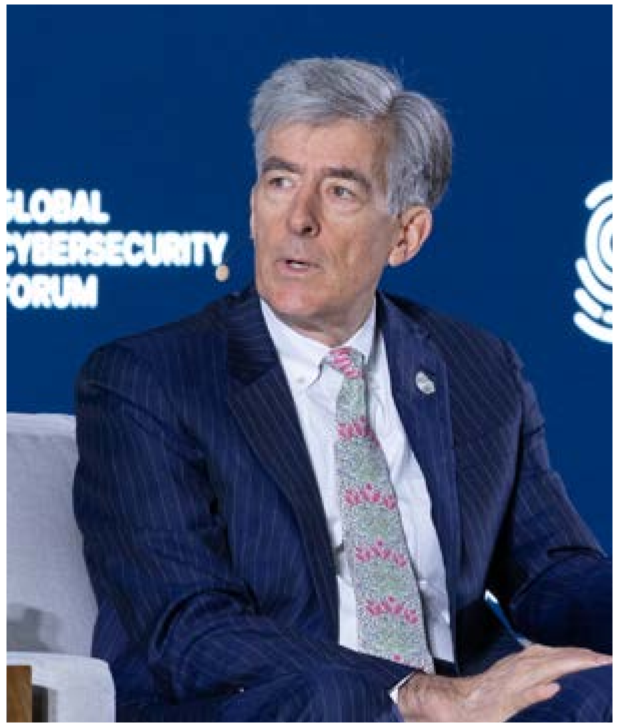
The New Chessboard of Geopolitics

- **Chris Inglis**, Former National Cyber Director, United States
- **Rima Maktabi (Moderator)**, Bureau Chief, Al Arabiya News Network

During the 'Cyber Statecraft: The New Chessboard of Geopolitics' fireside chat, Chris Inglis, former U.S. National Cyber Director, discussed the evolving dynamics of cybersecurity amid today's geopolitical landscape. He highlighted the growing prevalence of vulnerabilities in Cyberspace, the critical roles of both public and private sectors, and the transformative impact of emerging technologies like artificial intelligence. Central to Inglis' remarks was the need for a strategic, collaborative approach to tackle the complexities of cybersecurity in our interconnected world.

Inglis noted the fragility of current infrastructure, emphasizing that both national security and daily operations rely on increasingly vulnerable defense systems. He pointed out the persistent underinvestment in cybersecurity across sectors, which leaves vital infrastructure exposed to threats from nation states and organized criminal syndicates. He argued that the complacency surrounding these issues is what is most concerning, warning that the greatest cybersecurity threat may arise from a collective indifference towards proactive security efforts, which urgently need to be prioritized and implemented.

A key concept Inglis discussed was the need for a "new social contract" in Cyberspace to move from a competitive mindset to one of collective responsibility. He stressed that nations and organizations must collaborate to build trust, share information, and align capabilities rather than operate in isolation. For instance, while the finance sector in the U.S. has strong risk management capabilities, it may struggle with complex threats posed by nation state actors. Government intelligence can help inform the private sector and foster partnerships that enhance resilience. Without this collaborative effort, defenses against sophisticated cyber threats will remain inadequate.



Inglis urged countries to rethink their cybersecurity strategies as advancements in technology, including AI, continue to reshape the threat landscape. He underscored that fostering a resilient Cyberspace requires collaboration between governments, private entities, and citizens. By prioritizing collective action and shared responsibility, the global community can build stronger cyber defenses and pave the way towards a more secure and resilient future.

70% of leaders stated that geopolitics has at least moderately influenced their organization's cybersecurity strategy

(Source: World Economic Forum)

To watch the full session, scan the QR code:

SCAN HERE

Panel Discussion | **Beyond Cyber Discord**

OPEN FORUM

THE MULTILATERAL FRONTIER

Assessing the State of Play and Imperatives for Collective Action in Cyber Diplomacy

- **Dr. Robin Geiss**, Director, United Nations Institute for Disarmament Research (UNIDIR)
- **H.E. Massimo Marotti**, Managing Director, Strategies and Cooperation, National Cybersecurity Agency (ACN), Italy
- **Adam Hantman**, Deputy Director, Office of International Engagement and Capacity Building, Bureau of Cyberspace and Digital Policy, U.S. Department of State
- **Nisha Pillai (Moderator)**, International Moderator and Journalist

The panel discussion on 'The Multilateral Frontier: Assessing the State of Play and Imperatives for Collective Action in Cyber Diplomacy', explored the need for collaborative, international efforts to address the challenges of an increasingly complex Cyberspace. The session highlighted progress made by organizations such as the United Nations (UN), the European Union (EU) and the G7, while emphasizing the urgent need for deeper cooperation among nations to combat the escalating threat of cybercrime.

The session highlighted the UN's 25 years of negotiations, which culminated in the establishment of an international framework for responsible state behavior in Cyberspace in 2013. This framework confirmed that international law applies to Cyberspace, provided a foundation for norms governing state actions against malicious cyber activities, and dispelled the misconception that Cyberspace exists in a legal vacuum. However, panelists raised concerns about the challenges of assessing the impact of these diplomatic efforts in the face of rising tensions and escalating cyber threats, highlighting the complexities of evaluating the effectiveness of diplomatic efforts in such a high-risk environment.

Dr. Robin Geiss
Director, UN Institute for Disarmament Research (UNIDIR)
H.E. Massimo Marotti
Managing Director for Strategies and Cooperation, National Cybersecurity Agency (ACN), Italy
Adam Hantman
Deputy Director, Office of International Engagement and Capacity Building, Bureau of Cyberspace and Digital Policy, U.S. Department of State

Parallels were drawn between ongoing UN discussions and the protracted negotiations of the early nuclear age, emphasizing the need for established norms to govern state interactions in Cyberspace. These norms are not self-enforcing, necessitating collaboration between states to ensure they are being followed. The importance of capacity building to foster international cooperation was discussed, with a call for collective efforts to amplify these initiatives. In this context, the panelists noted that coalitions—some ad hoc and others more permanent—will be essential alongside the UN framework. Smaller coalitions with targeted objectives, such as those formed at the Global Cybersecurity Forum's Annual Meetings, can significantly contribute to addressing shared challenges and developing diverse strategies to strengthen global cybersecurity resilience.

The panelists asserted that effective cyber diplomacy requires a departure from traditional paradigms, advocating for innovative coalitions that transcend national borders and foster collective accountability. The discussions underscored the need for nations to engage in dynamic partnerships that not only share best practices but also contribute to creating actionable frameworks tailored to regional challenges. This proactive and collaborative stance is essential for addressing the complexities of cyber threats that impact the landscape of global cybersecurity. By prioritizing adaptive strategies and fostering inclusive dialogue, stakeholders can cultivate a more integrated response to the evolving cyber threat landscape.

125+ More than 125 countries have signed and/or ratified cybersecurity and cybercrime conventions, declarations, guidelines, or agreements, having resulted in fragmentation and diversity on the global level

(Source: UNODC)

To watch the full session, scan the QR code:

SCAN HERE

Panel Discussion | Thriving Cyber Economy

OPEN FORUM

CTRL + INVEST

Women Shaping the Future of Cyber Innovation

- **Christopher Steed**, CIO and Managing Director, Paladin Capital Group
- **David A. Hoffman**, Steed Family Professor of Cybersecurity Policy, Duke University & Stanford School of Public Policy
- **Dr. Mary Aiken**, Chair & Professor of the Cyberpsychology Department, Capitol Technology University
- **Lara Habib (Moderator)**, Senior Business News Presenter, Al Arabiya

The 'Ctrl + Invest: Women Shaping the Future of Cyber Innovation' session focused on the significant opportunities afforded by promoting gender diversity in cyber innovation. The panel addressed the challenges that women face in the cybersecurity startup world, particularly in securing venture capital funding – which remains disproportionately low for women-led startups. The session examined how increased diversity can positively impact innovation and resilience across the cybersecurity sector.

As things stand, only 2% of venture capital funding in Europe and the U.S. goes to women-led cybersecurity startups, and the figure is even lower in the Middle East. The panel emphasized the importance of creating inclusive environments to enable innovation and explored strategies to expand women's access to funding and mentorship opportunities that ultimately promote their broader participation in cybersecurity leadership and technological development.

Christopher Steed
CIO and Managing Director, Paladin Capital Group
Dr. Mary Aiken
Chair of the Cyberpsychology Department
Capitol Technology University
David A.
Duke University

The discussion underscored that diversity in leadership is not just an ethical imperative but a business one, with companies that demonstrate gender-diverse leadership teams shown to outperform their peers by 21% in profitability, according to the World Economic Forum. Panelists also reflected on the psychological barriers women often face, such as imposter syndrome, which can hinder their confidence in pursuing leadership roles or securing funding. Furthermore, the conversation emphasized the need for visible female role models in cybersecurity and the importance of introducing cybersecurity education at earlier stages, such as high school, to inspire young women to pursue careers in this field.

The discussion also highlighted the bias women face in securing venture capital, where women-led startups are often questioned about handling adversity, while male-led startups are asked about scaling. The panel stressed the need for more women in investment decision-making and advocated for targeted financing initiatives like micro-financing and crowdfunding. They called for focused efforts from investors to bridge the funding gap for women-led startups, which is crucial for driving innovation and resilience in cybersecurity.

11% While women hold 25% of tech jobs, they represent only 11% of executive roles in the tech industry in 2024

(Source: Forbes)

Panelists emphasized the importance of targeted initiatives from investors, government bodies, and corporate stakeholders to support women in cyber innovation, ensuring they have the tools, networks, and capital necessary to thrive. The session concluded with a shared commitment to fostering an ecosystem where women entrepreneurs can lead and drive the next wave of innovation in cybersecurity.

21% Companies with gender-diverse leadership are 21% more likely to outperform their peers in terms of profitability

(Source: WEF)

To watch the full session, scan the QR code:

SCAN HERE

Fireside Chat | Beyond Cyber Discord

OPEN FORUM

ECONOMIC SECURITY AND CRITICAL INFRASTRUCTURE

The Imperative of Building Trust in an Era of Geopolitical Competition

- **Heidi Crebo-Rediker**, Senior Fellow, Council on Foreign Relations
- **John Defterios (Moderator)**, former Emerging Markets Editor and anchor, CNN

In this session, Heidi Crebo-Rediker, Senior Fellow at the Council on Foreign Relations, delved into the crucial relationship between economic security and cyber threats, and the concerning risk they pose to critical infrastructure in an era of intensifying geopolitical competition. She highlighted the fact that critical infrastructure underpins every aspect of modern economies – from transportation systems to energy grids and financial networks – and emphasized that this infrastructure is now a frequent target of cyberattacks, often before kinetic warfare even begins.

Crebo-Rediker pointed out that today's critical infrastructure is no longer just about physical assets like roads or power lines; it has evolved into "smart" infrastructure that relies on connected technologies that make them highly susceptible to threats. She also highlighted the role of third-party providers in this landscape, who contribute to both the innovation and the vulnerabilities of these interconnected systems.

A key theme of the discussion was the challenge posed by the convergence of state-sponsored and criminal cyber actors, which complicates the task of protecting critical infrastructure. She emphasized that while there have been efforts to establish rules of engagement, particularly to protect civilian infrastructure from cyberattacks, these measures are often inadequate due to the complexity of the global cyber landscape.

Looking ahead, Crebo-Rediker underscored the importance of trusted international collaboration, not only among governments but also involving the private sector, to enhance resilience and build trust. She also noted that coalitions of willing nations could be more effective than broader multilateral bodies in addressing cyber threats.

Crebo-Rediker stressed that economic security depends on the global community's ability to build resilience into critical infrastructure by improving coordination for early warnings on vulnerabilities and ensuring accountability for cyberattacks through global sanctions.

$265B In 2023, cybersecurity incidents involving critical infrastructure surged, with ransomware alone predicted to cause damage exceeding $265 billion annually by 2031

(Source: Cybercrime Magazine)

GLOBAL CYBERSECURITY FORUM
ECONOMIC SECURITY AND CRITICAL INFRASTRUCTURE
John Defterios
Heidi Crebo-Rediker

To watch the full session, scan the QR code:

SCAN HERE

Panel Discussion | Beyond Cyber Discord

OPEN FORUM

BEYOND THE FIREWALL

Building a Cyber Resilient Supply Chain in a Hyperconnected World

- **Paul Selby**, CISO and Deputy CIO, U.S. Department of Energy
- **Akshay Joshi**, Head of Industry & Partnerships, Centre for Cybersecurity, World Economic Forum
- **Christophe Blassiau**, Senior Vice President, Cybersecurity & Product Security, Global CISO & CPSO, Schneider Electric
- **Michael Ruiz**, VP and General Manager for Cyber Products, Honeywell
- **Rebecca McLaughlin-Eastham (Moderator)**, independent TV anchor & media trainer

The panel discussion, 'Beyond the Firewall: Building a Cyber Resilient Supply Chain in a Hyperconnected World', explored the escalating vulnerabilities in global supply chains, underscoring the imperative to enhance cyber resilience within our interconnected world. The discourse highlighted the shortcomings in current cybersecurity practices and the essential role of public-private collaboration in strengthening supply chains. Participants emphasized that cultivating a resilient supply chain transcends mere technological solutions; it requires a holistic, collaborative approach to resilience.

The panelists highlighted the ongoing gap in foundational cybersecurity practices, such as the inconsistent implementation of multi-factor authentication and encryption across various sectors. Despite technological advances, many organizations still lag in fully adopting these essential protections, leaving critical vulnerabilities in industries that are integral to the global supply chain. Panelists stressed the importance of embedding cybersecurity from the outset and integrating it across all levels of operations to proactively address and mitigate risks.

The issue of "cyber inequity" was also discussed, which indicates the growing divide between organizations that are cyber resilient and those that are not. Panelists highlighted that disparities in cybersecurity maturity across organizations and nations are worsening and stressed that building a resilient ecosystem requires addressing these gaps through a global approach, where every player in the supply chain strengthens their cyber defenses.

The panel addressed the role of regulations in enhancing cybersecurity resilience, noting that over 60% of organizations have experienced positive impacts from regulatory measures. Far from being seen as a burden, these regulations are increasingly recognized as catalysts for both innovation and strengthened resilience.

The session concluded with a call for collective action, as the interconnected nature of supply chains means that cybersecurity challenges cannot be addressed through isolated efforts. Instead, a collaborative approach, built on strong public-private partnerships, shared responsibility, and standardized frameworks, is essential. The insights from this panel emphasize that cooperation, regulation, and proactive engagement are the cornerstones of securing global supply chains in an increasingly complex and connected world.

91% of organizations faced a software supply chain attack last year

(Source: Security Magazine)

To watch the full session, scan the QR code:

SCAN HERE

Panel Discussion | **New Cyber Frontier**

OPEN FORUM

BALANCING PROGRESS AND PERIL

Understanding the Challenges and Opportunities of AI in Cybersecurity

- **Brigaider-General Edward Chen**, Defense Cyber Chief, Ministry of Defense, Singapore
- **Ken Naumann**, CEO, NetWitness
- **Dr. Sadie Creese**, Professor of Cybersecurity, Oxford University
- **Dr. Helmut Reisinger**, CEO for EMEA and LATAM, Palo Alto Networks, Inc.
- **Adam Russell**, VP of Enterprise & Cloud Security, Oracle
- **Nisha Pillai (Moderator),** International Moderator and Journalist

This session on 'Balancing Progress and Peril: Understanding the Challenges and Opportunities of AI in Cybersecurity' examined the dual nature of artificial intelligence as both a driver of sophisticated cyber threats and a crucial asset in defense strategies. Panelists delved into the implications of AI advancements, highlighting the concerning increase in cyber threats enabled by AI technologies. They also explored strategies for organizations to effectively navigate these challenges and strengthen their cybersecurity defenses.

BALANCING
PROGRESS AND PERIL
Brigadier General Edward Chen
Defence Cyber Chief, Digital and Intelligence Service, Singapore
Ken Naumann
CEO, NetWitness
Dr. Sadie Creese
Professor of Cybersecurity, Oxford University
Dr. Helmut Reisinger
CEO for EMEA and LATAM, Palo Alto Networks, Inc.

A key area of focus was the "democratization of cyber skills," through which the accessibility of AI tools allows both seasoned hackers and novices, including teenagers, to exploit these technologies for malicious purposes. This lowered barrier to entry raises concerns about a potential surge in the sophistication and frequency of cyberattacks. Alarmingly, the time required to develop ransomware has decreased from 12 hours to just 3 hours with the advent of generative AI tools. Such rapid escalation underscores the urgent need for organizations to implement robust cybersecurity measures, especially as the average time for attackers to compromise systems and exfiltrate data has also significantly decreased.

The panelists reiterated that while AI integration presents formidable challenges, it also offers significant opportunities to enhance cybersecurity defenses. They underscored the importance of improved data quality and the adoption of AI-driven automation to streamline incident response, potentially reducing average response times from three and a half days to just 19 minutes. Furthermore, the panel emphasized the necessity of adaptive training for the emerging generation of cybersecurity professionals, referred to as 'AI natives', who can effectively harness these new technologies.

The discussion also highlighted the pressing need for clear regulations and governance surrounding AI technologies, stressing the importance of collaboration between governments and the private sector to mitigate risks. As the landscape evolves, these insights offer practical guidance for organizations looking to enhance security awareness and effectively navigate the complexities of rapidly evolving technologies in the cyber environment.

95% of cybersecurity professionals agree that AI-powered solutions will level up their organizations' defenses

(Source: Security Magazine)

To watch the full session, scan the QR code:

SCAN HERE

Plenary Session | **Beyond Cyber Discord**

OPEN FORUM

THE HISTORY OF CYBER DIPLOMACY FUTURE

Drawing Insights from Collaborative Progress on Trade, Nuclear, and Climate

- **H.E. Adel Al-Jubeir**, Minister of State for Foreign Affairs & Envoy for Climate Affairs, Saudi Arabia
- **Pascal Lamy**, Vice-President, Paris Peace Forum and former Director-General, World Trade Organization (WTO)
- **H.E. Ambassador Shyam Saran**, former Foreign Secretary, India
- **John Defterios (Moderator)**, former Emerging Markets Editor & anchor, CNN

The plenary session 'The History of Cyber Diplomacy Future: Drawing Insights from Collaborative Progress on Trade, Nuclear, and Climate' underscored the urgent need for innovative governance frameworks in Cyberspace. When contrasted with issues in more traditional domains like trade and climate change, the complexities of cyber threats highlight how anonymity and unpredictability can complicate accountability. The dialogue revealed that effectively addressing cybersecurity challenges requires not only national regulations, but also robust international collaboration grounded in education, shared norms, and standardized operating procedures.

A key insight was that classical multilateralism may not be sufficient in the case of addressing security challenges in Cyberspace, and that a "polylateral" approach, that engages various stakeholders beyond nation states, including private enterprises, NGOs, and academic institutions, is what is really needed. This paradigm shift is essential, given that entities influencing cyber dynamics extend beyond governmental borders, involving powerful corporations and mercenary hackers. The call for innovative engagement was reinforced by drawing parallels to established governance models like the International Civil Aviation Organization, which serves as a reference for how diverse stakeholders can contribute to the development of global standardized practices.

The dialogue also highlighted the disparity between developed and developing nations in terms of cybersecurity resilience. Concerns were raised about a potential "cyber fracture" that might exacerbate existing geopolitical challenges, emphasizing the need for more inclusive measures. It was suggested that more mature developing countries could play a pivotal role in bridging these divides, with a call for leading nations to commit to addressing disparities in technological access and expertise. Collaborative initiatives focused on child protection and women's empowerment were also proposed as a means to enhance cross-national cooperation in securing Cyberspace.

The discussion conveyed a unified message: as reliance on Cyberspace deepens, so must the global community's commitment to establishing comprehensive, agile cybersecurity governance frameworks that resonate globally. The collective aspirations expressed during the plenary emphasize a commitment to creating a secure and inclusive future for all, recognizing the shared challenges and connections between nations in the cyber age.

To watch the full session, scan the QR code:

SCAN HERE

Fireside Chat | New Cyber Frontier

OPEN FORUM

PRINCIPLES OF STABILITY

Applying the Lessons of the Past to the Current and Future Challenges in Cyberspace

- **Joy Chik, President**, Identity and Network Access, Microsoft
- **Rebecca McLaughlin-Eastham (Moderator)**, independent TV anchor & media trainer

The session on 'Principles of Stability: Applying the Lessons of the Past to the Current and Future Challenges in Cyberspace' took the form of an insightful fireside chat with Joy Chik, focusing on the evolving dynamics of cybersecurity. The discussion underscored the urgent need for organizations to shift from reactive measures to proactive strategies in response to emerging cyber threats. An estimated 600 million cyber-attacks daily highlight the need for a paradigm shift in cybersecurity practices to safeguard sensitive data and critical infrastructure.

A key takeaway from the conversation was the importance of fostering a proactive cybersecurity culture. Ms. Chik emphasized the importance of incorporating cybersecurity early in the product development lifecycle, advocating for a "secure by design" approach where security is embedded from the outset. This approach empowers organizations to identify and mitigate risks before they escalate, significantly reducing the likelihood of breaches in an increasingly complex and connected environment.

Collaboration and collective action across sectors emerged as another crucial theme. Ms. Chik characterized cybersecurity as a "team sport," asserting that no single entity can combat cyber threats in isolation. Strengthening overall defenses relies on partnerships among private enterprises, government agencies, and industry stakeholders. The conversation also emphasized the importance of intelligence sharing and collaborative problem-solving in building resilient cybersecurity frameworks.

Additionally, the discussion highlighted the utility of password-free authentication systems, such as passkeys, to address vulnerabilities associated with traditional passwords. These innovative solutions enhance security while simplifying user experience, representing a forward-thinking approach to a common challenge.

Ms. Chik reiterated the necessity for a multifaceted approach to cybersecurity, encompassing proactive measures, cross-sector collaboration, and innovative technologies. By embracing these strategies, stakeholders can navigate the complex cyber landscape more effectively, fortifying their defenses against persistent threats and ensuring a secure future.

To watch the full session, scan the QR code:

SCAN HERE

Panel Discussion | New Cyber Frontier

OPEN FORUM

SHIELDING CONNECTIVITY

Safeguarding Future Networks

- **Bocar Alpha Ba, CEO**, SAMENA Telecommunications Council
- **Yasser Alsuwailem**, Group VP for Cybersecurity, STC Group
- **H.E. Mohamed Ben Amor**, Director General, Arab ICT Organization
- **Yang Chengxi (Moderator)**, International Reporter, CGTN

The 'Shielding Connectivity: Safeguarding Future Networks' session delved into the challenges and opportunities posed by the shift from 5G to 6G technology. Panelists discussed the transformative potential of 6G, with near-zero latency and communication speeds that may reach up to 100 times faster than 5G. The conversation also underscored the incomplete deployment of 5G, which raises significant concerns regarding cybersecurity vulnerabilities that must be addressed prior to the full-scale implementation of 6G.

A key focus of the dialogue was the need for a proactive cybersecurity strategy that can keep pace with these advanced and evolving technologies. Panelists highlighted the indispensable role of artificial intelligence in enhancing network reliability, safeguarding data integrity, and ensuring privacy in increasingly complex environments. With projections that interconnected devices could grow to one million per square kilometer in the 6G ecosystem, the number and diversity of cyber threats are expected to increase.

Global collaboration emerged as a pivotal theme, with panelists asserting the necessity of collective action by governments, the public and private sectors, and academia. Such alliances are vital for crafting robust regulatory frameworks and enabling effective cross-border data sharing—both essential in mitigating cyber threats. Capacity building initiatives in nascent telecommunications markets were also identified as critical components in a more secure global network.

The principle of 'security by design' was also explored, with panelists noting that many cybersecurity vulnerabilities emerge from legacy systems in which security was not prioritized during the initial design process. Looking ahead, embedding security measures into the core architecture of emerging technologies like 6G is essential to building resilient networks capable of withstanding future threats and challenges.

While the transition to 6G promises unprecedented benefits, its associated cyber risks also demand a strategic and comprehensive response. A strong commitment to proactive strategies, global collaboration, and a security-first design philosophy will be crucial to safeguarding future networks and ensuring their resilience in an increasingly interconnected world.

4.1M At any given time, 4.1 million sites are infected with malware

(Source: SiteLock)

To watch the full session, scan the QR code:

SCAN HERE

Panel Discussion | Cyber Psychology

OPEN FORUM

COGNITIVE RESILIENCE

Building Psychological Defense Against Cyberattacks

- **Dr. Mary Aiken**, Chair & Professor of the Cyberpsychology Department, Capitol Technology University
- **Dr. Neal Jetton**, Director, Cybercrime, INTERPOL
- **Chris Gibson**, Executive Director, Forum of Incident Response & Security Teams (FIRST)
- **Major General (Rtd) Mohammad Boarki**, Chief, National Cyber Security Center, Kuwait
- **Filippo Cassini**, Global Technical Officer and Senior VP of Engineering, Fortinet
- **Riz Khan (Moderator)**, international journalist and TV host, Al Arabiya English

In the session on 'Cognitive Resilience,' panelists explored the concept of and sought actionable solutions around the building of psychological defenses against cyberattacks. The discussion began by outlining the human element in the cyber landscape, with emphasis placed on the need to mitigate vulnerabilities by strengthening both cognitive resilience and technological infrastructure. One panelist pointed out that psychological resilience varies greatly between individuals, highlighting that a one-size-fits-all approach is not effective when it comes to supporting people in Cyberspace.

Another expert emphasized the role of global collaboration between governments, law enforcement, and private sectors as key to advancing cybersecurity capabilities. The significance of knowledge-sharing and collective action was repeatedly stressed as crucial for preparing both individuals and organizations to deal with the psychological impact of cyberattacks.

The panel also explored strategies for handling high-pressure situations experienced by incident response teams, stressing the importance of maintaining mental preparedness and fostering teamwork. National approaches to cybersecurity were discussed, with particular attention paid to the need for rapid, coordinated responses to protect critical infrastructure during large-scale cyber threats.

Automation and artificial intelligence were seen as important tools to support cybersecurity professionals. However, a key focus remained on the differing psychological impacts of various cyberattacks, with panelists stressing that education and tailored responses to specific attack types are essential for effective resilience-building across all levels of society.

To watch the full session, scan the QR code:

SCAN HERE

Panel Discussion | **New Cyber Frontier**

OPEN FORUM

THE PULSE OF SECURITY

Securing the Healthcare Sector Amidst Technological Disruptions

- **Dr. Richard Staynings**, Chief Security Strategist, Cylera & Teaching Professor, University of Denver
- **Prof. Junaid Nabi**, Senior Fellow, The Aspen Institute
- **Mike Fell OBE, Director**, National Cyber Operations, NHS England
- **Lara Habib (Moderator)**, Senior Business News Presenter, Al Arabiya

The 'The Pulse of Security' panel explored the cybersecurity challenges faced by the healthcare sector amid rapid technological advancements. The healthcare industry has increasingly embraced tools such as telehealth and electronic health records, which have enhanced patient care and operational efficiency. However, this adoption has exposed healthcare systems to heightened risks, making them targets for cyberattacks.

Panelists highlighted how the healthcare sector's legacy systems and weak cybersecurity measures make it one of the most vulnerable areas of critical infrastructure. Cybercriminals are attracted to healthcare data due to its high value and long-term sensitivity: unlike financial data, which can be changed or reset, healthcare information remains static, making it particularly exploitable. The risks go beyond financial loss—cyberattacks can threaten patient safety, with recent ransomware attacks compelling hospitals to shut down critical systems and delay treatments.

In the discussion, experts examined the impact of emerging technologies such as artificial intelligence and machine learning. While these innovations offer enormous potential for enhancing medical diagnosis and treatment, they also introduce new vulnerabilities. AI can be exploited to manipulate healthcare data or disrupt medical devices, potentially putting lives at risk. Panelists emphasized the need for a robust cyber resilience strategy to protect sensitive health data and maintain trust in healthcare systems. The conversation emphasized that while global frameworks provide structured guidelines for managing risks, their effectiveness relies heavily on adequate funding and healthcare organizations' commitment to implementation.

In the context of an increasingly complex and connected healthcare environment, panelists called for a multi-faceted approach to cybersecurity. This includes stronger global cooperation, ongoing education for healthcare workers, and ensuring that cybersecurity is treated as a critical component of both operational efficiency and patient safety.

54% In 2023, 54% of healthcare organizations experienced a ransomware attack, up from 41% in 2022

(Source: HIPAA Journal)

To watch the full session, scan the QR code:

SCAN HERE

Fireside Chat | Beyond Cyber Discord

OPEN FORUM

NAVIGATING THE FUTURE

Advancing International Cooperation to Build Confidence in Cyberspace

- **Doreen Bogdan-Martin,** Secretary-General, International Telecommunication Union
- **Riz Khan (Moderator)**, International journalist and TV host, Al Arabiya English

The fireside chat, 'Navigating the Future: Advancing International Cooperation to Build Confidence in Cyberspace,' featured Doreen Bogdan-Martin, Secretary-General of the International Telecommunication Union (ITU). She highlighted the urgent need for strengthened international collaboration and collective action to address the rising cybersecurity threats facing global networks.

The discussion traced the evolution of the cyber threat landscape since the early 2000s, when the World Summit on the Information Society (WSIS) first convened and highlighted a surge of internet users that has seen the online population grow from 1 billion then to over 5.4 billion today. With this growth comes increased risks, exemplified by the recent 'RockYou2024' incident that demonstrated the vulnerability of a connected world by exposing 10 billion passwords. Addressing these challenges demands not only cutting-edge technical solutions but also adaptable global policy frameworks.

A key issue raised was the disparity between nations with advanced cybersecurity capabilities and those lacking critical resources. The conversation stressed that capacity building in under-resourced regions must be a priority for international collaboration, as failure to address this capacity gap could exacerbate global inequalities. Collective action was positioned as vital to ensuring no nation is left behind in addressing shared cyber threats.

The discussion also underscored the global cybersecurity skills shortage. Ms. Bogdan-Martin highlighted the importance of early education and targeted skills development to address this challenge, and ITU-led collaborations with countries around the world were showcased as examples of how nations can leapfrog in progress while embedding strong cybersecurity frameworks from the outset. The session concluded with a call for enhanced international cooperation, capacity building, and inclusivity, as cyber resilience becomes increasingly critical in a hyper-connected global landscape.

To watch the full session, scan the QR code:

SCAN HERE

Fireside Chat | Beyond Cyber Discord

OPEN FORUM

CRIME INC.

The Institutionalization of Organized Cybercrime

- **Josh Goldfoot**, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice
- **John Defterios (Moderator)**, former CNN, Emerging Markets Editor & anchor

The 'Crime Inc.' fireside chat provided an in-depth exploration of the increasing sophistication of organized cybercrime and its far-reaching impact on societies and economies. Josh Goldfoot, Deputy Assistant Attorney General at the U.S. Department of Justice, described how cybercrime has evolved from small-scale attacks into highly specialized networks that cross sectors and borders. These criminal networks function like decentralized marketplaces, where individuals with specialized skills—from reconnaissance and malware deployment to data theft and ransom collection—collaborate to carry out attacks.

Goldfoot emphasized that the rise of ransomware has become one of the most concerning trends, with criminals exploiting known vulnerabilities to penetrate systems and demand ransoms for encrypted data. He noted the role of cryptocurrency in facilitating these crimes, as it provides anonymity and a way for criminals to bypass traditional financial systems.

In response to the rising threat, Goldfoot stressed the necessity of international collaboration and collective action. He discussed how partnerships between law enforcement agencies across borders, including Europol and Interpol, have been instrumental in tackling cybercriminal operations. He noted that the challenge of combating cybercrime isn't simply about removing individual bad actors, but also about dismantling the underlying infrastructure that enables these activities.

The conversation also turned toward the future of cybersecurity. Goldfoot urged businesses to improve their defenses, specifically recommending hardware-based multi-factor authentication to protect against unauthorized access. He pointed out that recent regulatory changes, such as the U.S. Securities and Exchange Commission's (SEC) requirement for companies to disclose significant cybersecurity incidents, are a clear signal to investors that cyber resilience is becoming a critical factor in evaluating corporate risk. Ultimately, Goldfoot concluded that while prosecution remains a key tool in fighting cybercrime, the long-term solution lies in improving network security and taking proactive measures to prevent attacks before they occur.

$23.84T The global cost of cybercrime is forecast to jump to $23.84 trillion by 2027

(Source: Statista)

To watch the full session, scan the QR code:

SCAN HERE

OPEN FORUM

FROM SHORTAGE TO STRENGTH

Closing the Cybersecurity Skills Gap for a Resilient Cyberspace

- **Dr. Haji Amirudin Abdul Wahab**, Chief Executive Officer, CyberSecurity, Malaysia
- **Sheikh Salman bin Mohammed Al Khalifa**, CEO, National Cyber Security Center (NCSC), Kingdom of Bahrain
- **Dan Cîmpean**, Director, National Cybersecurity Directorate, Romania
- **Dr. Bernd Pichlmayer**, CEO and Founder, FTGG Cyber
- **Nisha Pillai (Moderator)**, international moderator and journalist

The 'From Shortage to Strength' panel provided an in-depth exploration of the global cybersecurity skills gap, a critical issue that is impacting both public and private sectors. The World Economic Forum estimates a global shortage of nearly 4 million cybersecurity professionals, underscoring the urgency of developing solutions. Panelists agreed that the skills gap is not simply a technical challenge but a multifaceted issue requiring a holistic response.

A key insight shared during the discussion was that cybersecurity roles are rapidly evolving beyond their traditional, technical scope. Panelists noted that today's cybersecurity landscape requires a broader set of skills, incorporating expertise from disciplines such as law, psychology, and economics.

Panelists highlighted innovative national programs aimed at training cybersecurity talent, including initiatives that combine academic knowledge with real-world experience. National cybersecurity academies are emerging as key drivers of workforce development, offering certification programs that are both industry-aligned and accessible. These academies collaborate with a range of stakeholders, from government agencies to private industry, to ensure a steady pipeline of talent. The importance of making cybersecurity training affordable and scalable was also emphasized as a critical component in addressing the workforce gap.

Sheikh Salman Alkhalifa
CEO, National Cyber Security Center, Kingdom of Bahrain
Dr. Haji Amirudin Abdul Wahab
CEO, CyberSecurity Malaysia
Dan Cîmpean
Director, National Cybersecu

The panel also delved into the role of artificial intelligence in shaping the future of cybersecurity. While AI presents new challenges by introducing sophisticated threats, it also offers opportunities to enhance cybersecurity operations in areas like automation. By reducing the burden of repetitive tasks, such as monitoring and threat detection, AI can free up cybersecurity professionals to focus on more strategic, high-impact activities like threat hunting and proactive defense.

Finally, the discussion emphasized the importance of addressing the skills gap holistically, cautioning against organizations poaching talent from each other—which only shifts the gap elsewhere—and instead focusing on supporting the development of new experts to close the gap. Panelists stressed the need for fostering long-term growth in cybersecurity talent through education, cross-sector collaboration, and the creation of flexible work environments that attract younger professionals. Cybersecurity is no longer an isolated technical function but a strategic imperative that requires multi-disciplinary expertise across the entire workforce.

2.8M It is estimated that the global cybersecurity workforce shortage stands at 2.8 million professionals

(Source: Global Cybersecurity Forum & Boston Consulting Group)

To watch the full session, scan the QR code:

SCAN HERE

Panel Discussion | Beyond Cyber Discord

OPEN FORUM

SECURING THE SPOTLIGHT

Cybersecurity Roadmap for Mega Events

- **Dr. Hazim S. Almuhimedi**, Deputy Governor, Risk & Compliance, National Cybersecurity Authority (NCA), Saudi Arabia
- **João Marcelo Azevedo Marques Mello da Silva**, Advisor, National Telecommunications Agency – Anatel, Brazil
- **Ahmed Mohammed Al Hammadi**, Director, National Cyber Fusion Affairs, National Cyber Security Agency, Qatar
- **Laura Buckwell (Moderator)**, international moderator

The 'Securing the Spotlight' panel focused on the pivotal role of cybersecurity in protecting large-scale global events such as the upcoming FIFA World Cup and Expo 2030. With the heightened attention these events attract, the panel stressed the increasing range of cyber threats and the shared responsibility of both public and private sectors in securing national interests. The discussion highlighted the importance of thorough preparation, strong collaboration across a range of stakeholders, and the adoption of advanced technologies to ensure comprehensive security measures.

A pivotal insight from the session was the imperative of fostering collaboration among stakeholders to effectively mitigate cybersecurity risks. Panelists emphasized the necessity of defining the scope of cybersecurity challenges by identifying all stakeholders and third-party contractors and navigating the complexities of public safety management, reflecting the multifaceted nature of securing major events. Compelling case studies from nations experienced in hosting large-scale gatherings illustrated the efficacy of deploying on-site personnel to promptly address technical issues—a crucial strategy for ensuring operational success.

The panel also explored the dual nature of advanced technologies, such as 5G and the Internet of Things (IoT). While these innovations enhance connectivity and operational efficiency, they also introduce new vulnerabilities. The discussion highlighted the need for robust risk management frameworks to secure these emerging systems, reflecting an overarching imperative for vigilance and preparedness. Establishing comprehensive cybersecurity frameworks and developing detailed risk mitigation plans were underscored as fundamental components of effective event preparation.

In conclusion, the panelists unanimously agreed on the critical need for international collaboration on cybersecurity. The recurring theme that 'cybersecurity is a shared responsibility' reinforced the importance of continuous dialogue, cross-border cooperation, and collective action.

To watch the full session, scan the QR code:

SCAN HERE

ANNUAL MEETING PROCEEDINGS: PARTICIPATORY TRACK

ROUNDTABLES

HIGH-LEVEL ROUNDTABLE ON COLLECTIVE ACTION IN CYBERSPACE

The 2024 High-Level Roundtable on Collective Action in Cyberspace brought together senior government officials, industry leaders, and representatives from international organizations to reinforce the global community's collective cybersecurity efforts. Building on the insights from previous discussions, this year's session focused on three critical issues: bridging the global cybersecurity workforce gap, leveraging the potential of generative AI, and mitigating the impact of ransomware on human beings. The discussions highlighted the pressing need for enhanced cross-border and cross-sector collaboration to secure the future of Cyberspace.

Closing the Global Cybersecurity Talent Gap
The session began by addressing the critical shortage of cybersecurity professionals around the world – a gap that threatens global cyber resilience. Findings from the 2024 Global Cybersecurity Workforce Report, published by GCF and BCG, highlighted that the current cybersecurity workforce is 2.8 million professionals short of meeting demand. This deficit is particularly acute in high-risk sectors like financial services, technology, and industry, which are increasingly targeted by cybercriminals. Speakers underscored that bridging this gap will require more than traditional training approaches. Instead, it calls for innovative solutions such as targeted re-skilling programs and interdisciplinary training, and cooperation among governments, industry, and academia will be vital to developing a workforce capable of navigating the rapidly evolving cybersecurity landscape.

ADVANCING COLLECTIVE ACTION IN CYBERSPACE
GLOBAL CYBERSECURITY FORUM

Harnessing the Potential of Generative AI for Cybersecurity
The discussion then moved on to the dual nature of generative AI (GenAI), which presents both significant opportunities and complex challenges in cybersecurity. On one hand, GenAI has the potential to revolutionize defenses through automation and real-time threat detection. On the other hand, it reduces the barrier to entry for cybercriminals, enabling them to launch more sophisticated and rapid attacks. Stakeholders stressed the importance of global cooperation in establishing regulatory frameworks for AI in Cyberspace, underscoring the need for public-private partnerships to create ethical standards and ensure responsible use of AI technologies. Additionally, speakers noted that when properly integrated into security strategies, AI can help address the talent shortage by automating routine tasks and strengthening overall defensive capabilities.

Mitigating the Human Impact of Ransomware
Finally, the devastating impact of ransomware was discussed by participants, with a focus on shifting away from its financial consequences to the profound toll it takes on people. Attacks on critical infrastructure, particularly in the healthcare and energy sectors, have jeopardized lives and shaken public confidence in cybersecurity to protect critical infrastructure. Speakers emphasized the pressing need for coordinated global efforts to bolster resilience against ransomware, including enhanced real-time intelligence sharing and more robust public-private partnerships. Law enforcement representatives stressed the importance of unified actions to dismantle ransomware networks and ensure perpetrators are held accountable. The consensus was unequivocal: global cooperation is vital to address the escalating human impact of ransomware attacks.

The roundtable concluded with a renewed commitment from all participants to collaborate in addressing these urgent challenges. The discussions reaffirmed the global community's commitment to building a more secure, resilient, and cooperative cyber landscape, foregrounding collective action as the key to navigating an increasingly interconnected world.

CYBER CXO

CYBER CXO MEETING

An invite-only C-suite meeting to discuss key challenges, implications, and collaborative strategies in cybersecurity

The second Cyber CxO Meeting was held during the GCF Annual Meeting 2024, building on GCF's mission to provide a collaborative platform for global cybersecurity stakeholders to engage, share insights, and drive collective action. This exclusive gathering brought together 26 C-suite executives from leading cybersecurity firms across 12 countries. The discussions focused on two critical areas - cyber resilience in critical infrastructure and cyber Generative AI (GenAI), aiming to explore emerging challenges, their implications for the private sector, and actionable pathways for progress.

Discussion topics included the evolving threats in supply chain security and the need to balance innovation and stability in legacy systems. Participants also highlighted challenges related to the rapid advancement of AI, with the discussion focusing on the dual impact of Gen AI and the development of policies for safe AI integration.

Strengthening Supply Chain Security
Participants emphasized the importance of strengthening supply chain security through measures including adoption of Zero Trust architectures and implementation of robust software quality assurance. Furthermore, prioritizing digital sovereignty by minimizing external dependencies can ensure control over critical national assets and reduce potential risks.

Enhancing Resilience in Legacy Systems
The meeting addressed the need to enhance resilience in legacy systems, highlighting the critical role of public-private collaboration in modernizing these outdated systems while avoiding operational disruptions. Building trust through strategic partnerships and adopting a client-focused approach tailored to specific needs can further support this transformation.

Leveraging AI for Cyber Defense
Artificial intelligence (AI) was a key topic of discussion, with participants exploring how its power can be harnessed for cyber defense. The dialogue centred on the role of AI in enhancing monitoring capabilities, identifying anomalies, and automating incident responses, ensuring proactive and efficient cybersecurity across critical systems.

Protecting AI Models and Establishing Regulations
The discussion highlighted the importance of protecting AI models and establishing regulations for cybersecurity. Securing AI against tampering, biases, and adversarial attacks safeguards its reliability, whilst the development of comprehensive regulatory frameworks promotes the responsible use of AI, balancing the need for innovation with ethical and secure practices.

HIGH-LEVEL MULTISTAKEHOLDER ROUNDTABLE DISCUSSION

The 2024 High-Level Multistakeholder Roundtable brought together government officials, industry leaders, and representatives from international organizations to discuss the critical challenges and opportunities shaping Cyberspace. Building on insights from previous years, this discussion focused on three pressing topics: rethinking the cybersecurity workforce in the age of AI, optimizing the regulatory environment to foster innovation, and identifying new pathways to unleash future innovation in cybersecurity. The dialogue underscored the importance of building a resilient and future-ready cyber ecosystem through cross-border collaboration and collective action.

Rethinking the Cyber Workforce in the Age of AI
The roundtable addressed the growing challenges of building a future-ready cybersecurity workforce in an era increasingly shaped by AI. Participants discussed the findings of the 2024 Global Cybersecurity Workforce Report, which identified a shortage of 2.8 million professionals in the sector. The report outlined three key skill gaps expected to persist over the next five years: leadership in cybersecurity (a top concern for over 50% of organizations), network and security architecture (reported by 45% of organizations), and cloud security (a pressing issue for 44% of organizations, due to the rapid shift toward cloud services). Traditional training approaches were deemed insufficient, with speakers advocating for adaptive learning programs that leverage AI to provide real-time, hands-on experience. Collaboration across the entire cybersecurity ecosystem was highlighted as critical to closing the workforce gap. Participants also noted the role of AI-driven training platforms in enhancing both recruitment and skill-building efforts. Innovative approaches to training, such as integrating AI tutors, were discussed as effective solutions to enhance the workforce's ability to address complex threats.

Optimizing the Regulatory Environment for Cybersecurity Innovation
Participants explored the challenges posed by fragmented regulatory frameworks, which can hinder the ability of companies to innovate and operate efficiently across borders. Policymakers were urged to harmonize these frameworks to align security needs with growth and innovation goals. The importance of developing open standards to facilitate cross-border collaboration was a key theme, with participants calling for regulatory consistency to reduce compliance burdens on businesses. Participants underscored the importance of public-private collaboration in fostering innovation, noting that regulatory frameworks should not stifle innovation but rather support companies in adopting new technologies, while maintaining strong cybersecurity practices.

Unleashing Future Cyber Innovation
The discussion on innovation also focused on identifying potential barriers and enablers for advancements in cybersecurity. While participants acknowledged the increasing flow of investment and talent into the sector, they noted that cybersecurity still lags behind other industries in terms of innovation. Calls were made for stronger government support to incentivize private sector innovation, including providing infrastructure that allows start-ups to test and scale solutions effectively. Participants emphasized the importance of balancing global competitiveness with local needs, urging companies to develop solutions that support national markets. The growing trend toward digital sovereignty was discussed, with speakers advocating for the localization of cybersecurity solutions to meet country-specific challenges.

The roundtable concluded with the consensus that innovation in cybersecurity must not only focus on the development of new technologies but also address the maintenance of legacy systems. Participants emphasized the importance of fostering resilience and innovation by aligning security efforts with the rapidly evolving landscape of cybersecurity.

ROUNDTABLES

ROUNDTABLE ON ACTIVE DEFENSE

The Roundtable on Active Defense brought together cybersecurity professionals, government representatives, and industry leaders to tackle one of the most pressing challenges in Cyberspace: shifting from a reactive defense posture to an active one. The session welcomed experts from fields across cyberpsychology, law enforcement, and the private sector to address the rapidly evolving landscape of cyber threats. The discussion emphasized the urgent need to move beyond passive defense strategies and adopt dynamic, proactive solutions that place human-centric cybersecurity at the forefront of defense.

Reframing the Human Element in Cyber Defense

One of the key insights from the discussion was the importance of addressing psychological vulnerabilities in Cyberspace, a critical area often overlooked in traditional cybersecurity frameworks. Drawing from the U.S. Joint Cyber Doctrine, which identifies three layers of Cyberspace—the physical, logical, and cyber persona—participants highlighted that while systems effectively protect the physical and logical layers, the human, or cyber persona layer, remains particularly exposed. Many cyberattacks exploit human behaviors, with 90% to 95% of attacks stemming from social engineering tactics like phishing. Participants emphasized the need to integrate psychological defenses into cybersecurity strategies, focusing on disrupting the decision-making processes of cybercriminals. Emerging doctrines, such as the "cognitive effect" (e.g., influencing or disrupting the cognitive processes of an adversary, often through non-kinetic means like psychological operations, information warfare, or cyber strategies), aim to counter these threats by targeting the psychological vulnerabilities of attackers through proactive measures.

Integrating AI for Scalable Active Defense

The roundtable also explored the role of artificial intelligence (AI) and machine learning (ML) in scaling active cyber defense. Given the increasing volume and complexity of cyberattacks, human responses alone are no longer sufficient. Participants discussed the potential of AI-driven solutions, such as automated systems, to intercept and respond to cyberattacks in real-time, particularly in the event of ransomware and malware attacks. However, it was agreed that human oversight remains crucial to ensure that AI-driven defense systems respond ethically and strategically. AI should assist in creating behavioral profiles of attackers and predicting their moves, giving defenders an advantage in real-time responses. The consensus was that AI should enhance, rather than replace, human decision-making in active defense strategies.

A Call for Global Collaboration

Throughout the discussion, participants emphasized the need for global collaboration to address increasingly sophisticated cyber threats. Given the borderless nature of cyberattacks, a collective response involving governments, industries, and research institutions is critical. The roundtable highlighted the crucial role that private sector innovation plays in defending against cyberattacks and stressed the importance of multi-level coordination, combining national, organizational, and international efforts to form a unified defense system that addresses the complexities of the modern cyber threat landscape.

The roundtable concluded with a strong call for collective action in shaping the future of active cyber defense. While AI and advanced technologies will play a critical role, human insight remains essential. Law enforcement alone cannot manage the growing cyber threat landscape, and private sector collaboration will be indispensable. The session underscored the need for proactive defense measures, with participants agreeing that active defense must become a core component of national and organizational cybersecurity strategies. As cyber threats continue to evolve, transitioning from passive to active defense is no longer optional but necessary to ensure the protection of Cyberspace for people around the world.

Panel Discussion

DEEP DIVE SESSIONS

PERSPECTIVE REVERSAL

Cognitive Strategies and Orientations of Attackers

- **Dr. Yacine Djemaiel,** CEO, National Agency for Cybersecurity (TunCERT), Tunisia
- **Oliver Väärtnõu,** CEO, Cybernetica
- **Harold Rivas,** CISO, Trellix
- **Kevin Brown,** Chief Operation Officer, NCC Group
- **Yang Chengxi (Moderator),** International Reporter, CGTN

The 'Perspective Reversal: Cognitive Strategies and Orientations of Attackers' panel explored the advanced psychological tactics increasingly used by cybercriminals, stressing the importance of understanding these cognitive strategies to strengthen cybersecurity defenses. In today's interconnected landscape, attackers exploit human vulnerabilities to manipulate users and bypass technical safeguards, making it critical to incorporate the human element into security protocols. The discussion highlighted that many cybercriminals aim to steal sensitive personal information by exploiting these cognitive vulnerabilities, often bypassing even the most robust security measures through social engineering and other psychological methods.

78% of deepfake phishing attacks are delivered via email

(Source: Global Incident Response Threat Report)

The conversation highlighted the fact that phishing attacks are becoming increasingly sophisticated, driven by advancements in artificial intelligence (AI) and open-source intelligence. Attackers have begun to impersonate high-profile individuals more convincingly, making it harder for victims to differentiate between legitimate communications and scams. Additionally, the rise of generative AI has escalated the risks, enabling deepfake campaigns and advanced data analyses that allow attackers to map internal business relationships and launch highly targeted attacks.

Looking forward, the panelists emphasized the need for interdisciplinary collaboration between cybersecurity experts and psychologists to enhance cognitive resilience among individuals facing these threats. Proactive measures, including structured training programs and support systems for incident response teams, were deemed critical to mitigate the psychological strain caused by high-pressure cyber incidents. The panelists agreed that comprehensive national strategies, which integrate frameworks for mental health preparedness into cybersecurity defense measures, are critical to foster societal resilience in the face of large-scale cyber threats.

Panel Discussion

DEEP DIVE SESSIONS

EQUIPPING THE DEFENDERS

What Law Enforcement Needs to Win

- **Pablo Muñoz, Principal Commissar,** General Secretary of Operations and Digital Transformation Division, Directorate General of Spanish National Police, Spain
- **Dr. Neal Jetton,** Director, Cybercrime, INTERPOL
- **Mustafa Ünal Erten,** Chief, Centre for Combating Cybercrime, United Nations Office on Drugs and Crime (UNODC)
- **Rudolph Lohmeyer (Moderator),** Partner, Kearney

This session examined the challenges and opportunities for law enforcement agencies in the fight against online child exploitation amidst an evolving cyber landscape. Key themes included the impact of emerging technologies on online child abuse, and the necessity for multistakeholder collaboration to boost information sharing.

The discussion focused on strategies to enhance law enforcement's response to these crimes, highlighting the risks that accompany an expanding attack surface and the need for specialized skills to address future threats. Panelists emphasized the critical role of international organizations in supporting law enforcement agencies as they continue to face unique new challenges, including the growing issue of child abuse facilitated by emerging technologies.

Additionally, the session delved into innovative approaches for collaboration between law enforcement and technology companies, which can play a transformative role in combating these issues. The importance of real-time intelligence sharing and overcoming jurisdictional barriers was also underscored, along with the potential for cutting-edge technologies to significantly strengthen law enforcement capabilities in addressing online child abuse.

The session concluded by reinforcing the need for continued global collaboration and technological innovation, in areas such as artificial intelligence (AI), to protect vulnerable communities like children in Cyberspace.

82% rise in online grooming crimes against children in the last 5 years

Source: (NSPCC)

Invite-only Brief

DEEP DIVE SESSIONS

SAFEGUARDING THE CYBER HEARTBEAT

Insight on Leveraging AI for Patient Data Protection

- **Prof. Junaid Nabi,** Senior Fellow, The Aspen Institute
- **Shoaib Yousuf (Moderator),** Managing Director & Partner, BCG

During the fireside chat on 'Safeguarding the Cyber Heartbeat: Insight on Leveraging AI for Patient Data Protection', Professor Junaid Nabi, Senior Fellow at the Aspen Institute, explored the pressing cybersecurity challenges facing the healthcare sector. As the sector undergoes rapid digitalization, particularly in the areas of telehealth and patient data, the risks of disruptive cyberattacks are growing. Professor Nabi highlighted that the healthcare sector accounts for 17% of global cybersecurity incidents, emphasizing the need for stronger cybersecurity measures.

The discussion focused on the increased vulnerabilities that accompany a broadening reliance on AI and machine learning technologies. While these technologies offer powerful tools for analyzing vast amounts of patient data and detecting anomalies, they also expose the sector to new risks. Professor Nabi emphasized the importance of building trust through transparency and accountability, urging healthcare providers to proactively communicate their cybersecurity measures to patients. He further stressed that addressing cybersecurity in healthcare is not just a technical issue but a matter of trust, requiring collaboration between public and private sectors to ensure robust and adaptable protections.

82% of healthcare CFOs identified privacy breaches as a significant risk for 2024

(Source: BDO)

Invite-only Brief

DEEP DIVE SESSIONS

GLOBAL VIEW SERIES

Korea's Cybersecurity Journey

- **Dr. Jinyoung Oh,** Vice President, Korea Internet & Security Agency (KISA)

This Deep Dive session of the Global View Series was on Korea's Cybersecurity Journey. Dr. Jinyoung Oh, Vice President of Korea Internet & Security Agency (KISA), outlined Korea's robust efforts in advancing its cybersecurity ecosystem. The session delved into Korea's multi-faceted approach, focusing on the nation's commitment to cultivating a strong cybersecurity workforce, with a goal to train 100,000 security professionals through diverse programs and initiatives. Dr. Oh highlighted key collaborations with global partners and stressed the importance of mutual progress through frameworks like the Cybersecurity Alliance for Mutual Progress (CAMP), which fosters international cooperation in cybersecurity.

Furthermore, Dr. Oh discussed the nation's focus on securing critical infrastructure and expanding into emerging fields, such as autonomous vehicles and healthcare cybersecurity. The session highlighted Korea's approach to AI governance, underscoring the need for privacy protection and regulatory advancements to keep pace with AI developments. The session emphasized that a zero-trust security model and bolstering supply chain security are both critical components of a resilient cybersecurity strategy.

$612M South Korean Ministry of Science and ICT has allocated over $612 million to strengthen R&D efforts and cybersecurity competitiveness through projects with academia and private firms

(Source: Wilson Center)

Panel Discussion

DEEP DIVE SESSIONS

CYBER (S)HEROES

Breaking Stereotypes, Building Careers

- **Dr. Ohoud Shehail,** Director General, Department of Digital Ajman, UAE
- **Orhan Osmani,** Head, Cybersecurity Division at BDT, International Telecommunication Union (ITU)
- **Jim O'Connor,** Chairman and CEO, United States Telecommunications Training Institute (USTTI)
- **Dr. Almerindo Graziano,** CEO, Cyber Ranges
- **Alexandra Topalian (Moderator),** International Moderator

The 'Cyber (S)heroes: Breaking Stereotypes, Building Careers' panel emphasized the importance of gender diversity in cybersecurity, highlighting the significant underrepresentation of women in the field. Despite increasing demand for skilled professionals, the industry remains overwhelmingly male dominated, with women facing high barriers to entry and challenges in terms of career progression. The discussion addressed how pervasive gender stereotypes often discourage women from pursuing cybersecurity roles and stressed the need for innovative policies to promote women's leadership in the field across both the public and private sectors.

A key insight from the discussion was the impact of cultural perceptions, which tend to frame women primarily as caregivers, making cybersecurity roles — often requiring 24/7 availability — less appealing. Expanded mentorship programs were identified as essential, not only for supporting women already in the field but also for inspiring younger generations to explore cybersecurity careers. Programs offering tuition fee free training and expert mentorship were presented to bridge the current cybersecurity talent gap and provide practical support for women entering the field.

(S)HEROES
Breaking stereotypes, building careers
indo Graziano
Jim O'Connor
Chairman and CEO
Orhan Osmani
Head, Cybersecurity Division at BDT
International Telecommunication Union (ITU)
Dr. Ohoud S
Department of Digital

The panel also discussed initiatives that aim to build capacity among young women, encouraging them to pursue technology careers. Advanced training simulations were highlighted as a tool to create more inclusive environments, allowing women to gain hands-on experience in a supportive setting. The discussion concluded with participants agreeing on the need for collective action across sectors to dismantle barriers and develop sustainable mentorship frameworks, ultimately paving the way for a more inclusive and innovative cybersecurity workforce.

11% of cybersecurity teams have no women at all

(Source: Infosecurity Magazine)

Invite-only Brief

DEEP DIVE SESSIONS

BEYOND CODE

The Institutional Machinery of Cyber Diplomacy

- **Katherine Prizeman,** Political Affairs Officer, United Nations Office for Disarmament Affairs (UNODA)

This session focused on the evolution of cyber diplomacy, particularly examining the work of the UN's Open-Ended Working Group (OEWG) and its role in shaping norms for responsible state behavior in Cyberspace. The discussion explored how international mechanisms, such as the OEWG and the Group of Governmental Experts (GGE), have contributed to developing consensus on key issues like cybersecurity capacity building, confidence building measures, and the applicability of international law in Cyberspace.

The second OEWG (2021-2025), which operates by consensus, has achieved significant milestones. These include the establishment of a global, intergovernmental directory of points of contact (POC), the development of global confidence building measures, and a shared understanding of the cybersecurity threat landscape. Another crucial theme was the ongoing dialogue about how international humanitarian law applies to cyber operations and the responsibilities of states in Cyberspace.

The session concluded by reflecting on the UN's Summit of the Future 2024, with the Global Digital Compact set to introduce a comprehensive global framework for digital cooperation. The compact will foreground the importance of human rights, accountability amongst technology companies, and the promotion of digital public goods, representing a critical step forward for a safer, more equitable future.

In 2024, two major successes were achieved: The POC Directory was officially launched, and the delegations agreed on the basic elements of the mechanism that will follow the OEWG

(Source: Digwatch)

Fireside Chat

DEEP DIVE SESSIONS

CURING THE GAP

Promoting Cybersecurity Solutions for Vulnerable Health Systems

- **Dr. Richard Staynings,** Chief Security Strategist, Cylera and Teaching Professor, University of Denver
- **Alexandra Topalian (Moderator),** International Moderator

The fireside chat, titled 'Curing the Gap: Promoting Cybersecurity Solutions for Vulnerable Health Systems', focused on the crucial need to secure global healthcare systems, particularly in the context of the rise in cyber threats impacting critical infrastructure. Dr. Richard Staynings highlighted how medical devices, healthcare networks, and patient data are increasingly vulnerable to threats like ransomware, which can have dire consequences on patient safety and hospital operations. The conversation underscored the need for effective security controls, including network segmentation and automated security processes driven by AI and machine learning, to protect the resilience of healthcare systems.

A significant challenge addressed during the discussion was the disparity in technology adoption between younger and older healthcare professionals and the overall lack of cybersecurity training across the sector. Dr. Staynings emphasized the importance of continuous testing of security protocols and response plans, as well as adopting a zero-trust approach to protect sensitive medical data. He pointed out that new regulations, such as those from the U.S. Food and Drug Administration (FDA) for medical devices, mirror the evolving landscape of healthcare security. The session concluded with a call for healthcare organizations to prioritize cybersecurity and leverage automation to strengthen their defenses against emerging threats.

30% Statistics for data breaches in healthcare reveal that 30% of all large data breaches occur in hospitals

(Source: Astra)

Panel Discussion

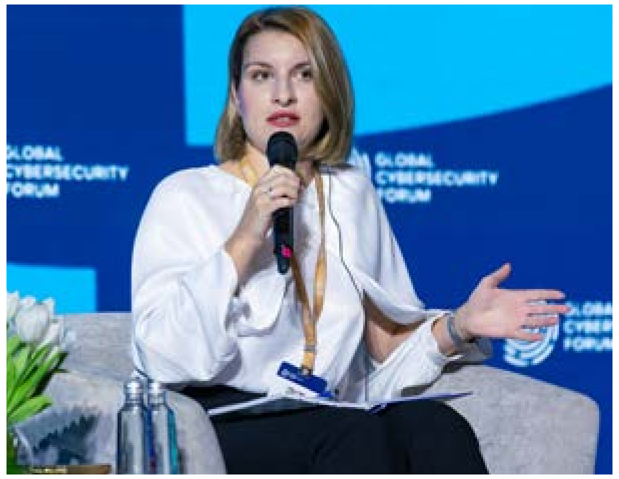
DEEP DIVE SESSIONS

TOWARDS A RESILIENT CYBER FUTURE

Insights on the Global Cyber Workforce Gap and Skills Shortage

- **Abdurahman Al Hassan,** Acting CEO, Global Cybersecurity Forum (GCF)
- **Prof. William H. Dutton,** Martin Fellow, Oxford University's Global Cyber Security Capacity Centre, and Emeritus Professor, University of Southern California
- **Shoaib Yousuf,** Managing Director & Partner, BCG
- **Natasa Perucica,** Lead for Capacity Building, Centre for Cybersecurity, World Economic Forum (WEF)
- **Lara Habib (Moderator),** Senior Presenter, Al Arabiya News

The 'Towards a Resilient Cyber Future: Insights on the Global Cyber Workforce Gap and Skills Shortage' panel discussed the widening gap between the demand for cybersecurity professionals and the industry's capacity to meet this need. This shortage poses a critical risk to cyber resilience globally, as organizations struggle to secure their infrastructures from cyber threats. The session highlighted findings from a comprehensive report jointly produced by GCF and the Boston Consulting Group (BCG), outlining current cybersecurity workforce challenges and actionable strategies to address them. Key topics included the underrepresentation of women in cybersecurity, skill shortages in essential areas like cloud security and leadership, and the role of academia in providing training that aligns with industry needs.



Statistics: The gap between supply and demand is biggest in the Asia-Pacific region, accounting for more than half of the global shortage

(Source: GCF)

The panelists emphasized the pressing issue that the global shortfall of 2.8 million cybersecurity professionals presents, with Asia-Pacific and the Americas facing the most significant regional gaps. Many organizations report that their teams lack critical skills, leaving them vulnerable to increasingly sophisticated cyber threats. The panel called for stronger collaboration between industry and academia to better align education and practical needs, providing future professionals with essential hands-on experience through internships and mentorship programs.

The discussion concluded with a call for collective action to address these challenges. A broader and more diverse talent pool that taps into women's full potential in the sector is essential. Talent retention is also key, with a focus on ensuring continuous development and well-being, alongside appropriate compensation. As cybersecurity becomes more integral to organizational strategy, the need for a skilled and resilient workforce has never been more urgent.

Panel Discussion

DEEP DIVE SESSIONS

CODE, CLICKS, AND CULTURE

Social Transformation in the Technological Age

- **Wael Fattouh,** Chief Advisory Officer, SITE
- **Erik Bertman,** Group CEO, Conscia
- **Daren Smith,** Managing Director, International Government, BAE Systems Digital Intelligence
- **Sauvik Tegta (Moderator),** Partner, Kearney

The panel discussion on 'Code, Clicks, and Culture: Social Transformation in the Technological Age' focused on the profound shifts in society driven by the rapid adoption of emerging technologies. The panelists explored how technological advancements are reshaping social norms and values across different cultures and demographics. A key theme was the potential of technology to foster greater social inclusion. However, the conversation also sought to temper the enthusiasm regarding its positive impacts. While the benefits are evident, the panelists underscored the need to address and manage the downsides of technology that are already manifesting today. They highlighted the importance of establishing ethical and regulatory frameworks to guide technology's integration and development, while preserving diverse cultural identities.

1/3 More than a third of women worldwide have experienced abuse online, and this figure rises to almost 50% for younger women

(Source: SDD)

Overall, the panelists agreed that the key to achieving meaningful social transformation through technology lies not in the technology itself but in people. Success will depend on addressing human-centered challenges rather than technical ones. The panelists were unanimous in emphasizing the importance of interdisciplinary collaboration among technologists, sociologists, and policymakers to ensure that technological innovation drives positive cultural change. The panelists emphasized the importance of training younger generations on embracing emerging technologies which, in turn, will enable inclusive and sustainable development at the societal level. In this context, the session also highlighted the growing need for public-private partnerships to effectively guide and manage the cultural transformation spurred by rapid advancements in technology.

Invite-only Breakfast

DEEP DIVE SESSIONS

CYBER LEADERSHIP LAUNCHPAD

Launch of the 'Cyber Leadership Launchpad' Global Mentoring Program

- **Doreen Bogdan-Martin,** Secretary-General, International Telecommunication Union (ITU)
- **Heidi Crebo-Rediker,** Senior Fellow, Council on Foreign Relations
- **Joy Chik,** President, Identity and Network Access, Microsoft
- **Silvana Koch-Mehrin,** Founder and President, Women Political Leaders (WPL)
- **Rebecca McLaughlin-Eastham (Moderator),** Independent TV Anchor & Media Trainer

Day 2 of the Annual Meeting 2024 began with a networking breakfast to announce the launch of GCF's 'Cyber Leadership Launchpad' mentoring program, which represents a significant step forward in global efforts to increase women's representation and leadership in cybersecurity. The session highlighted the urgent need for a more inclusive workforce in the sector, noting that current representation remains notably low compared to other technological fields. The discussion stressed the value of diverse perspectives in cybersecurity, emphasizing that equitable, gender diverse teams are essential for effective problem-solving.

The key themes of the discussion included the collaborative role of international organizations in building supportive environments for women in cybersecurity, as well as the need for visible role models to inspire future generations. The panel also addressed the challenges of the "leaky pipeline" of talent and called for more inclusive workplace cultures to ensure women are retained in the field.

The dialogue went on to highlight the best practices for cultivating environments that support advancements in women's careers. The speakers identified mentorship and sponsorship programs as essential for promoting women into leadership roles within the sector. Insights shared during the session underscored the need for a strong commitment to empowering women to drive lasting change in the cybersecurity sector.

<1% Fewer than 1% of women cybersecurity professionals hold executive positions within organizations

(Source: US Cybersecurity Magazine)

Panel Discussion

DEEP DIVE SESSIONS

FORTIFYING THE FIELD

Securing Operational Technology in the Oil Industry in a Hyperconnected World

- **Phil Tonkin,** Field CTO, Dragos
- **Salem S. Al-Elwi,** Manager, OT Cybersecurity, Aramco
- **Filipe Beato,** Lead, Centre for Cybersecurity, World Economic Forum (WEF)
- **Lara Habib (Moderator),** Senior Presenter, Al Arabiya News

The panel discussion on 'Fortifying the Field: Securing Operational Technology in the Oil Industry in a Hyperconnected World' focused on the significant cybersecurity challenges facing the oil sector as it increasingly adopts operational technologies (OT). While the convergence of OT and IT systems has driven efficiency and innovation, it has also exposed critical infrastructure to heightened cyber risks. With incidents like the Colonial Pipeline attack highlighting the scale of potential damage, panelists discussed the urgent need for tailored cybersecurity strategies to protect the sector.

The session underscored the diverse range of threat actors, from state-sponsored entities to criminal organizations, targeting the oil industry's OT systems. Panelists highlighted that as these systems become more interconnected and rely on intricate supply chains, the potential points of vulnerability increase, making them more exposed to cyberattacks. As a result, organizations face greater risks in terms of disruptions to vital operations. This is particularly true in the case of emerging technologies like artificial intelligence (AI) and automation, which are both enhancing operational capabilities and introducing new vulnerabilities, making it easier for adversaries to exploit gaps in security.

The panel asserted that addressing these challenges requires a collective effort. Enhanced collaboration within the industry, investment in advanced security solutions, and the development of clear, industry-specific guidelines were identified as essential measures to fortify OT systems. Panelists stressed the need for a shift away from traditional security approaches toward more adaptive, tailored cybersecurity strategies that can better defend against the evolving threat landscape in this critical sector.

91% of oil and gas professionals believe cybersecurity is a prerequisite for the digital transformation initiatives that are making the future of the energy industry possible

(Source: World Oil)

Panel Discussion

DEEP DIVE SESSIONS

HACKING TRUST

Cybercrime's Role in Transforming Social Norms

- **Dr. Abdulaziz Almaslukh,** Senior RDI Executive, SITE
- **Anand Kashyap,** CEO & Co-Founder, Fortanix
- **Dr. Moataz Bin Ali,** Regional Vice President and Managing Director, MMEA, Trend Micro
- **Alexandra Topalian (Moderator),** International Moderator

The panel discussion, 'Hacking Trust: Cybercrime's Role in Transforming Social Norms', examined the profound impact of cybercrime on social trust in today's hyperconnected world. Panelists discussed how advancements in technology, particularly artificial intelligence (AI), have not only amplified the scale and sophistication of cyberattacks but also eroded public trust in interactions, privacy, and security in Cyberspace. The increasing prevalence of AI-driven attacks, such as deepfakes and real-time phishing, has created a new layer of complexity, challenging consumers' ability to discern between legitimate and malicious activity online.

A key insight from the discussion was the shift in societal behavior as individuals and businesses grow increasingly cautious in their interactions with Cyberspace. Trust has become a critical factor, with users becoming more wary of sharing personal information and businesses adopting more stringent security measures, such as zero-trust frameworks. Panelists stressed the importance of a multi-layered approach to combating these threats, which includes technological innovation, robust regulation, and widespread digital literacy.

Looking ahead, the panel underscored the need for collaborative efforts between governments, businesses, and cybersecurity vendors to develop policies that ensure privacy, accountability, and transparency in the cyber age. Education was highlighted as a cornerstone in fostering awareness and resilience against cyber threats, alongside the development of AI-driven security tools to counteract increasingly sophisticated attacks. The session concluded by emphasizing the need for joint efforts to restore trust in digital platforms to ensure a secure future for interactions in Cyberspace.

$900M Projections suggest that cybercrime groups earned more than $900 million from extortion in 2023, a year-on-year increase of 80%

(Source: Station X)

Panel Discussion

DEEP DIVE SESSIONS

REDUCING CYBER CARBON FOOTPRINT

Making Cybersecurity Sustainable

- **Dr Manar Alohaly,** Senior RDI Executive, SITE
- **Dr. Antonio J. Jara,** CSO, Libelium
- **Jay Bhatnagar (Moderator),** Principal, BCG

This session addressed the intersection between cybersecurity and environmental sustainability, highlighting how organizations can reduce their cyber carbon footprint. The discussion was centered around the key challenges and opportunities in this area, focusing on the increasing energy demands driven by modern technologies, such as 5G, and the critical importance of cooling systems in data centers.

Panelists explored the role of sustainable technologies, noting that organizations often face difficulties in finding the expertise needed to integrate sustainability into cybersecurity effectively. They emphasized the importance of collaboration between international organizations to achieve economies of scale in sustainability efforts. Furthermore, the conversation underscored that reducing energy consumption and carbon emissions does not need to compromise cybersecurity. Instead, sustainable practices and secure operations must evolve together, ensuring that both goals are pursued simultaneously.

The session concluded with a call to action for collective efforts and continued innovation, as well as the development of global frameworks to drive sustainable cybersecurity practices across sectors and industries.

50% Resilience activities and endpoints requested by cybersecurity account for almost 50% of cyber emissions

(Source: Station X)

OTC CoE ACTIVATION

OTC CENTER OF EXCELLENCE

The GCF Annual Meeting 2024 marked a significant milestone with the formal activation of the Operational Technology Cybersecurity Center of Excellence (OTC CoE). Jointly launched by GCF and Aramco at last year's Annual Meeting, in collaboration with NEOM, SITE, Sabic, Honeywell, and Schneider Electric, the Center is designed as a global platform for knowledge sharing and multistakeholder collaboration to address the increasingly complex cybersecurity challenges related to Operational Technology (OT). This year's session focused on transitioning from planning to execution, emphasizing how the Center will begin tackling the cybersecurity risks associated with OT systems across multiple sectors.

The activation phase marks a pivotal step in turning strategy into actionable programs, with the Center focused on uniting diverse stakeholders to strengthen the global OT cybersecurity ecosystem. As OT and IT systems converge and cyber threats grow more sophisticated, the need for a coordinated, collective response has never been greater. Bringing together global thought leaders and industry pioneers, the OTC CoE aims to catalyze collaboration across the entire OT cybersecurity value chain and advance the maturity of global OT cybersecurity through capability development, standardization and policy advocacy, research and innovation, awareness raising, and thought leadership generation.

One of the key achievements highlighted during the session was the detailed governance model for the Center's operations. The Center will undergo the activation phase from 2024 to 2026, during which it will be jointly managed by its founding members, with Aramco playing a pivotal role. This phase will focus on refining the Center's structure, membership model, and key activities. From 2027 onwards, the OTC CoE will transition to independent operations with its own full-time staff, governance structures, and member-driven initiatives.

At the core of the session was the importance of capability development in OT cybersecurity. The Center's capability development initiatives will focus on training programs designed to upskill the cybersecurity workforce, especially in OT environments. These efforts will involve academic partnerships and tailored programs to address the critical shortage of skilled professionals in this domain. Aramco's leadership in this initiative has already laid the groundwork for workforce development programs, including collaborations with universities and national institutions to create OT-specific training courses that prepare future professionals for the unique cybersecurity challenges of OT systems.

By fostering partnerships between industry leaders, governmental bodies, and academia, the OTC CoE is creating a collaborative framework for addressing cybersecurity challenges. The Center's roundtables and working groups provide a platform for key stakeholders to exchange insights, best practices, and innovative solutions. This collaborative approach ensures that the global OT cybersecurity ecosystem benefits from a broad range of expertise and perspectives.

As the OTC CoE transitions from the strategy phase to operational execution, the Center's partners have a clear focus on building capacity, driving innovation, and promoting collaboration to address global OT cybersecurity challenges. Under the leadership of Aramco and GCF, along with the contributions of diverse stakeholders, the OTC CoE will serve as a central hub for advancing cybersecurity resilience across OT systems worldwide to ensure that critical infrastructures around the world are better secured against evolving threats.

KNOWLEDGE COMMUNITY MEETING

FUTURE OF CYBERSECURITY

By harnessing diverse expertise and forecasting capabilities, this Knowledge Community brings together over 25 organizations to navigate the transformations driven by emerging technologies and foster sustainable cyber resilience. During the meeting, members reflected on their recent achievements and charted the path forward for the year ahead, establishing key priorities and outlining a strategic action plan to guide future efforts.

In conjunction with the Annual Meeting, the 'Future of Cybersecurity' Knowledge Community, led by SITE, unveiled a whitepaper titled "Navigating GenAI's Threats and Opportunities in Cybersecurity." The paper offers a strategic roadmap to help organizations address emerging risks while capitalizing on the opportunities presented by GenAI. It includes real-world case studies showcasing how global entities can leverage GenAI to enhance their cybersecurity. The whitepaper highlights three key themes, crucial for organizations seeking to balance the opportunities and risks associated with GenAI in today's cybersecurity landscape:

Adopting GenAI for cybersecurity readiness: GenAI is transforming cybersecurity, with 93% of organizations adopting it to some extent. However, over half have yet to fully integrate it into their cybersecurity strategies, which exposes their infrastructure to vulnerabilities. GenAI can enhance threat detection and intelligence, so comprehensive adoption is essential to unlock its full potential and effectively mitigate risks.

Addressing the double-edged sword of GenAI: While GenAI has the ability to strengthen cybersecurity, it simultaneously introduces new risks. Cybercriminals now leverage AI to conduct phishing campaigns, create deepfakes, and program advanced malware. With 45% of organizations concerned about AI-driven attacks, addressing these threats through proactive strategies is critical for overall cybersecurity resilience.

Strengthening resilience through AI governance and secure integration: To fully leverage GenAI's potential while mitigating associated risks, organizations must implement robust AI governance frameworks, secure data management practices, and advance vulnerability detection mechanisms. At the same time, embedding security into the development process for GenAI and prioritizing data privacy are essential steps to navigate its challenges and opportunities effectively.

KNOWLEDGE COMMUNITY MEETING

SECURING INDUSTRIAL SYSTEMS FOR GLOBAL ENERGY SUPPLY

With an aim to fortify the infrastructure that supports global energy supply, this community brings together over 20 international stakeholders to collaborate and work towards ensuring a resilient and secure energy future for all. During this meeting, the community discussed their achievements in recent months and set the course for the upcoming year by establishing key priorities and outlining an action plan to drive their mission forward.

In conjunction with the Annual Meeting, the 'Securing Industrial Systems for Global Energy Supply' Knowledge Community, led by Aramco, released a whitepaper titled "Safeguarding Critical Infrastructure by Evolving Monitoring and Response Capabilities." The paper explores the pressing need for a comprehensive approach to protect complex industrial systems and ensure the resilience of critical infrastructure. It highlights three key areas where organizations can direct their efforts in strengthening their defenses and enhancing resilience against the ever-evolving landscape of cyber threats to operational technology (OT):

Mitigating vulnerabilities in IT-OT convergence: The integration of IT and OT systems has improved operational efficiency, while simultaneously expanding the attack surface and exposing OT environments to new cyber threats. This demands comprehensive governance frameworks to unify cybersecurity strategies across both domains.

Managing supply chain risks and vendor oversight: Dependence on third-party vendors with inconsistent security practices introduces significant risks to OT systems. Enforcing stricter cybersecurity measures in contracts and actively monitoring vendor activities are essential to protect critical infrastructure.

Closing the OT cybersecurity skills gap: A shortage of skilled professionals hinders effective monitoring and incident response. Addressing this gap requires investing in talent development and specialized training, while fostering industry collaboration to build robust defenses.

KNOWLEDGE COMMUNITY MEETING

SAFEGUARDING THE FUTURE NETWORKS & EMERGING TECHNOLOGIES

Networks are the backbone of our interconnected world. This community is dedicated to promoting and safeguarding the networks of the future, such as 6G, and harnessing their capabilities for the benefit of society. During this meeting, the community discussed their achievements over the past few months and set the course for the upcoming year, establishing key priorities and outlining an action plan to drive their collaborative efforts forward.

In conjunction with the Annual Meeting, the 'Safeguarding the Future Networks & Emerging Technologies' Knowledge Community, led by stc, released a whitepaper titled, "Silencing the Voice Imposters: Tackling CLI Spoofing in an Interconnected World." This report provides a solutions-focused analysis of Caller Line Identification (CLI) spoofing, detailing its underlying mechanisms, attack techniques, and impacts. The whitepaper outlined three essential findings that telecom operators need to take into account to protect networks and enhance resilience against the growing threat of CLI spoofing:

Mitigating CLI spoofing to protect networks: Addressing the rising threat of CLI spoofing, especially in outbound roamer calls, is critical. Fraudsters manipulate caller IDs to impersonate trusted entities, compromising network security and causing financial and reputational damage. Telecom operators must adopt stronger defenses to combat this growing threat.

Deploying advanced detection and security measures: Implementing AI-powered fraud detection, real-time monitoring, and robust security protocols is essential for preventing Voice over Internet Protocol (VoIP) based spoofing attacks. These proactive measures can detect and stop spoofing attempts before they impact critical telecom infrastructure.

Enhancing industry collaboration and compliance: Stronger cooperation between telecom operators, regulators, and technology providers, through sharing intelligence and adopting standards like SHAKEN/STIR, is crucial. This coordinated approach will ensure accurate caller identity verification, reduce fraud, and bolster customer trust and network security.

SHAPING THE GLOBAL CONVERSATION

KEY TAKEAWAYS

In alignment with this year's Annual Meeting theme, "Advancing Collective Action in Cyberspace," a number of strategic imperatives for collective action emerged from two days of in-depth discussions. In addition to the insights generated by each session, summarized in this book, the Annual Meeting 2024 identified five cross-cutting imperatives that are critical to shaping a secure future through effective cybersecurity. As an action-oriented platform, empowered by its community and partners, GCF will continue to advance targeted initiatives, knowledge creation, and collaborative projects that aim to address these imperatives and drive meaningful change.

IMPERATIVE #1

HARNESSING THE POWER OF COLLABORATION

In an increasingly interconnected world, cyber threats transcend national borders. Data breaches increased by 20% from 2022 to 2023, and state-sponsored actors and criminal networks are capitalizing on emerging vulnerabilities, requiring a response that goes beyond the traditional frameworks of multilateralism. The international community recognizes the need to embrace a new and more comprehensive style of collaboration – a polylateral approach that fosters engagement between governments, private companies, civil society, and international organizations – to address the growing complexities of modern cybersecurity challenges.

Across numerous sessions, speakers highlighted the growing inadequacy of traditional multilateral frameworks in addressing the rapidly changing cyber threat landscape. Panelists emphasized that maximizing the social and economic benefits of Cyberspace, while addressing the scale and sophistication of today's cyberattacks, requires a fundamental shift in how the international community collaborates. State-centric diplomacy, although essential, cannot fully address the complex challenges and opportunities presented by Cyberspace, and a polylateral approach is needed to build security frameworks that are flexible, resilient, and enablers of prosperity. By leveraging the expertise of multiple, international stakeholders, this model will enable faster, more coordinated responses to emerging risks that will strengthen trust in the global cybersecurity ecosystem.

A key theme that emerged was the need for enhanced coordination between governments and the private sector to support information sharing and threat detection that mitigates the impact of breaches and strengthens defense mechanisms across sectors. As technology companies and cybersecurity firms develop advanced solutions, they have a key role to play in safeguarding critical sectors and infrastructure. The Annual Meeting also highlighted the fact that public-private partnerships can aid in standardizing best practices, ensuring accountability, and fostering trust in increasingly interconnected environments.

Successfully combating the rising tide of cyber threats, particularly those targeting critical infrastructure and supply chains, requires the international community to adopt a polylateral approach that integrates expertise from all sectors. This collaboration will enable more effective, comprehensive, and timely responses to rising cyber threats on critical infrastructure.

IMPERATIVE #2

INNOVATING TO ACCELERATE THE DEVELOPMENT OF THE CYBER WORKFORCE

The shortage of skilled cybersecurity professionals is one of the most pressing challenges facing both the public and private sectors today. As identified in the *"2024 Cybersecurity Workforce Report"* – a new report from GCF and BCG – the global shortfall of cybersecurity professionals has reached 2.8 million and only 72% of cybersecurity roles are filled, leaving organizations vulnerable to increasingly sophisticated cyber threats. Discussions at the Annual Meeting underscored the urgency of addressing this talent gap through comprehensive, multi-disciplinary approaches that go beyond traditional technical education.

As the cybersecurity landscape evolves, the demand is growing for professionals skilled not only in technical areas – such as cloud security and AI-driven threat detection – but also in leadership, psychology, and law. The convergence of cybersecurity and business acumen is particularly essential, yet difficult to find among the existing cadre of professionals, and 50% of organizations identify effective cybersecurity leadership as their top challenge now and in five years. The Annual Meeting emphasized the importance of aligning cybersecurity training with real-world challenges, promoting cross-sector collaboration, and developing curricula that reflect the complex nature of modern cyber threats.

A critical area of focus at the Annual Meeting was the underrepresentation of women in cybersecurity, who currently account for only 24% of the workforce. Panelists called for increased mentorship programs, career development initiatives, and collaborative efforts to promote diversity. Echoing the key aims of the Women Empowerment in Cybersecurity (WEC) global initiative overseen by GCF, they stressed that fostering a more inclusive workforce is essential not only to fill talent gaps but also to drive innovation and resilience across the sector.

This year's Annual Meeting highlighted the need for robust retention strategies to ensure the long-term sustainability of the cybersecurity workforce. These strategies should encompass continuous professional development, support for mental well-being, and the adoption of flexible work environments. Governments, industry leaders, and global stakeholders must collaborate to cultivate a talent pipeline capable of meeting future cybersecurity challenges. This includes fostering partnerships with universities, creating internship opportunities, and establishing clear career pathways.

Cybersecurity is more than a technical function; it is a strategic imperative requiring a diverse, and skilled workforce. By nurturing talent, building inclusive environments, and aligning efforts across sectors, we can ensure a secure and resilient cyber future.

IMPERATIVE #3

SAFEGUARDING THE FUTURE OF OUR CHILDREN IN CYBERSPACE

The increasing use of technology has exposed children to unprecedented cyber risks, making their protection in Cyberspace a critical priority. According to GCF's *"Why Children are Unsafe in Cyberspace"* report, 72% of children globally have experienced at least one cyber threat – a statistic that could escalate significantly with the rise of artificial intelligence (AI) and other emerging technologies. Cybercriminals are already leveraging these advanced tools to engage in grooming, harassment, and exploitation, creating increasingly complex threats that demand urgent and coordinated action.

Throughout the Annual Meeting, discussions emphasized the growing vulnerability of children in Cyberspace, as emerging technologies and tools are increasingly used to deceive and target young users. Panelists stressed that traditional safety measures are insufficient, calling for real-time threat detection, AI-driven security solutions, and strengthened law enforcement collaboration to counter these threats effectively. Another issue highlighted was the need to adopt a safety-by-design approach to child protection in Cyberspace, embedding safeguards from the outset across technology platforms to proactively mitigate risks and ensure a secure environment for younger users in Cyberspace.

This year also saw the first ever Child Protection in Cyberspace (CPC) Global Summit take place, held in collaboration with the International Telecommunication Union (ITU), UNICEF, DQ Institute, and WeProtect Global Alliance, to drive collective action towards ensuring that children are safe in Cyberspace. The focus was on fostering international cooperation, exploring innovative frameworks to address cyber risks, and ensuring child protection remains a priority in global decision-making.

As cyber threats continue to evolve, discussions at the Annual Meeting and the CPC Global Summit underscored the need for multistakeholder collaboration and real-time intelligence sharing. In line with the objectives of the Child Protection in Cyberspace (CPC) global initiative overseen by GCF, these efforts aim to build a safer cyber environment for the next generation, ensuring children are protected from exploitation in an increasingly interconnected world.

IMPERATIVE #4

CREATING SUSTAINABLE AI ADVANTAGE FOR CYBERSPACE

The rapid advancement of AI technologies, particularly generative AI and automation, presents both transformative opportunities and critical challenges for cybersecurity. AI-powered tools enable real-time threat detection, predictive analysis, and faster incident response, revolutionizing how organizations defend against threats. However, the same technologies empower cybercriminals, facilitating phishing campaigns, deepfakes, and automated malware at an unprecedented scale and speed. A recent Darktrace report revealed that 60% of respondents fear their organizations are unprepared to counter AI-driven threats, underscoring the urgency of integrating AI-powered solutions into cybersecurity strategies.

Panelists at the GCF Annual Meeting 2024 stressed the need for organizations to embed AI into cybersecurity frameworks proactively, enhancing zero-trust models and continuous monitoring. Yet, these technical measures alone are not enough. Global stakeholders including governments, the private sector, academia, and international bodies must address the regulatory complexities around AI, such as ensuring data privacy, accountability, and mitigating cyber threats. In particular, governments have an imperative to collaborate in building unified ethical frameworks that govern both the offensive and defensive use of AI. This cooperation and collective action should extend beyond national borders to promote transparency, facilitate knowledge-sharing, and safeguard against AI's potential misuse in Cyberspace.

Looking ahead, AI's role in cybersecurity will become even more significant. Its successful integration requires proactive strategies that foster adaptive defenses capable of evolving alongside emerging threats. However, while AI offers a transformative potential to revolutionize cyber defense, it also introduces new risks. According to the *"2024 Cybersecurity Workforce Report"*, 58% of cybersecurity leaders express concern over new adversarial techniques and AI-enabled cyberattacks. The key lies in striking a balance – leveraging innovations in AI to bolster defenses while ensuring robust governance frameworks to mitigate the risks of unchecked deployment. This delicate equilibrium will be crucial to creating a future where AI not only enhances security but drives sustainable, resilient cyber innovation.

IMPERATIVE #5

DECODING HUMAN BEHAVIOR TO PROTECT PEOPLE AND DISRUPT CRIME

The intersection of human behavior and technology plays a pivotal role in today's cybersecurity landscape. Cybercriminals exploit psychological biases and cognitive vulnerabilities, making cybercrime more than a technical challenge – it's a behavioral one. For instance, over 90% of cyberattacks in 2023 relied on social engineering tactics, highlighting the critical role human behavior plays in cybersecurity breaches. At the Annual Meeting, discussions underscored the importance of decoding cyberpsychology to better understand the motivations of attackers and protect users from manipulation.

Panelists emphasized that building psychological defenses is as crucial as deploying technological safeguards. The discussions highlighted that individual mental preparedness, especially in high-pressure incident response teams, can determine the success of cybersecurity efforts. Furthermore, experts delved into how organized cybercriminal networks mimic legitimate business operations, using tactics such as reconnaissance, malware deployment, and ransomware to exploit cognitive blind spots.

The rise of generative AI technologies has added new layers of complexity, making it easier to create deepfakes and phishing schemes that deceive users by manipulating trust and perception. Experts agreed that future cybersecurity strategies must blend behavioral insights with advanced technologies to predict, detect, and mitigate these emerging threats effectively.

This holistic approach to cybersecurity – combining human and technological defenses – will be essential to protect both individuals and organizations. GCF's *"Introduction to Cyberpsychology"* Briefing Paper, authored by cyberspsychology expert, Dr. Mary Aiken, underscores the need to understand the minds of both attackers and users to create resilient systems that preempt manipulation and ensure safer interactions in Cyberspace.

IMPERATIVE #6

SECURING CRITICAL INFRASTRUCTURE FOR A RESILIENT FUTURE

Critical infrastructure systems – especially in key sectors such as energy, healthcare, and telecommunications – are increasingly vulnerable to cyberattacks. While the integration of emerging technologies within these systems is enabling operational efficiency, they have also significantly expanded the attack surface, raising the stakes for cybersecurity. In 2023, there was a 30% surge in cyberattacks targeting critical infrastructure, highlighting the growing focus of attackers on these essential assets.

Discussions at the GCF Annual Meeting 2024 underscored the pressing need to strengthen the cybersecurity of critical infrastructure. Incidents such as the Colonial Pipeline ransomware attack, which resulted in the temporary shutdown of one of the United States' largest fuel pipelines, highlight the catastrophic ripple effects that cyberattacks on OT systems can have – not only disrupting the economy by halting fuel distribution, but also threatening public safety and undermining societal trust in essential services.

Traditional cybersecurity approaches, primarily focused on IT, are no longer sufficient to protect OT environments. A fundamental shift is required to embrace adaptable defense mechanisms, which maximize the potential of emerging technologies and implement zero-trust frameworks tailored specifically to OT systems. Experts at the Annual Meeting emphasized the importance of industry-specific threat intelligence, real-time monitoring, and collaboration between the public and private sectors to mitigate the evolving risks facing critical sectors and infrastructure.

Throughout the Annual Meeting, participants stressed that the urgent need for global collaboration has never been greater. At a time when cyberattacks on critical infrastructure can destabilize economies and endanger lives, collective action is the only viable path forward, and governments, industry stakeholders, and academic institutions must forge stronger alliances to share real-time threat intelligence and best practices. It is also essential for these stakeholders to come together to develop robust, forward-thinking cybersecurity strategies that not only counter immediate threats but also anticipate and mitigate future risks to our most vital systems.

REACHING A WIDER AUDIENCE GLOBALLY

GCF established several strategic media partnerships, engaged extensively with local, regional, international, and trade publications, and delivered a dynamic social media campaign before, during, and following the GCF Annual Meeting 2024 - ultimately amplifying the conversation and announcements made on-ground to reach a wider global audience.

MEDIA COVERAGE - KEY FIGURES

LIVE STUDIO

67
Interviews

40
News platforms reached

MOMENTS OF GENIUS

3.6M
Impressions

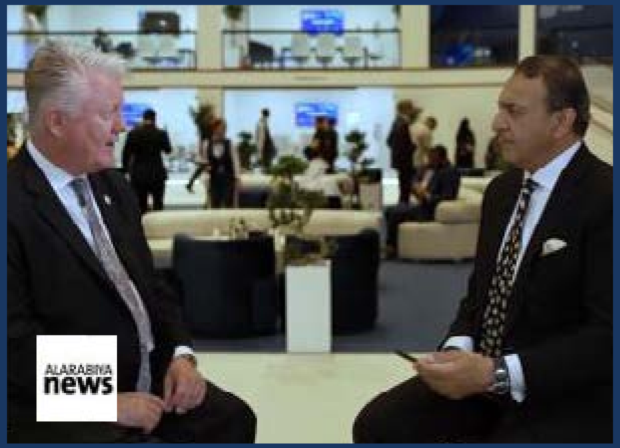
21K
Hours of watch time

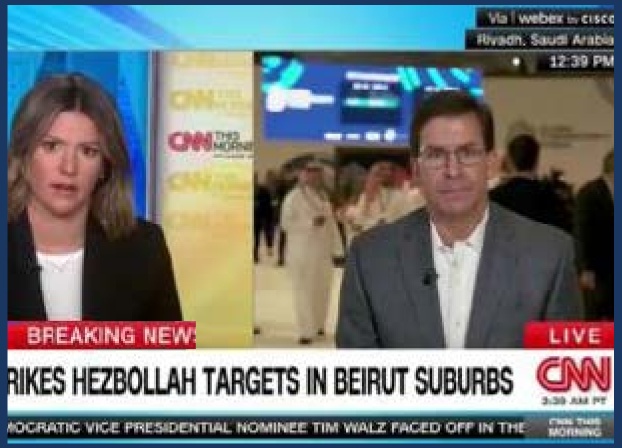
EARNED COVERAGE

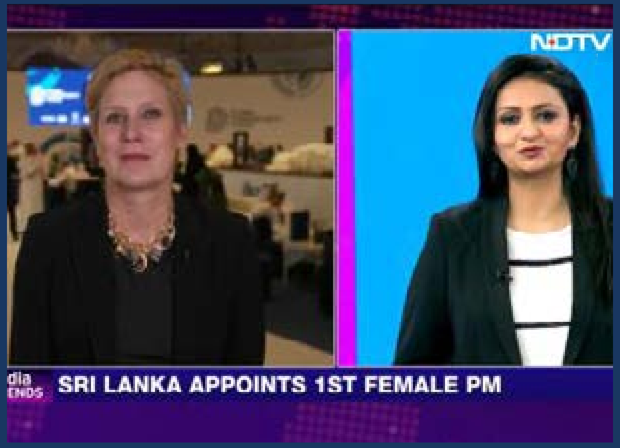
542M
Total reach

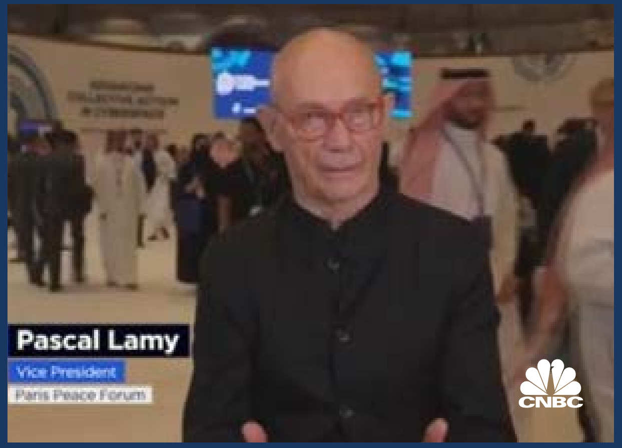
533
Mentions in regional and international press

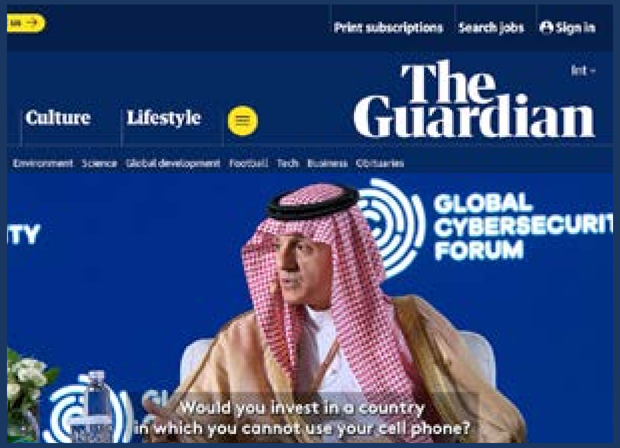
Between Monday September 30th, 2024 - Sunday 6th October, 2024

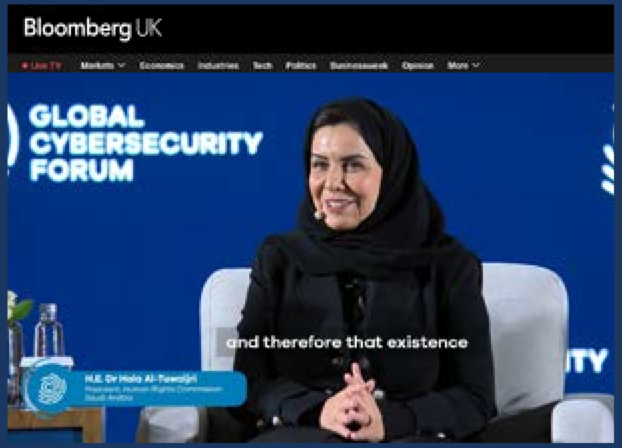


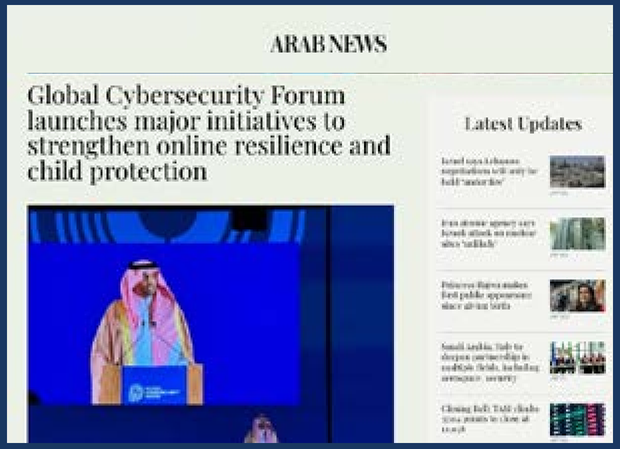

Via webex by cisco
Riyadh, Saudi Arabia
12:39 PM
BREAKING NEWS
LIVE
RIKES HEZBOLLAH TARGETS IN BEIRUT SUBURBS
CNN
MOCRATIC VICE PRESIDENTIAL NOMINEE TIM WALZ FACED OFF IN THE





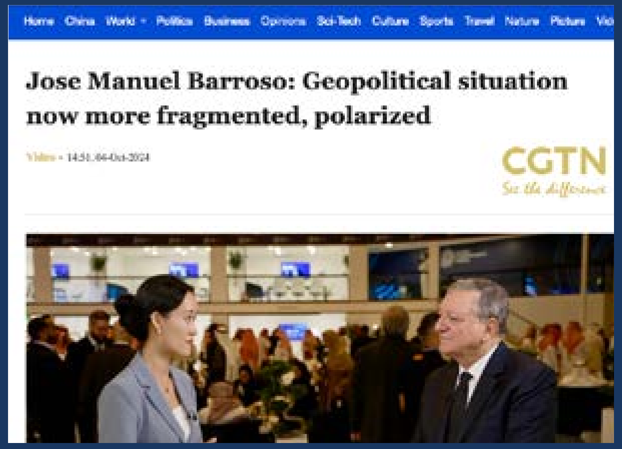

Print subscriptions
Search jobs
Sign in
The Guardian
Culture
Lifestyle
GLOBAL CYBERSECURITY FORUM
Would you invest in a country in which you cannot use your cell phone?




ARAB NEWS

Global Cybersecurity Forum launches major initiatives to strengthen online resilience and child protection

Latest Updates


Home China World Politics Business Opinions Sci-Tech Culture Sports Travel Nature Picture Video

Jose Manuel Barroso: Geopolitical situation now more fragmented, polarized

Video • 14:51, 04-Oct-2024

MEDIA OUTREACH & IMPACTS

GCF 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.

KEY FIGURES

67 Interviews booked in the GCF Live Studio

40 Individual news platforms reached

23 Speakers interviewed

MEDIA OUTLETS

CNN · CNBC · CNBC AFRICA · CGTN AFRICA · sky news · REUTERS · NDTV · news 24

GCF Live Studio Coverage

BUSINESS LIVE GLOBAL CYBERSECURITY FORUM HELD IN RIY
Joining us now in the Cipher Brief studio is former Secretary of Defense Mark Esper. Mr.
DR. MARY AIKEN
CYBER PSYCHOLOGIST
GLOBAL BUSINESS TODAY
INCLUSIVE CYBER POLICIES: THE ROLE OF WOMEN IN DECISION-MAKING
Pascal Lamy
P DOWNPLAYS U.S. TROOP BRAIN INJURIES ON HIS WATCH
Esper | Former Trump Defense Secretary
India ASCENDS
IS EUROPE RAMPING UP DEFENCE EFFORTS AMID GLOBAL CONFLICTS?
Global Cybersecurity Forum Annual Meetin
RI LANKA APPOINTS 1ST FEMALE PM
Experts address AI, global security threats, solutions to cybercrimes
VOWS IRAN "WILL PAY" FOR UNPRECEDENTED MISSILE ATTACK
Yeah, and now it's a scary environment because we're putting voluntarily so much
CIPHER
L STRIKES HEZBOLLAH TARGETS IN BEIRUT SUBURBS

MOMENTS OF GENIUS

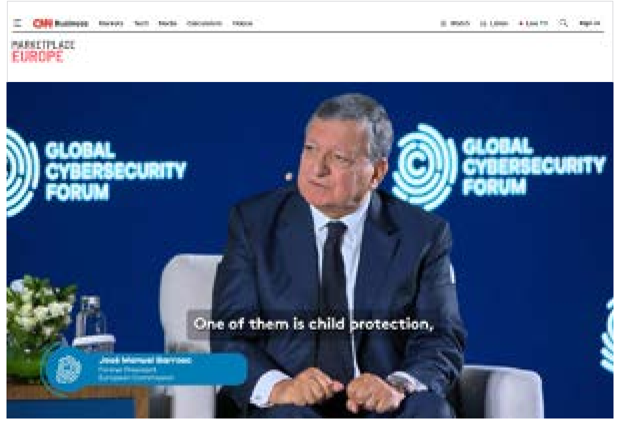
GCF's 'Moments of Genius' campaign captured impactful 30-60 second soundbites from a selection of high-level experts and decision-makers participating in the Annual Meeting 2024, each showcasing thought leadership. These Moments of Genius were distributed along with GCF branding across hundreds of Tier 1 news outlets over a four-week period, bringing GCF and the insights shared during the Annual Meeting to a global audience.

KEY FIGURES

300+	Outlets distributed across
3.6M	Total impressions
1.6M	Total video views
21K	Total hours viewed

MEDIA OUTLETS

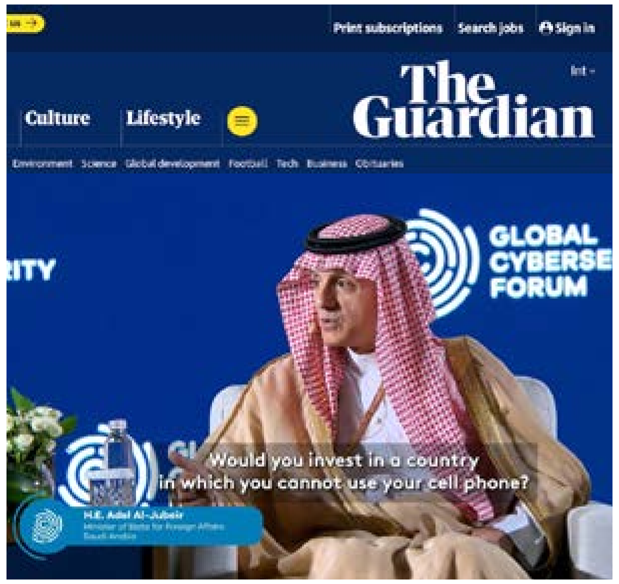
- The Telegraph
- Le Monde.fr
- Frankfurter Allgemeine
- abc NEWS
- ESTADÃO
- Chicago Tribune
- GIANTSWIRE
- GULF NEWS
- Gulf Today
- HUFFPOST
- Investing.com
- Khaleej Times
- FORTUNE
- The Economic Times
- the japan times
- THE TIMES OF INDIA
- THE STRAITS TIMES
- The INDEPENDENT
- SPIEGEL ONLINE
- sueddeutsche.de
- DER TAGESSPIEGEL
- The New York Times
- THE NEW YORKER
- MarketWatch
- THE TIMES
- Newsweek
- The Guardian
- The National
- 讀賣新聞
- USA TODAY
- THE VERGE
- The Atlantic
- NBT नवभारत टाइम्स
- POLITICO
- VentureBeat
- WeLT
- WIRED
- yahoo!
- yahoo! finance
- REUTERS
- BUSINESS INSIDER
- msn
- NBC NEWS
- MIT Technology Review
- TIME
- WSJ
- NTV
- Inc.
- CNBC
- FOX BUSINESS
- KYODO
- FOCUS
- WeLT
- FOX NEWS radio
- Forbes
- 연합뉴스
- Vox
- CNN عربي
- CNN
- CNN
- AOL
- CBC news
- CBS NEWS
- AP
- Investing.com
- ET
- THE HILL
- Science Times
- FOX NEWS channel
- FRANCE 24
- NDTV
- The Economist
- LE FIGARO
- asia one
- USA TODAY


CNN Business

MARKETPLACE EUROPE

One of them is child protection,

José Manuel Barroso


Print subscriptions Search jobs Sign in

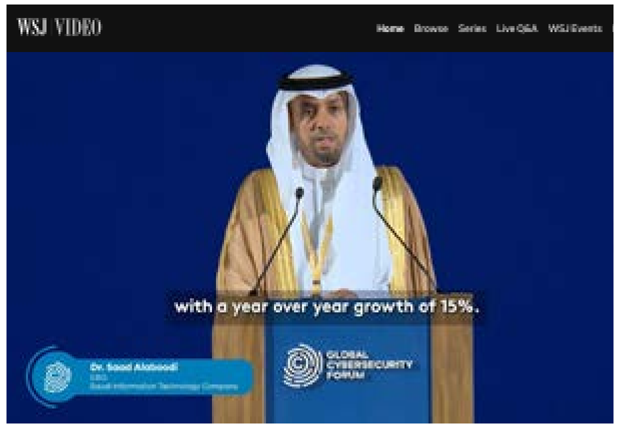
Culture Lifestyle

The Guardian

Environment Science Global development Football Tech Business Obituaries

Would you invest in a country in which you cannot use your cell phone?

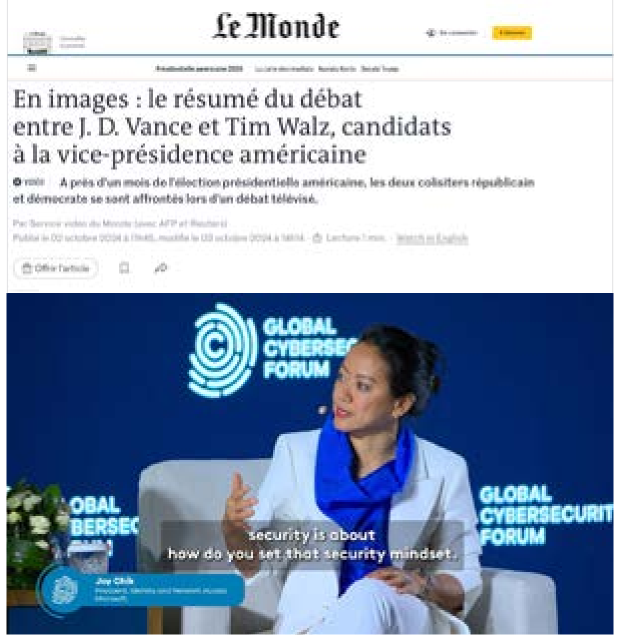
H.E. Adel Al-Jubeir


WSJ VIDEO

Home Browse Series Live Q&A WSJ Events

with a year over year growth of 15%.

Dr. Saad Alaboodi


Le Monde

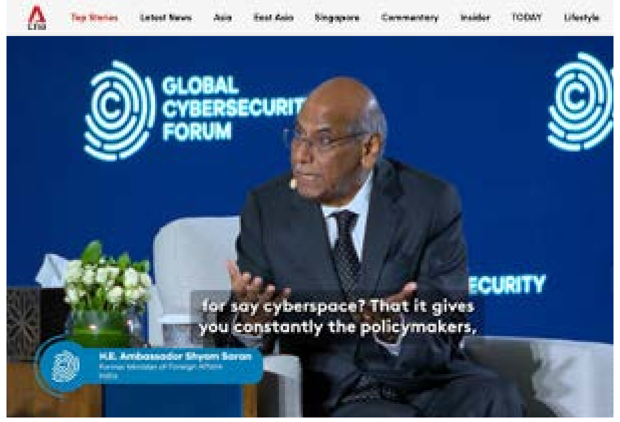
En images : le résumé du débat entre J. D. Vance et Tim Walz, candidats à la vice-présidence américaine

VIDEO A près d'un mois de l'élection présidentielle américaine, les deux colistiers républicain et démocrate se sont affrontés lors d'un débat télévisé.

Offrir l'article

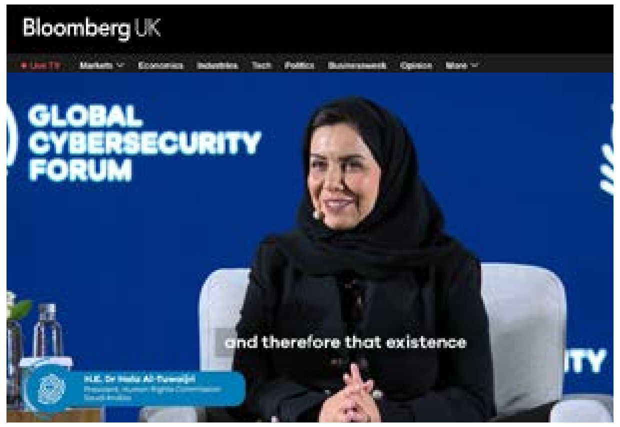
security is about how do you set that security mindset.

Joy Chik


Top Stories Latest News Asia East Asia Singapore Commentary Insider TODAY Lifestyle

for say cyberspace? That it gives you constantly the policymakers,

H.E. Ambassador Shyam Saran


Bloomberg UK

Live TV Markets Economics Industries Tech Politics Businessweek Opinion More

and therefore that existence

H.E. Dr Hala Al-Tuwaijri

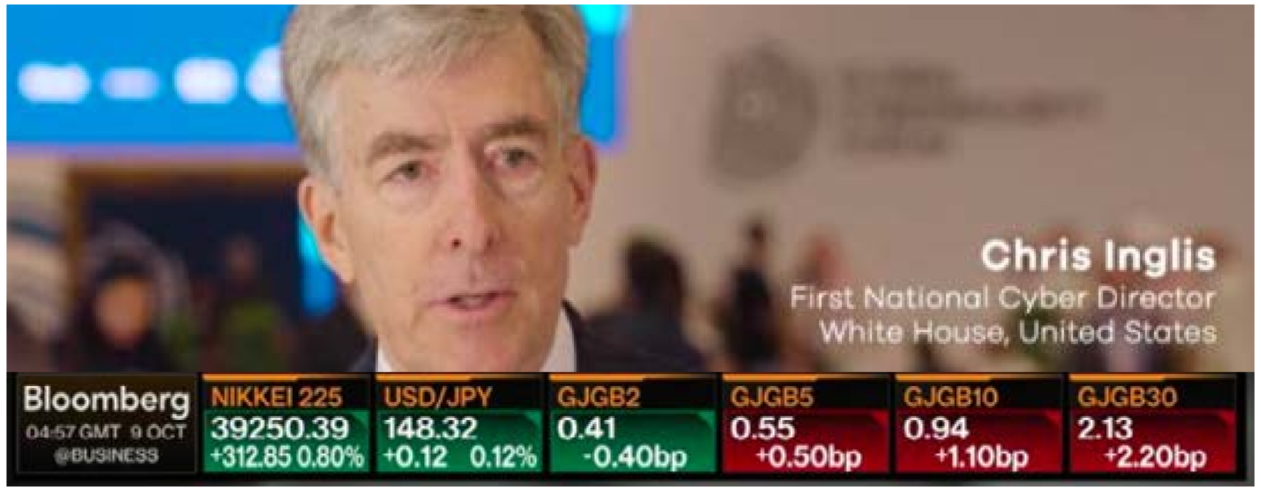
GCF MEDIA PARTNERS

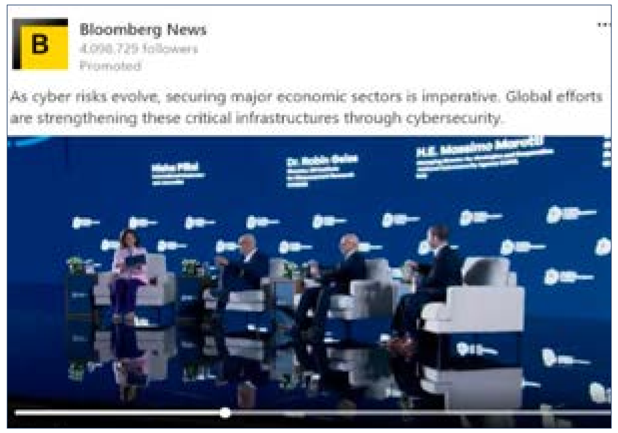
Bloomberg Media

GCF partnered with Bloomberg Media – a global news platform that provides news, insights, and analysis across 120+ news bureaus in 70+ countries. With a full production team deployed on-ground to interview and produce content in real-time, the partnership resulted in coverage across broadcast, digital and social media, reaching audiences of millions.

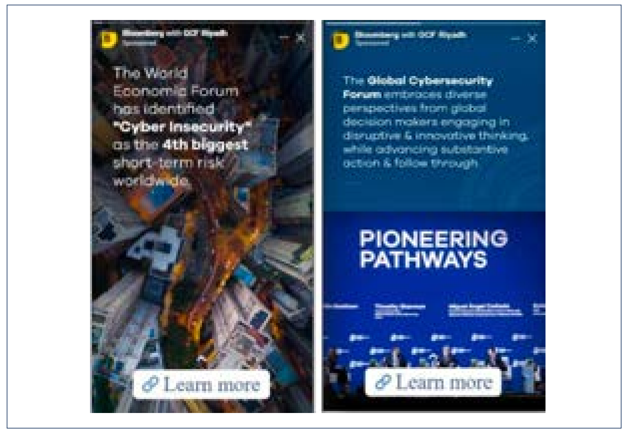
CONTENT & COVERAGE

- **17.5m** – audience size for Bloomberg TV on which a selection of videos featured
- **800K impressions** - guaranteed on two videos on the GCF Annual Meeting 2024 background themes and event sessions, featured on Bloomberg.com, Bloomberg App, YouTube and LinkedIn network
- **150K views** - guaranteed on editorial storycard distributed across Bloomberg Business's social media channels




Bloomberg News
4,098,729 followers
Promoted

As cyber risks evolve, securing major economic sectors is imperative. Global efforts are strengthening these critical infrastructures through cybersecurity.


Bloomberg with GCF Riyadh
Sponsored

The World Economic Forum has identified **"Cyber Insecurity"** as the **4th biggest** short-term risk worldwide.

Learn more

Bloomberg with GCF Riyadh
Sponsored

The **Global Cybersecurity Forum** embraces diverse perspectives from global decision makers engaging in disruptive & innovative thinking, while advancing substantive action & follow through

PIONEERING PATHWAYS

Learn more

CGTN

GCF partnered with China Global Television Network (CGTN) to deliver a range of editorial coverage and interviews at the GCF Annual Meeting 2024, with Presenter Yang Chengxi on-ground at the event. Headquartered in Beijing, CGTN has locations in Nairobi, Washington D.C. and London, and its TV channels are available in more than 160 countries and regions worldwide.

CONTENT & COVERAGE

- **400m** - audience size for CGTN's global shows in which 3 editorial pieces were featured
- **13m people per month –** size of CGTN audience to which on-ground interviews & coverage were shared

CGTN
WORLD TODAY
JOSE MANUEL BARROSO
Former President of the European Commission
15:09 NAIROBI
Gaza health ministry: At least 41,825 Palestinians killed in Israeli attacks si

العربية
alarabiya

GCF partnered with leading 24-hour digital news platform, Al Arabiya, to provide multi-platform editorial coverage of the GCF Annual Meeting to a global audience. Presenters Lara Habib, Riz Khan, Rima Maktabi, and Obaida Alladdan led activity on-ground, supported by a full production team.

CONTENT & COVERAGE

- **29.9m visits –** to Al Arabiya online platforms hosting Annual Meeting 2024, coverage, reporting, and interviews
- **9m** – approximate reach per piece of coverage on the Annual Meeting 2024

ADVANCING COLLECTIVE ACTION … SPACE
لانها تستطيع التحدث مع الجميع وهذ شيء جيد
جوزيه مانويل باروسو > رئيس المفوضية الاوروبية السابق
BUSINESS

المنتدى الدولي للامن السيبراني
يتولى إعداد الدراسات والبحوث
بالتعاون مع الجهات الدولية
والشركاء العالميين
العربية

Experts address AI, global security threats, solutions to cybercrimes

العربية
عادل الجبير > وزير الدولة للشؤون الخارجية ومبعوث شؤون المناخ في السعودية
BUSINESS

GLOBAL CYBERSECURITY
الرياض > "تعظيم العمل المشترك في الفضاء السيبراني" شعار المنتدى الدولي للامن السيبراني
BUSINESS

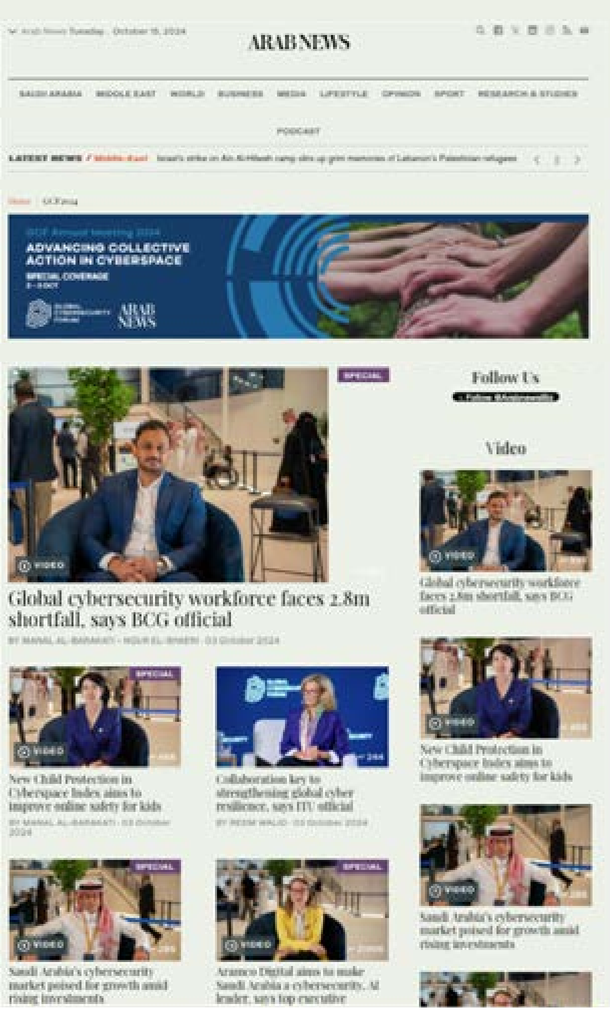
ARAB NEWS

GCF partnered with Saudi Arabia's leading English-language newspaper, Arab News, to deliver 360-degree coverage of the GCF Annual Meeting 2024. A team of journalists, led by Business Editor Reina Takla, were on-ground to conduct interviews, live reporting, and social media promotion of the event.

CONTENT & COVERAGE

In total, Arab News published **18 pieces of content** across its channels – including a dedicated page on the Arab News website:

- **2.2m visits** - to Arab News online platforms hosting Annual Meeting 2024 coverage, reporting, and interviews
- **1m -** approximate reach per piece of coverage on the Annual Meeting 2024


Arab News Tuesday, October 15, 2024

ARAB NEWS

SAUDI ARABIA MIDDLE EAST WORLD BUSINESS MEDIA LIFESTYLE OPINION SPORT RESEARCH & STUDIES

PODCAST

LATEST NEWS / Middle-East Israel's strike on Ain Al-Hilweh camp stirs up grim memories of Lebanon's Palestinian refugees

Home / GCF2024

GCF Annual Meeting 2024
ADVANCING COLLECTIVE ACTION IN CYBERSPACE
SPECIAL COVERAGE
1–3 OCT
GLOBAL CYBERSECURITY FORUM ARAB NEWS

SPECIAL

Global cybersecurity workforce faces 2.8m shortfall, says BCG official
BY MANAL AL-BARAKATI - NOUR EL-SHAEIN · 03 October 2024

New Child Protection in Cyberspace Index aims to improve online safety for kids
BY MANAL AL-BARAKATI · 03 October 2024

Collaboration key to strengthening global cyber resilience, says ITU official
BY REEM WALID · 03 October 2024

Saudi Arabia's cybersecurity market poised for growth amid rising investments

Aramco Digital aims to make Saudi Arabia a cybersecurity, AI leader, says top executive

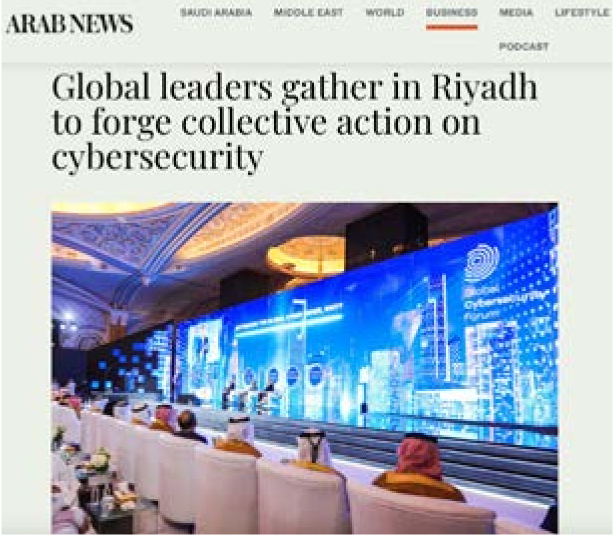
Follow Us

Video

Global cybersecurity workforce faces 2.8m shortfall, says BCG official

New Child Protection in Cyberspace Index aims to improve online safety for kids

Saudi Arabia's cybersecurity market poised for growth amid rising investments


ARAB NEWS

SAUDI ARABIA MIDDLE EAST WORLD BUSINESS MEDIA LIFESTYLE

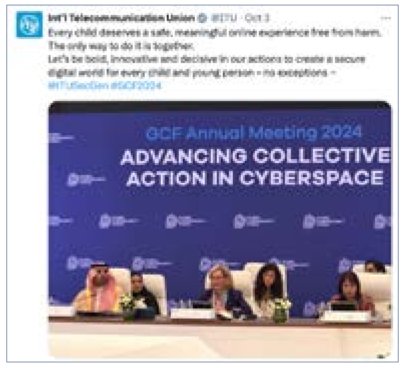
PODCAST

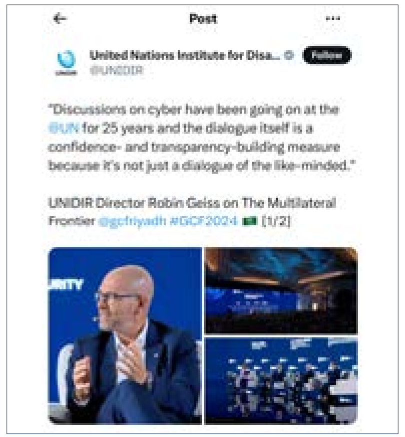
Global leaders gather in Riyadh to forge collective action on cybersecurity

GCF COMMUNITY: SUSTAINED ENGAGEMENT

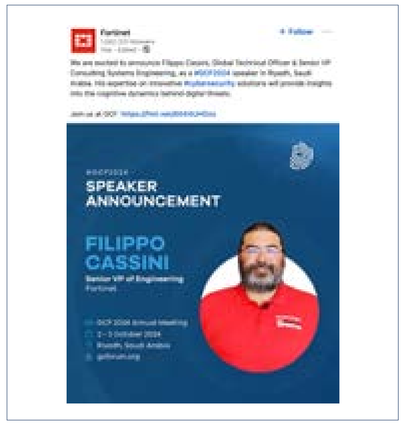
Bringing together experts and decision makers from government, the private sector, international organizations, and academia, the GCF Annual Meeting 2024's impact was far-reaching, generating diverse engagement across the GCF community as speakers, delegates, and partners joined the conversation beyond the Annual Meeting stage.

COMMUNITY-GENERATED CONTENT

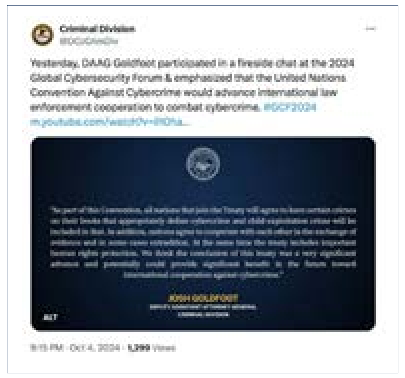

Int'l Telecommunication Union @ITU · Oct 3
Every child deserves a safe, meaningful online experience free from harm. The only way to do it is together.
Let's be bold, innovative and decisive in our actions to create a secure digital world for every child and young person – no exceptions →
#ITUSecGen #GCF2024


Post
United Nations Institute for Disa... Follow
@UNIDIR
"Discussions on cyber have been going on at the @UN for 25 years and the dialogue itself is a confidence- and transparency-building measure because it's not just a dialogue of the like-minded."

UNIDIR Director Robin Geiss on The Multilateral Frontier @gcfriyadh #GCF2024 🇸🇦 [1/2]

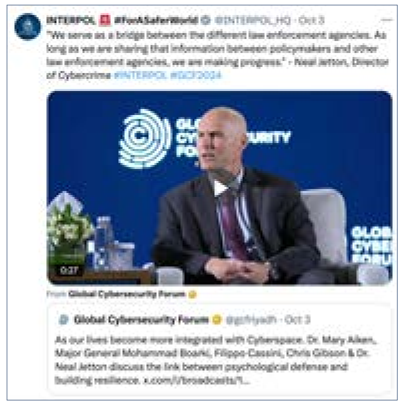

Fortinet + Follow
We are excited to announce Filippo Cassini, Global Technical Officer & Senior VP Consulting Systems Engineering, as a #GCF2024 speaker in Riyadh, Saudi Arabia. His expertise on innovative #cybersecurity solutions will provide insights into the cognitive dynamics behind digital threats.

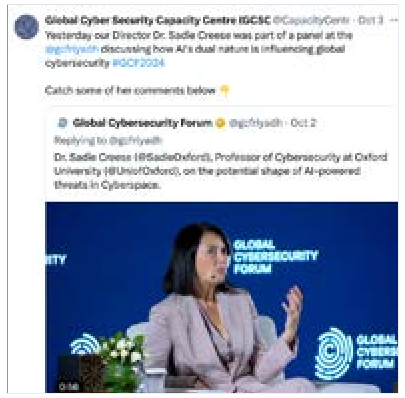
Join us at GCF: https://[illegible]


Criminal Division
@DOJCrimDiv
Yesterday, DAAG Goldfoot participated in a fireside chat at the 2024 Global Cybersecurity Forum & emphasized that the United Nations Convention Against Cybercrime would advance international law enforcement cooperation to combat cybercrime. #GCF2024
m.youtube.com/watch?v=lR0ha...

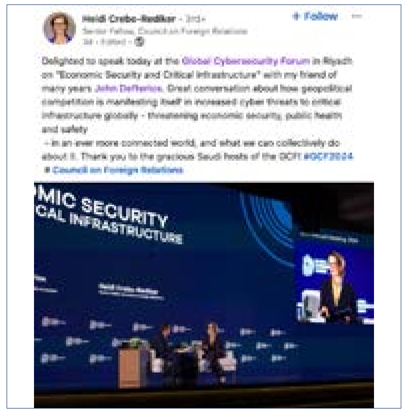
"As part of this Convention, all nations that join the Treaty will agree to have certain crimes on their books that appropriately define cybercrime and child exploitation crime will be included in that. In addition, nations agree to cooperate with each other in the exchange of evidence and in some cases extradition. At the same time the treaty includes important human rights protection. We think the conclusion of this treaty was a very significant advance and potentially could provide significant benefit in the future toward international cooperation against cybercrime."
JOSH GOLDFOOT

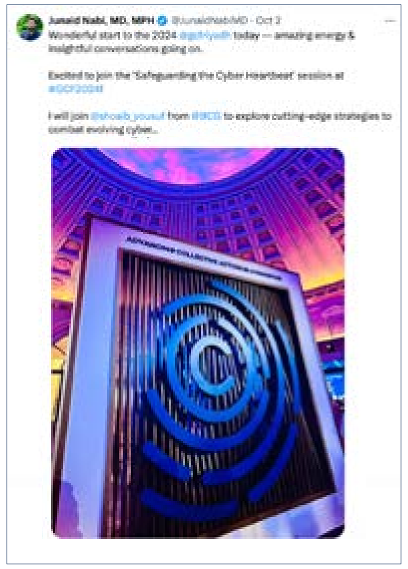
9:15 PM · Oct 4, 2024 · 1,399 Views


INTERPOL #ForASaferWorld @INTERPOL_HQ · Oct 3
"We serve as a bridge between the different law enforcement agencies. As long as we are sharing that information between policymakers and other law enforcement agencies, we are making progress." - Neal Jetton, Director of Cybercrime #INTERPOL #GCF2024
From Global Cybersecurity Forum
Global Cybersecurity Forum @gcfriyadh · Oct 3
As our lives become more integrated with Cyberspace, Dr. Mary Aiken, Major General Mohammad Boarki, Filippo Cassini, Chris Gibson & Dr. Neal Jetton discuss the link between psychological defense and building resilience. x.com/i/broadcasts/1...


Global Cyber Security Capacity Centre (GCSC @CapacityCentr · Oct 3
Yesterday our Director Dr. Sadie Creese was part of a panel at the @gcfriyadh discussing how AI's dual nature is influencing global cybersecurity #GCF2024

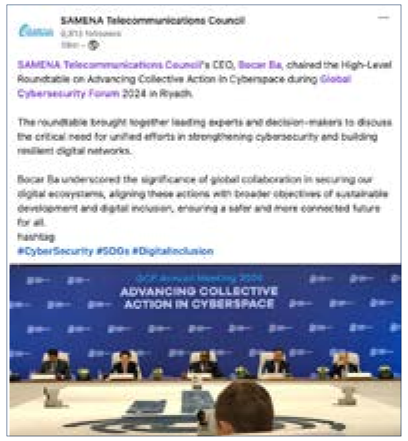
Catch some of her comments below 👇
Global Cybersecurity Forum @gcfriyadh · Oct 2
Replying to @gcfriyadh
Dr. Sadie Creese (@SadieOxford), Professor of Cybersecurity at Oxford University (@UniofOxford), on the potential shape of AI-powered threats in Cyberspace.


Heidi Crebo-Rediker · 3rd+ + Follow
Senior Fellow, Council on Foreign Relations
3d · Edited
Delighted to speak today at the Global Cybersecurity Forum in Riyadh on "Economic Security and Critical Infrastructure" with my friend of many years John Defterios. Great conversation about how geopolitical competition is manifesting itself in increased cyber threats to critical infrastructure globally - threatening economic security, public health and safety
– in an ever more connected world, and what we can collectively do about it. Thank you to the gracious Saudi hosts of the GCF! #GCF2024
Council on Foreign Relations


Junaid Nabi, MD, MPH @JunaidNabiMD · Oct 2
Wonderful start to the 2024 @gcfriyadh today — amazing energy & insightful conversations going on.

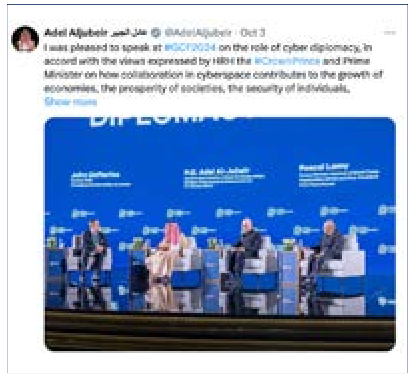
Excited to join the 'Safeguarding the Cyber Heartbeat' session at #GCF2024!

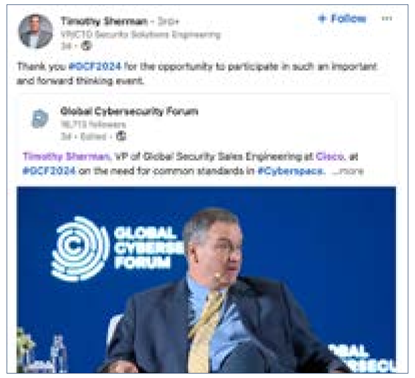
I will join @shoaib_yousuf from @BCG to explore cutting-edge strategies to combat evolving cyber...

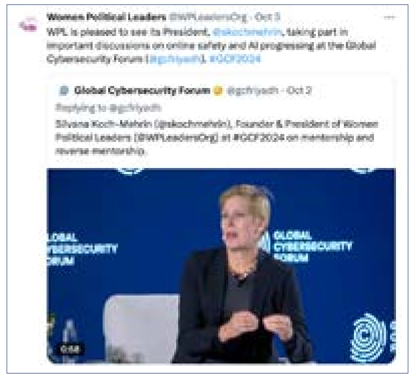

SAMENA Telecommunications Council
6,813 followers
10mo
SAMENA Telecommunications Council's CEO, Bocar Ba, chaired the High-Level Roundtable on Advancing Collective Action in Cyberspace during Global Cybersecurity Forum 2024 in Riyadh.

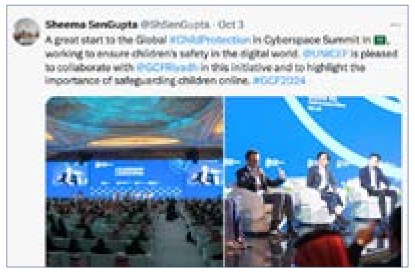
The roundtable brought together leading experts and decision-makers to discuss the critical need for unified efforts in strengthening cybersecurity and building resilient digital networks.

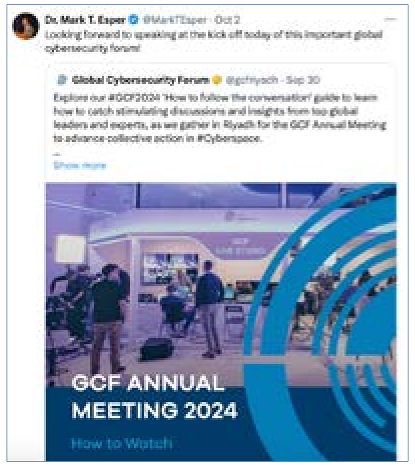
Bocar Ba underscored the significance of global collaboration in securing our digital ecosystems, aligning these actions with broader objectives of sustainable development and digital inclusion, ensuring a safer and more connected future for all.
hashtag
#CyberSecurity #SDGs #DigitalInclusion

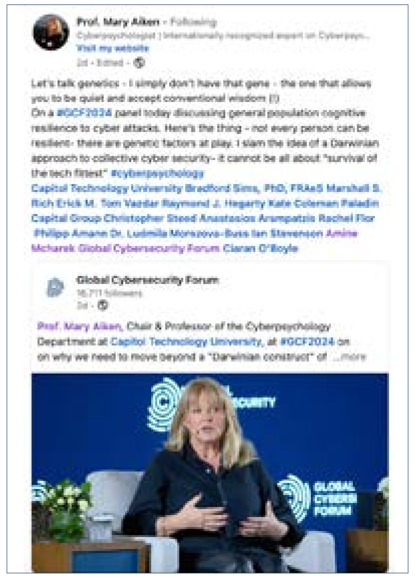

Adel Aljubeir عادل الجبير @AdelAljubeir · Oct 3
I was pleased to speak at #GCF2024 on the role of cyber diplomacy, in accord with the views expressed by HRH the #CrownPrince and Prime Minister on how collaboration in cyberspace contributes to the growth of economies, the prosperity of societies, the security of individuals,
Show more

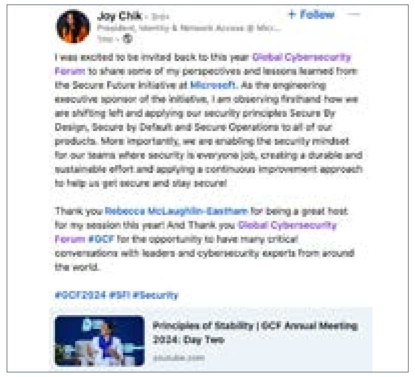

Timothy Sherman · 3rd+ + Follow
VP/CTO Security Solutions Engineering
3d
Thank you #GCF2024 for the opportunity to participate in such an important and forward thinking event.
Global Cybersecurity Forum
16,713 followers
3d · Edited
Timothy Sherman, VP of Global Security Sales Engineering at Cisco, at #GCF2024 on the need for common standards in #Cyberspace. ...more


Women Political Leaders @WPLeadersOrg · Oct 3
WPL is pleased to see its President, @skochmehrin, taking part in important discussions on online safety and AI progressing at the Global Cybersecurity Forum (@gcfriyadh). #GCF2024
Global Cybersecurity Forum @gcfriyadh · Oct 2
Replying to @gcfriyadh
Silvana Koch-Mehrin (@skochmehrin), Founder & President of Women Political Leaders (@WPLeadersOrg) at #GCF2024 on mentorship and reverse mentorship.


Sheema SenGupta @ShSenGupta · Oct 3
A great start to the Global #ChildProtection in Cyberspace Summit in 🇸🇦, working to ensure children's safety in the digital world. @UNICEF is pleased to collaborate with @GCFRiyadh in this initiative and to highlight the importance of safeguarding children online. #GCF2024


Dr. Mark T. Esper @MarkTEsper · Oct 2
Looking forward to speaking at the kick off today of this important global cybersecurity forum!
Global Cybersecurity Forum @gcfriyadh · Sep 30
Explore our #GCF2024 'How to follow the conversation' guide to learn how to catch stimulating discussions and insights from top global leaders and experts, as we gather in Riyadh for the GCF Annual Meeting to advance collective action in #Cyberspace.
...
Show more


Prof. Mary Aiken · Following
Cyberpsychologist | Internationally recognized expert on Cyberpsy...
Visit my website
2d · Edited
Let's talk genetics - I simply don't have that gene - the one that allows you to be quiet and accept conventional wisdom (!)
On a #GCF2024 panel today discussing general population cognitive resilience to cyber attacks. Here's the thing - not every person can be resilient- there are genetic factors at play. I slam the idea of a Darwinian approach to collective cyber security- it cannot be all about "survival of the tech fittest" #cyberpsychology
Capitol Technology University Bradford Sims, PhD, FRAeS Marshall S. Rich Erick M. Tom Vazdar Raymond J. Hegarty Kate Coleman Paladin Capital Group Christopher Steed Anastasios Arampatzis Rachel Flor Philipp Amann Dr. Ludmila Morozova-Buss Ian Stevenson Amine Mcharek Global Cybersecurity Forum Ciaran O'Boyle
Global Cybersecurity Forum
16,711 followers
2d
Prof. Mary Aiken, Chair & Professor of the Cyberpsychology Department at Capitol Technology University, at #GCF2024 on on why we need to move beyond a "Darwinian construct" of ...more


Joy Chik · 3rd+ + Follow
President, Identity & Network Access @ Micr...
1mo
I was excited to be invited back to this year Global Cybersecurity Forum to share some of my perspectives and lessons learned from the Secure Future Initiative at Microsoft. As the engineering executive sponsor of the initiative, I am observing firsthand how we are shifting left and applying our security principles Secure By Design, Secure by Default and Secure Operations to all of our products. More importantly, we are enabling the security mindset for our teams where security is everyone job, creating a durable and sustainable effort and applying a continuous improvement approach to help us get secure and stay secure!

Thank you Rebecca McLaughlin-Eastham for being a great host for my session this year! And Thank you Global Cybersecurity Forum #GCF for the opportunity to have many critical conversations with leaders and cybersecurity experts from around the world.

#GCF2024 #SFI #Security

Principles of Stability | GCF Annual Meeting 2024: Day Two
youtube.com

GCF PODCAST

Helping to transform the way we think about Cyberspace, the GCF podcast returns for another season.

Launched in 2022, the GCF **Rethinking Cyber** podcast has brought together a selection of GCF speakers and experts over two successful seasons for thought-provoking and accessible conversations on the opportunities and challenges shaping Cyberspace.

With sessions recorded live from on the ground at the GCF Annual Meeting 2024, Rethinking Cyber is returning for its third season, capturing engaging conversations with the world's foremost voices in the field.

This season promises more insightful episodes with top decision makers, experts, and thought leaders from around the world.

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

Listen on Spotify

Listen on

GUESTS FOR SEASON 3

Dr. Mark Esper
27th U.S. Secretary of Defense

Chris Inglis
Former National Cyber Director, United States Government

Sir Jeremy Fleming
Former Director, GCHQ, United Kingdom

Dr. Junaid Nabi
Senior Fellow, The Aspen Institute

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

Shyam Saran
Former Minister of Foreign Affairs, India

Pascal Lamy
Vice President, Paris Peace Forum
Former Director General, World Trade Organization (WTO)

Professor William H. Dutton
Oxford Martin Fellow, Global Cyber Security Capacity Centre (GCSCC), University of Oxford

Professor Richard Staynings
Chief Security Strategist, Cylera
Teaching Professor, University of Denver

QUOTES FROM OUR COMMUNITY

" GCF was a master class in action-oriented cyber strategy, policy, and practice. The quality of the agenda, the speakers and the venue were all superb, enabling real progress in the goal of collective action in Cyberspace. "

CHRIS INGLIS

Former U.S. National Cyber Director

" I really enjoyed participating, for the second consecutive year, at the Global Cybersecurity Forum... I believe Riyadh and Saudi Arabia are establishing themselves as a prime hub for international cooperation, both public and private, on cybersecurity. "

JOSÉ MANUEL BARROSO

Former President of the European Commission,
and former Prime Minister of Portugal

" While we live in a globally connected world, geography still matters. So it is wonderful that the GCF can bring people from 125 different countries together to share insights on such critical issues of cybersecurity. "

DR. WILLIAM H. DUTTON

Martin Fellow, Global Cyber Security
Capacity Centre, University of Oxford

" GCF's success in bridging the geopolitical divide and bringing together all key stakeholders from across the world – government representatives, civil society, scientific experts, and diplomatic practitioners – in the promotion of cybersecurity is truly remarkable. "

SHYAM SARAN

Former Foreign Secretary of India

" GCF 2024 was a great event rightly focused on the pressing cyber issues of the day: from the threats cyberspace presents to our nations' security, prosperity, societies, and peoples, to the need to strengthen and harmonize cybersecurity laws, regulations, and cooperation between likeminded countries. GCF's success was further built upon by the broad and diverse group of experts and leaders it assembled to address all aspects of these important cyber issues. "

DR. MARK ESPER

27th Secretary of Defense, United States

" I am proud to be a longstanding academic contributor to the Global Cybersecurity Forum – an exemplar of global cyber leadership. Every year, the event grows from strength to strength, with a dedicated team and a wide range of international experts and stakeholders working tirelessly to enhance global cooperation in Cyberspace. "

DR. MARY AIKEN

Chair and Professor, Cyberpsychology Department,
Capitol Technology University

" The 2024 Global Cybersecurity Forum in Riyadh exemplified GCF's unique ability to convene global leaders and drive actionable solutions in cybersecurity... The quality of discussions and diversity of perspectives from government, private sector, and academia created an unparalleled environment for addressing critical cybersecurity challenges. "

DR. JUNAID NABI

Senior Fellow, The Aspen Institute

" As a platform that brought stakeholders together from all around the world, the GCF Annual Meeting 2024 provided the necessary momentum for all of us to face, with collective strength, the multifaceted challenges associated with resilient connectivity, Cyberspace security, digital inclusivity, and sustainability. "

BOCAR A. BA

CEO, SAMENA Telecommunications Council

AN EVENING OF CULTURAL IMMERSION

October 2nd, 2024 Al Murabba

On October 2nd, 2024, delegates and speakers from the GCF Annual Meeting 2024 gathered at Al Murabba for an evening of cultural immersion.

Hosted at this iconic venue, renowned for its historical significance and cultural charm, guests had the opportunity to embark on a captivating tour that delved into the rich history of the location. Traditional artwork was showcased alongside artisan crafts and enchanting artistic performances, truly immersing attendees in local culture.

Attendees were also able to network with their peers and reflect on the critical discussions that had taken place that day.

03

CHILD PROTECTION IN CYBERSPACE GLOBAL SUMMIT

CPC GLOBAL SUMMIT

The Child Protection in Cyberspace (CPC) Global Summit was held in conjunction with the GCF Annual Meeting 2024, in collaboration with the International Telecommunication Union (ITU), United Nations Children's Fund (UNICEF), the Global Cybersecurity Forum, DQ Institute, and WeProtect Global Alliance. The summit brought together key stakeholders from around the world to identify pathways for collaboration and collective action towards ensuring that children are safe in Cyberspace.

OBJECTIVES

Consolidating global efforts and advancing collective action

Enhancing the global response to pressing challenges

Mitigating emerging threats facing children in Cyberspace

Ensuring that CPC resonates with the agenda of global decision makers

These objectives are in line with the goals of the

- Child Protection in Cyberspace (CPC) initiative
- United Nations Sustainable Development Goals (SDGs) 4, 5, 16 and 17, under the 2030 Agenda for Sustainable Development

IN COLLABORATION WITH

ITU · unicef for every child · GLOBAL CYBERSECURITY FORUM · DQ Institute Global Standards for Digital Intelligence · WeProtect GLOBAL ALLIANCE

CPC GLOBAL SUMMIT PROGRAM

OCTOBER 2ND, 2024 (DAY 1)

11:00 **ITU BRIEF: CHILD ONLINE PROTECTION** ROOM C1 20 MIN

Carla Licciardello
Child Protection Focal Point
ITU

12:50 **CHILD PROTECTION IN CYBERSPACE: TRENDS, CHALLENGES AND OPPORTUNITIES FOR PROGRESS** ROOM G 20 MIN

Rima Maktabi (Moderator)
London Bureau Chief
Al Arabiya

Dr. Najat Maalla
Special Representative of
the UN Secretary-General on
Violence against Children
– SRSG VAC

14:00 **DQ INSTITUTE BRIEF: DIGITAL INTELLIGENCE FOR ALL** ROOM C1 20 MIN

Dr. Yuhyun Park
Founder & CEO
DQ Institute

15:30 **CRACKING THE CODE: UNDERSTANDING THE TOOLS FOR CHILD ONLINE PROTECTION** ROOM C2 30 MIN

Jay Bhatnagar (Moderator)
Principal
BCG

Alain Penel
Vice President Middle East,
Turkey, & CIS
Fortinet

Afrooz Johnson
Child Protection Specialist
UNICEF HQ

Davis Vu
Chief Creative Officer
DQ LAB

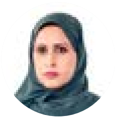
Orhan Osmani
Head, Cybersecurity
Division at BDT
ITU

Partner Brief Panel Discussion Roundtable Fireside Chat

OCTOBER 3RD, 2024 (DAY 2)

10:00 **CHILD PROTECTION ONLINE: AN AGENDA FOR COLLABORATIVE INNOVATION** ROOM C2 30 MIN

Laura Buckwell (Moderator)
International
moderator


Dr. Maimoonah Al Khalil
Secretary General
Family Affairs Council,
Saudi Arabia

Dr. Yuhyun Park
Founder & CEO
DQ Institute

Iain Drennan
Executive Director
WePROTECT Global Alliance

11:30 **HIGH-LEVEL ROUNDTABLE: ADVANCING COLLECTIVE ACTION FOR CHILD PROTECTION IN CYBERSPACE** ROOM F 90 MIN

14:00 **WEPROTECT BRIEF: FOCUS ON THE FUTURE: EMERGING TRENDS IN CHILD PROTECTION ONLINE** ROOM C1 20 MIN

Iain Drennan
Executive Director
WePROTECT Global Alliance

14:00 **UNICEF BRIEF: A CYBERSPACE FIT FOR CHILDREN - PROTECTING AND PRIORITIZING CHILD RIGHTS AND SAFETY IN CYBERSPACE** ROOM C1 20 MIN

Afrooz Johnson
Child Protection Specialist
UNICEF HQ

Partner Brief Panel Discussion Roundtable Fireside Chat

CPC GLOBAL SUMMIT PROCEEDINGS

CPC GLOBAL SUMMIT ROUNDTABLE

The CPC Global Summit Roundtable opened with remarks by representatives of the summit partners: Doreen Bogdan-Martin, Secretary-General of the ITU, Sheema Sen Gupta, Director of Child Protection at UNICEF, His Excellency Majed bin Mohammed Al-Mazyed, Governor of the National Cybersecurity Authority of Saudi Arabia, representing the GCF Board of Trustees, Dr. Yuhyun Park, Founder and CEO of DQ Institute, and Iain Drennan, Executive Director of WeProtect Global Alliance.

It led into a high-level roundtable session, "Advancing Collective Action for Child Protection in Cyberspace." Discussions centered on the four summit objectives, exploring key questions and challenges facing the global community in preventing harm and achieving greater protection for all children in Cyberspace.

ROUNDTABLE PARTICIPANTS

RECOMMENDATIONS

A number of recommendations for collective action on child cyber safety were highlighted by participants of the CPC Global Summit Roundtable.

Integrate Child Protection into Development Goals: Make child safety a core element of Environmental, Social, and Governance (ESG) goals and integrate it into the Sustainable Development Goals (SDGs) with a target to reduce online risks to children to zero by 2030.

Enhance Public-Private Partnerships: Foster collaboration between the public and private sectors, emphasizing the importance of cross-sector cooperation and national coordination for effective child protection.

Leverage Technology: Utilize artificial intelligence (AI) and machine learning to detect and prevent online crimes and ensure transparency from tech companies regarding their responsibilities in protecting children.

Empower Parents and Educators: Provide parents with the knowledge and tools needed to guide their children in the online environment, while ensuring children have safe, age-appropriate access to technology.

Update Legislation and Policies: Revise and create updated legislation to address emerging threats, ensuring child protection remains central in policy discussions.

Establish Global Standards: Work towards creating global standards to combat threats, such as deep fakes and AI-generated content, and encourage consistent practices across platforms for detecting and reporting harmful content.

Develop Context-Specific Solutions: Recognize that each country faces unique challenges and approach child protection with tailored, context-specific solutions while respecting children's rights.

Incentivize Proactive Measures: Shift from reactive responses to proactive strategies by incentivizing companies to adopt forward-thinking approaches to child protection and prepare for future threats.

Promote Age-Appropriate Technology Use: Encourage initiatives that promote age-appropriate access to technology and foster resilience among children to navigate future challenges effectively.

Engage Stakeholders in Collective Action: Leverage existing momentum to unite all stakeholders around child protection, encouraging collaboration and shared responsibility.

Focus on Mental Health and Accountability: Address the increasing mental health issues in children related to online activities and hold social media companies accountable to their own standards, especially concerning age restrictions.

Leverage Existing Efforts: Leverage the momentum of existing frameworks, such as the United Nations convention against cybercrime, the Global Digital Compact, and the outcomes of the WSIS+20 Forum High-Level Event to strengthen international cooperation and facilitate evidence-sharing to combat crimes committed using information and communications technology.

The participants reaffirmed their commitment to advancing Child Online Protection by consolidating actions, enhancing responses, addressing emerging threats, and ensuring that it is prioritized within global agendas. They called upon all stakeholders to join their efforts in this essential endeavor to protect the next generation in Cyberspace and suggested the Global Summit to be held every two years to monitor and assess progress.

Partner Brief

CPC GLOBAL SUMMIT

ITU BRIEF

Child Online Protection

- **Carla Licciardello,** Child Online Protection Focal Point, International Telecommunication Union (ITU)

The presentation by the International Telecommunication Union (ITU) focused on the critical need to protect children in Cyberspace through the Child Online Protection initiative. This global effort, launched in 2008, emphasizes a comprehensive approach to cyber safety and is designed to safeguard vulnerable communities, especially children, by developing tools to address the issue and raise awareness. The session outlined how the ITU is addressing cyber risks through policy frameworks and partnerships with organizations like UNICEF.

A key element of the initiative is its five-pillar approach, which includes legal measures, technical solutions, organizational structures, capacity building, and international cooperation. A notable achievement was the creation of the Child Online Protection Guidelines, which are available in six languages and adaptable for the national level. These guidelines target various stakeholders, including policymakers, educators, industry professionals, and children themselves. The Child Online Protection initiative has evolved to empower children to take an active role in their own protection, ensuring that they are part of the solution to online risks.

The ITU also stressed the importance of global collaboration, especially in tackling new threats from artificial intelligence (AI). Initiatives like self-paced training on the ITU Academy platform aim to equip a wide range of stakeholders with the skills needed to address challenges to children's safety online. Going forward, the focus will be on using technology, not only for protection purposes, but also to empower children to continue adapting to the evolving cyber landscape.

Fireside Chat

CPC GLOBAL SUMMIT

CHILD PROTECTION IN CYBERSPACE

Trends, Challenges, and Opportunities for Progress

- **Dr. Najat Maalla,** Special Representative of the UN Secretary-General on Violence against Children, SRSG VAC
- **Rima Maktabi (Moderator),** London Bureau Chief, Al Arabiya

During the fireside chat on 'Child Protection in Cyberspace: Trends, Challenges, and Opportunities for Progress', Dr. Najat Maalla examined the growing risks children face in Cyberspace today. While it offers a myriad of opportunities for learning and socialization, Cyberspace also exposes children to threats like sexual exploitation, cyberbullying, hate speech, and misinformation. Dr. Maalla highlighted the challenge of underreporting, as only one third of children report abuse due to fear, stigma, or a lack of appropriate reporting mechanisms.

According to Dr. Maalla, over 300 million children become victims of online sexual abuse annually. Hate speech exposure ranges from 8% to 50%, while 25% of children encounter content related to self-harm. The discussion stressed the need for a more proactive approach, calling for stronger collaboration between technology companies and law enforcement, as well prioritizing child safety and privacy by design across all platforms. Artificial intelligence (AI) plays a critical role in identifying and removing harmful content swiftly, but significant challenges remain in terms of reporting and enforcement.

The discussion emphasized the need for collective action by parents, the technology sector, and governments to enhance child protection in Cyberspace. It stressed the importance of empowering children to be both learners and protectors, promoting responsible technology use, and leveraging AI for swift detection of harmful content. Collaborating with technology companies is essential to ensure that platforms are designed with child safety in mind and maintaining a balance between fostering creativity and ensuring children's security.

Partner Brief

CPC GLOBAL SUMMIT

DQ INSTITUTE BRIEF

Digital Intelligence for All

- **Dr. Yuhyun Park,** Founder & CEO, DQ Institute

During the DQ Institute Brief, Dr. Yuhyun Park, the organization's Founder and CEO, addressed the critical challenge of child online protection, emphasizing that 70% of children worldwide are exposed to cyber risks. She explained that this is not merely a technology or parenting issue but a broader societal concern. Dr. Park presented a three-part action plan aimed at mitigating these risks, highlighting the urgent need to educate cyber citizens and implement stronger policies to keep pace with technological advancement.

Dr. Park proposed setting measurable targets to reduce child cyber risk, comparing the effort to global climate initiatives. A key element of this strategy is equipping children with essential cyber citizenship skills, helping them navigate the cyber world responsibly. She also stressed the need for rapidly scaling cyber literacy education, empowering teachers globally to provide high-quality training. Additionally, Dr. Park called for embedding "safety by design" principles into cyber infrastructure, ensuring that governments and companies commit to building safer environments for children.

The session concluded with a call for collective global action, as Dr. Park emphasized that cyber safety must become a priority, requiring coordinated efforts between governments, companies, educators, and families. By combining comprehensive cyber education with proactive safety measures, the goal is to create a safer and more secure Cyberspace for children globally.

Panel Discussion

CPC GLOBAL SUMMIT

CHILD PROTECTION ONLINE

An Agenda for Collaborative Innovation

- **Iain Drennan,** Executive Director, WePROTECT Global Alliance
- **Dr. Yuhyun Park,** Founder & CEO, DQ Institute
- **Dr. Maimoonah Al Khalil,** Secretary General, Family Affairs Council, Saudi Arabia
- **Laura Buckwell,** International Moderator

The 'Child Protection Online: An Agenda for Collaborative Innovation' panel examined the critical risks and challenges children face in the cyber age, emphasizing the need for stronger collaboration and innovative strategies to ensure their safety. As technology becomes increasingly embedded in children's daily lives, threats such as exposure to inappropriate content, online predators, and cyberbullying pose serious risks to their mental health, privacy, and overall well-being. The discussion focused on how governments, private-sector organizations, parents, and educators can join forces to create a safer Cyberspace for children around the world.

A core theme of the session was the need for a comprehensive, multistakeholder approach to protect children in Cyberspace. This includes coordinated efforts between governments, law enforcement, and educational institutions at the national level, as well as regional and international cooperation to address the borderless, global nature of these threats. The panelists underscored the importance of empowering children through digital literacy, while schools and parents need to play an active role in educating children about cyber risks to foster responsible cyber citizens. Equipping children with the skills to navigate the cyber landscape safely and ethically not only mitigates risks but also unlocks opportunities for personal growth and development.

The panel concluded by highlighting that protecting children in Cyberspace demands continuous, adaptive efforts. Governments must establish robust regulatory frameworks, parents need to be actively involved in their children's online activities, and tech companies must embed protective features within their platforms to enhance safety. Effective collaboration between all stakeholders is crucial, with innovative solutions – such as AI-powered content moderation and age-verification technologies – playing a key role in addressing emerging threats.

The panelists concluded that, moving forward, children's safety and well-being should be prioritized by key stakeholders as Cyberspace continues to evolve.

Panel Discussion

CPC GLOBAL SUMMIT

CRACKING THE CODE

Understanding the Tools for Child Online Protection

- **Alain Penel,** Vice President Middle East, Turkey, & CIS, Fortinet
- **Afrooz Johnson,** Child Protection Specialist, UNICEF HQ
- **Davis Vu,** Chief Creative Officer, DQ LAB
- **Orhan Osmani,** Head, Cybersecurity Division, BDT ITU
- **Jay Bhatnagar (Moderator),** Principal, BCG

The 'Cracking the Code' session addressed the growing complexity of the threats facing children in Cyberspace, emphasizing the need for robust technological and policy frameworks to ensure their safety. The discussion began by highlighting that over 90% of children are online by the age of 12, with a significant number having been exposed to cyber threats. The global, interconnected nature of Cyberspace has made it increasingly challenging to protect children, necessitating a multistakeholder approach to ensure their safety.

A key focus was on leveraging technological advancements to enhance children's safety in Cyberspace. It was emphasized that schools must prioritize securing their networks, especially with the growing prevalence of students using personal devices. Additionally, participants talked of the importance of teaching cyber literacy and risk awareness from an early age to ensure that children are prepared to identify and respond effectively to potential threats.

The panel also highlighted the importance of a regulatory framework that addresses children's rights and safety in Cyberspace. International guidelines, such as the UN Guiding Principles on Business and Human Rights, were referenced as critical foundations upon which to build policies that mandate the safety of children in Cyberspace. While regulations like the EU Digital Services Act and Australia's Online Safety Act were cited as positive models, the fragmented nature of global laws continues to present significant challenges. Establishing harmonized, global standards for child protection online remains a critical and urgent priority to ensure consistent safeguards across jurisdictions.

Panelists suggested that the path forward requires a three-fold approach: education, regulation, and innovation. First, expanding cybersecurity education in schools – targeting not only students but also educators and parents – will be essential to building long-term resilience. Second, there is an urgent need for harmonized global regulations to close gaps in child protection standards across borders. Effective collaboration between governments, the private sector, and civil society can help ensure that these regulations remain comprehensive and adaptable to the ever-changing landscape of Cyberspace. Finally, fostering innovation, particularly in developing cross-sector tools for child protection, is critical. As Cyberspace continues to evolve, only a unified, multistakeholder approach can ensure children's safety online.

Alain Penel
Vice President Middle East, Turkey, & CIS
Fortinet
Afrooz Johnson
Child Protection Specialist
UNICEF HQ

Partner Brief

CPC GLOBAL SUMMIT

WEPROTECT BRIEF

Focus on the Future: Emerging Trends in Child Protection Online

- **Iain Drennan,** Executive Director, WeProtect Global Alliance

The presentation by WeProtect Global Alliance addressed the evolving threats children face in Cyberspace, with a particular focus on the growing prevalence of child sexual abuse and exploitation. It highlighted how emerging technologies, such as AI-generated content and virtual and augmented reality (VR/AR), are being exploited to spread new forms of child sexual abuse material, including deepfakes.

Key insights from the presentation included the alarming rise in financial sexual extortion targeting young boys, reflecting a shift from traditional abuse patterns. It also highlighted that criminal networks are increasingly using AI tools and cross-border operations to scale their activities, underscoring the critical need for international cooperation.

The session emphasized that an effective response requires collective action, starting with empowering children to actively participate in developing solutions. Strengthening support for frontline responders and fostering greater collaboration at the global level were also highlighted as equally important in enhancing current efforts. Looking forward, the session called for technology companies to embed safety-by-design principles from the outset, ensuring that platforms are equipped to protect children from growing risks in Cyberspace.

Partner Brief

CPC GLOBAL SUMMIT

UNICEF BRIEF

A Cyberspace Fit for Children: Protecting and Prioritizing Child Rights and Safety in Cyberspace

- **Afrooz Johnson,** Child Protection Specialist, UNICEF HQ

UNICEF's presentation focused on the critical role the organization plays in safeguarding children's rights in Cyberspace. Afrooz Johnson, UNICEF HQ's Child Protection Specialist, emphasized the need to incorporate children's needs from the outset of designing new technologies, warning of the potential harm caused by excluding them from the development process. As an estimated one in three people in Cyberspace are children, prioritizing their safety and well-being is essential in today's interconnected world.

Key risks were outlined through the 4C's framework: content, conduct, contact, and contract risks. These range from exposure to violent material to exploitation by online predators. While not all children encounter these risks, those who do can suffer significant harm that impacts on their mental health and development.

Looking forward, Johnson stressed the need for collaborative efforts that involve governments, private sector stakeholders, educators, and families. She emphasized that the focus needs to be on building stronger policies and systems, ensuring industry accountability, and promoting cyber literacy among children and parents. UNICEF remains committed to expanding its research and advocacy, working toward a Cyberspace that not only protects children from harm but also empowers them to reach their full potential.

04

GCF: A GLOBAL PLATFORM FOR ACTION-ORIENTED COLLABORATION

THE GCF JOURNEY

The Global Cybersecurity Forum (GCF) was launched as an event in 2020, during Saudi Arabia's G20 presidency, to convene stakeholders from around the world to address the most pressing global priorities for Cyberspace.

Since then, GCF has evolved as a platform for dialogue and multistakeholder engagement, culminating in its establishment in 2023, by Royal Decree, as an independent, non-profit organization headquartered in Riyadh.

GCF'S VISION AND STRATEGIC OBJECTIVES

Vision

Strengthen Cyberspace safety and resilience globally through collaborative priorities, purpose-driven dialogue, and impactful initiatives

Strategic objectives

1

Catalyze social impact

Champion actions with social impact to directly benefit global communities

2

Enable economic prosperity and security

Enhance the cybersecurity resilience of the global economy and accelerate growth in the cybersecurity sector

3

Push the boundaries of knowledge

Strengthen knowledge sharing and develop research networks on Cyberspace

4

Advance collaboration and collective action

Bring together key stakeholders around platforms for collaboration and purposeful dialogue

HOW WE WORK

Intersectional focus

Expanding knowledge boundaries by design
GCF has been advancing dialogue that integrates the geopolitical, social, economic, behavioral, and technical drivers shaping Cyberspace, thereby expanding knowledge boundaries.

Sustained community formation

Building networks and enduring relationships
GCF seeks to integrate Cyberspace stakeholders into a cohesive, global community by fostering the development of long-lasting personal connections and working relationships.

Action-oriented approach

Advancing progress through multistakeholder action
GCF facilitates direct collaboration between government entities, private sector actors, academics, and representatives from intergovernmental and non-governmental organizations.

Perspectival diversity

Convening international experts for cutting-edge expertise and thought leadership
GCF integrates intellectual sectoral and geographical diversity into all of its events. By bringing together participants with a varied range of perspectives and backgrounds, GCF ensures a blend of applied knowledge and academic expertise across a wide array of topics.

GCF ACTIVITIES

In support of its vision and mission, GCF is delivering a program of activities throughout the year under five key pillars:

INITIATIVES

As part of its mission, GCF undertakes various initiatives aimed at addressing specific challenges in Cyberspace. These initiatives are designed with clear, quantifiable targets and are typically time-bound to ensure focused and effective implementation dedicated to enhancing security and promoting safe online environments for all.

PLATFORMS

GCF's platforms are designed to empower and enable various stakeholder groups to take action on specific topics or sectors related to cybersecurity. These activities are typically enduring in nature, providing a continuous foundation for collaboration, innovation, and progress.

CENTERS

Centers are enduring institutional structures managed by GCF, either independently or in collaboration with partners, and are directed toward achieving a collective goal within a specialized domain of cybersecurity.

GCF has launched an Operational Technology Cybersecurity Center of Excellence (OTC CoE), a global platform to extend the boundaries of shared knowledge and facilitate multistakeholder collaboration to advance shared interests in OT cybersecurity.

Initiatives Platforms Centers Research & Studies Events

RESEARCH & STUDIES

GCF collaborates with stakeholders in industry and academia to publish world-leading primary research and studies on the most pressing issues in an evolving cyber landscape. This research is published under the Knowledge Hub on the GCF website.

EVENTS

GCF hosts a range of events to facilitate dialogue and advance collaboration among stakeholders involved in GCF activities, while convening leading speakers and experts from around the world to address strategic socioeconomic and geopolitical issues related to cybersecurity. Alongside the Annual Meeting, GCF delivers a wider program of events year-round, including its Meet GCF events in cities across the globe.

CHILD PROTECTION IN CYBERSPACE (CPC)

Almost all children are now active in Cyberspace and the risks they face are worsening:

93%

of children are online by the age of 12

81%

of children go online daily

72%

of children have experienced at least one cyber threat

Through the Child Protection in Cyberspace Initiative, instated by His Royal Highness Prince Mohammed bin Salman, GCF is taking action to ensure a safe and empowering Cyberspace for children around the world.

STRATEGIC OBJECTIVES:

- Strengthen collaboration
- Raise awareness and recognition
- Advance knowledge
- Develop cyber safety skills
- Enhance the global response

KEY TARGETS:

50+

countries with child protection frameworks developed

16M

people upskilled in child cyber safety

150M

children protected globally

At the 2024 Annual Meeting:

GCF signed collaboration agreements with UNICEF and DQ Institute to implement two new projects.

Protecting Children in Cyberspace Program

A new global program with UNICEF to contribute to fostering a safer digital environment for children.

5M

Parents and caregivers upskilled and educated on child cyber safety

30+ countries

Support provided to strengthen child helplines globally

Collaboration Agreement
Between
Global Cybersecurity Forum (GCF)
And
United Nations Children's Fund (UNICEF)
unicef
GLOBAL CYBERSECURITY FORUM

CPC Index

GCF and DQ Institute will develop the world's most comprehensive index on child protection in Cyberspace.

100+ countries

National-level data on child safety from around the world

100+ programs

Registry of top digital citizenship and literacy programs worldwide

WOMEN EMPOWERMENT IN CYBERSECURITY (WEC)

Globally, the talent gap in cybersecurity is significant and continues to grow:

2.8M	24%	22%
current shortage of cybersecurity professionals globally	of today's cybersecurity workforce are women	of female STEM students say they could be interested in a career in cybersecurity

The WEC Initiative, instated by His Royal Highness Prince Mohammed bin Salman, aims to contribute to a safer, more resilient Cyberspace by bridging the global talent gap through efforts to upskill and empower more women in the sector.

STRATEGIC OBJECTIVES:

- Expand the pipeline of talent
- Raise awareness and recognition
- Advance women to leadership
- Recruit and upskill talent
- Retain middle managers

KEY TARGETS:

6M	4M	30K
women in STEM educated in cybersecurity	female students upskilled	women given access to mentorship

At the 2024 Annual Meeting:

GCF launched its Cyber Leadership Launchpad mentoring program for women in cybersecurity.

Cyber Leadership Launchpad

This mentoring program will:

- Accelerate and help aspiring and current women professionals in building and sustaining meaningful careers in cybersecurity.
- Deliver thought-provoking conversations with women thought leaders and decision makers.
- Provide real life best practices to sustain and advance their careers into leadership positions.

LAUNCH OF 'WOMEN LEADERSHIP IN CYBER' GLOBAL MENTORING PROGRAM
Doreen Bogdan-Martin
Secretary-General, ITU
Heidi Crebo-Rediker
Senior Fellow, Council on Foreign Relations
Joy Chik
President, Identity and Network Access, Microsoft

KNOWLEDGE COMMUNITIES

GCF Knowledge Communities are multistakeholder thought leadership and action-oriented groups, comprising a globally diverse group of entities with shared interests and concerns related to a given domain in Cybersecurity.

First established at GCF 2023 last November, more than 20 Knowledge Community meetings have since been held, facilitating collaboration between more than 80 organizations on critical sector issues and advancing knowledge through the publication of whitepapers and reports.

The GCF Annual Meeting 2024 provided a timely opportunity for the Knowledge Communities to reflect on recent achievements and chart a path forward for the year ahead, establishing key priorities and strategic action plans that will guide their future efforts.

SECURING INDUSTRIAL SYSTEMS FOR GLOBAL ENERGY SUPPLY KNOWLEDGE COMMUNITY

The Securing Industrial Systems for Global Energy Supply Knowledge Community, led by Aramco, brings together energy companies, technology providers, infrastructure operators, industrial manufacturers and other stakeholders, with the shared goal of fortifying the world's energy lifelines and ensuring a resilient and secure energy future for all.

Led by aramco

SECURING THE FUTURE OF URBAN LIVING KNOWLEDGE COMMUNITY

The Securing the Future of Urban Living Knowledge Community, led by NEOM, unites smart city stakeholders, global cybersecurity organizations, technology companies, think tanks, and academia, to collaborate and explore solutions that enable secure, resilient, and sustainable cognitive cities.

Led by NEOM نيوم

FUTURE OF CYBERSECURITY KNOWLEDGE COMMUNITY

The Future of Cybersecurity Knowledge Community, led by SITE, brings together global technology and cybersecurity companies, research centers and think tanks, and other stakeholders and institutions with an interest in addressing the opportunities and challenges impacting the future of cybersecurity.

Led by Site

SAFEGUARDING THE FUTURE NETWORKS & EMERGING TECHNOLOGIES KNOWLEDGE COMMUNITY

The Safeguarding the Future Networks & Emerging Technologies Knowledge Community, led by stc, brings together stakeholders including ICT providers, telecom companies, cybersecurity research organizations, infrastructure operators, think tanks, and academics, to promote secure ICT networks and emerging technologies.

Led by stc

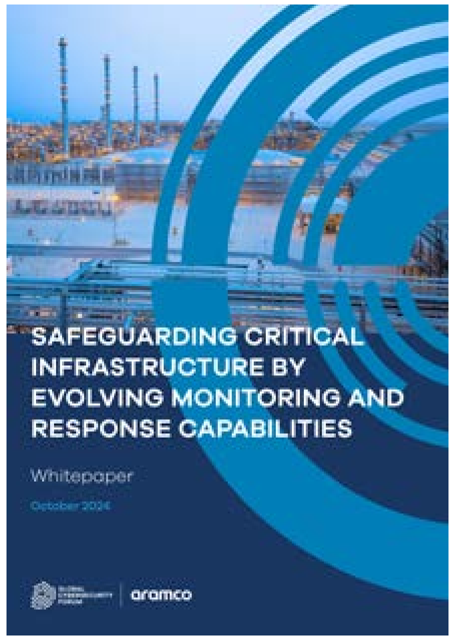
SECURING INDUSTRIAL SYSTEMS FOR GLOBAL ENERGY SUPPLY KNOWLEDGE COMMUNITY

This Knowledge Community is committed to fortifying the resilience and cybersecurity of the global energy supply chain. It works year-round in support of that goal, analyzing current and emerging threats, identifying frameworks for leveraging emerging technologies, and assessing potential modifications to policy and regulation to address risks and opportunities.

23	5
organizations represented	meetings in 2023/24

KNOWLEDGE COMMUNITY MEMBERS

aramco
Cyberani by aramco digital
Deloitte.
DRAGOS
EMERSON
SIEMENS energy
MOTIVA
Honeywell
YOKOGAWA
Schneider Electric
جامعة الملك عبدالله للعلوم والتقنية King Abdullah University of Science and Technology
جامعة الملك سعود King Saud University
KPMG
SLAC NATIONAL ACCELERATOR LABORATORY
شركة تنمية نفط عمان Petroleum Development Oman
PETRONAS
FURTINET
Shell
EY
KACST مدينة الملك عبدالعزيز للعلوم والتقنية
splunk> a cisco company
IBM



SAFEGUARDING CRITICAL INFRASTRUCTURE BY EVOLVING MONITORING AND RESPONSE CAPABILITIES

Whitepaper

October 2024

Global Cybersecurity Forum | aramco

This whitepaper examines how the global energy sector can ensure the secure operation of critical infrastructure amid rapid technological advancement.

SCAN HERE

SECURING THE FUTURE OF URBAN LIVING KNOWLEDGE COMMUNITY

This Knowledge Community is committed to building a more resilient, sustainable, and equitable urban future. Its members collaborate throughout the year, exploring the threats and vulnerabilities for urban living, conducting benchmarking of global cybersecurity practices, and assessing the impact of public-private sector practices on implementation of cybersecurity measures.

9	4
organizations represented	meetings in 2023/24

KNOWLEDGE COMMUNITY MEMBERS

NEOM نيوم

European Smart Cities Association

libelium

Smart City Cluster

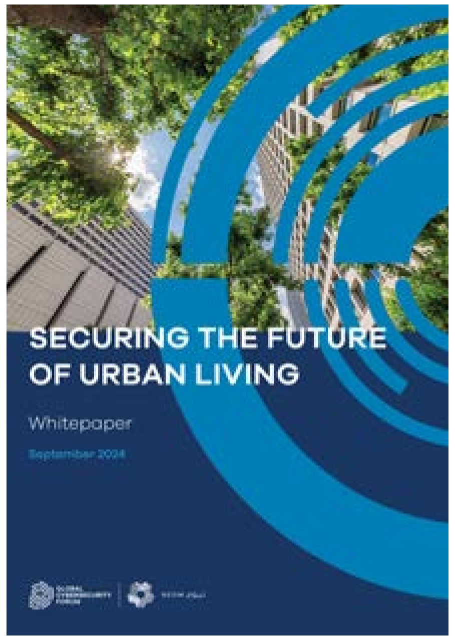
Syracuse University

IMD

SmartCitiesWorld

Swiss Cyber Institute

UNSW Sydney



SECURING THE FUTURE OF URBAN LIVING

Whitepaper

September 2024

This whitepaper explores the cybersecurity challenges and opportunities facing urban landscapes as they evolve from smart into cognitive cities.

SCAN HERE

FUTURE OF CYBERSECURITY KNOWLEDGE COMMUNITY

This Knowledge Community is committed to safeguarding the cyber realm in the face of ever-evolving cyber threats. As part of its year-round program of work, it is identifying forward-looking cybersecurity areas of foresight, undertaking forecasting on specific areas impacting cybersecurity, and conducting foresight exercises.

26	4
organizations represented	meetings in 2023/24

KNOWLEDGE COMMUNITY MEMBERS

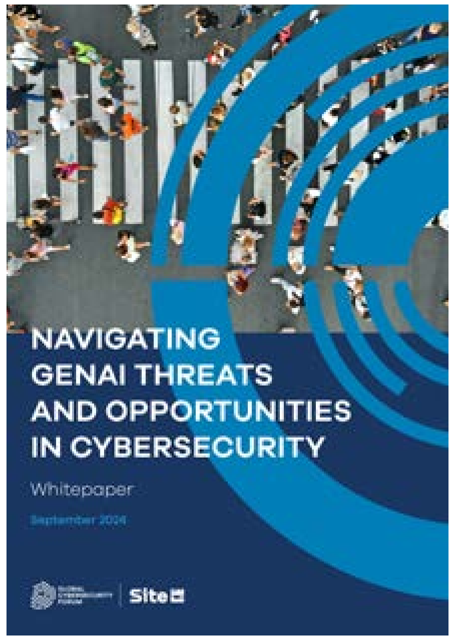
Site, BCG Boston Consulting Group, Chainalysis, CIPHER, Cisco, Fortinet

CrowdStrike, NTIS, CYBERCRYPT., CYBERNETICA, DRAGOS

IDQ, KACST, CYBER RANGES, (one) eSecurity, Privafy, pwc

SANS GIAC Certifications, Schneider Electric, sirar by stc, AXON, Trellix, TREND MICRO

CNTXT, UL, IBM



NAVIGATING GENAI THREATS AND OPPORTUNITIES IN CYBERSECURITY

Whitepaper

September 2024

Global Cybersecurity Forum | Site

This whitepaper explores the dual-edged nature of GenAI, proposing a roadmap for organizations to navigate threats and opportunities.

SCAN HERE

SAFEGUARDING THE FUTURE NETWORKS & EMERGING TECHNOLOGIES KNOWLEDGE COMMUNITY

This Knowledge Community is committed to promoting and safeguarding the current and future ICT networks. Meeting regularly throughout the year, it is assessing the potential impacts of emerging ICT technologies on the security of telecom networks, conducting benchmarking on industry standards, and defining models and frameworks for the resilience of telecom networks.

27	7
organizations represented	meetings in 2023/24

KNOWLEDGE COMMUNITY MEMBERS

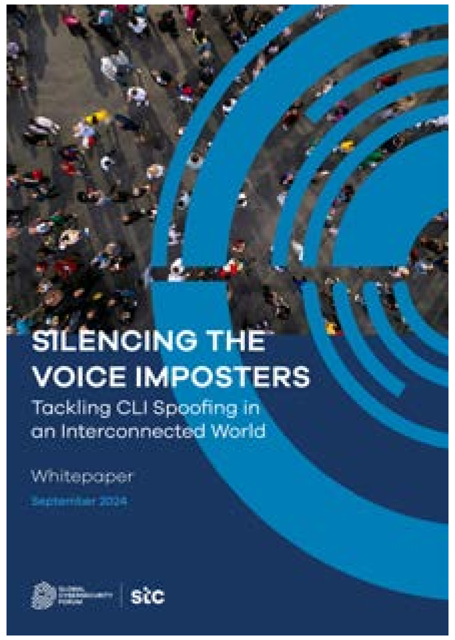
stc, accenture, Cellusys, ERICSSON, Deloitte.

ENEA, IMMERSIVELABS, JUNIPER NETWORKS, Google, mobileum

NETWITNESS, NOKIA, THALES, orange, paloalto NETWORKS

IBM, FORTINET, AUJAS CYBERSECURITY, CISCO, KPMG, HUAWEI

pwc, sirar by stc, splunk>, f5, academy from stc, ORACLE


SILENCING THE VOICE IMPOSTERS

Tackling CLI Spoofing in an Interconnected World

Whitepaper

September 2024

GLOBAL CYBERSECURITY FORUM | stc

This whitepaper assesses and proposes guidelines for the telecoms industry to address vulnerabilities and fortify networks against Caller Line Identification (CLI) spoofing.

SCAN HERE

OPERATIONAL TECHNOLOGY CYBERSECURITY CENTER OF EXCELLENCE

Launched in 2023, the Operational Technology Cybersecurity Center of Excellence (OTC CoE) is a global platform for knowledge sharing and multistakeholder collaboration, which brings together global thought leaders and industry pioneers to address the increasingly complex cybersecurity challenges associated with Operational Technology (OT).

Founding member

aramco

In collaboration with

NEOM نيوم

Site

سابك sabic

Honeywell

Schneider Electric

The OTC CoE aims to catalyze collaboration across the entire OT cybersecurity value chain and advance the maturity of global OT cybersecurity through:

1 **Capability development**

2 **Standardization and policy advocacy**

3 **Research and innovation**

4 **Thought leadership generation**

5 **Awareness raising**

ANNUAL MEETING & CENTER ACTIVATION

During the Annual Meeting 2024, the OTC CoE partners gathered to officially activate the Center and approve a detailed governance model for its operations. Capability development in OT cybersecurity was also discussed, with the Center aiming to develop academic partnerships and tailored programs to upskill the cybersecurity workforce and address the critical shortage of skilled professionals in this area.

Through its activities, which will include innovation and incubation initiatives, original publications, insights on technology and product development, upskilling programs, and multistakeholder events, the OTC CoE aims to ensure that critical infrastructures around the world are better secured against evolving threats.

The Center's activation phase will take place from 2024 to 2026, during which the focus will be on refining the Center's structure, membership model, and key activities.

CENTRE FOR CYBER ECONOMICS (CCE)

At the Annual Meeting, GCF announced its partnership with the World Economic Forum (WEF) to develop the Centre for Cyber Economics (CCE) – a global center which aims to enable economic stability and prosperity by advancing collaboration and knowledge sharing that contributes to enhancing global resilience against cyber threats.

GLOBAL CYBERSECURITY FORUM

WORLD ECONOMIC FORUM

CCE OBJECTIVES

- Advance knowledge on the economic dimension of cybersecurity
- Empower industries through collaboration and knowledge sharing
- Foster diversity in cybersecurity

2024 CYBERSECURITY WORKFORCE REPORT:
Bridging the Workforce Shortage and Skills Gap

GLOBAL CYBERSECURITY FORUM | BCG

2024 CYBERSECURITY WORKFORCE REPORT: BRIDGING THE WORKFORCE SHORTAGE AND SKILLS GAP

SCAN HERE

Released by GCF in partnership with Boston Consulting Group (BCG), the "2024 Cybersecurity Workforce Report" presents the results of research into the current state of the global cybersecurity workforce. The report highlights:

7.1 M
current size of the global cybersecurity workforce

2.8 M
global shortage of cybersecurity professionals

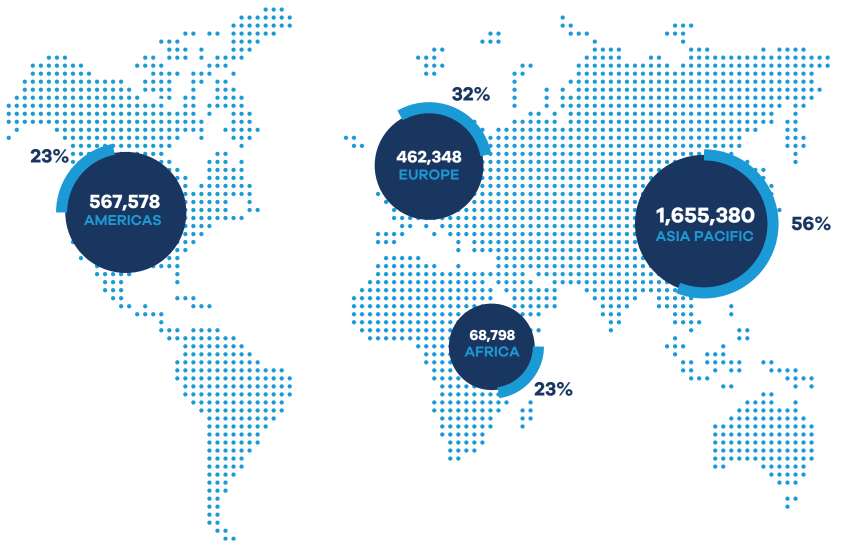
Less Than 4
professionals to fill every five cybersecurity jobs

Only 24%
of the cybersecurity workforce are women

64%
of the cybersecurity workforce shortage is concentrated across four industries: Tech, Financial Services, Consumer Goods, and Materials and Industrials

70%
of organizations use GenAI in their cybersecurity operations

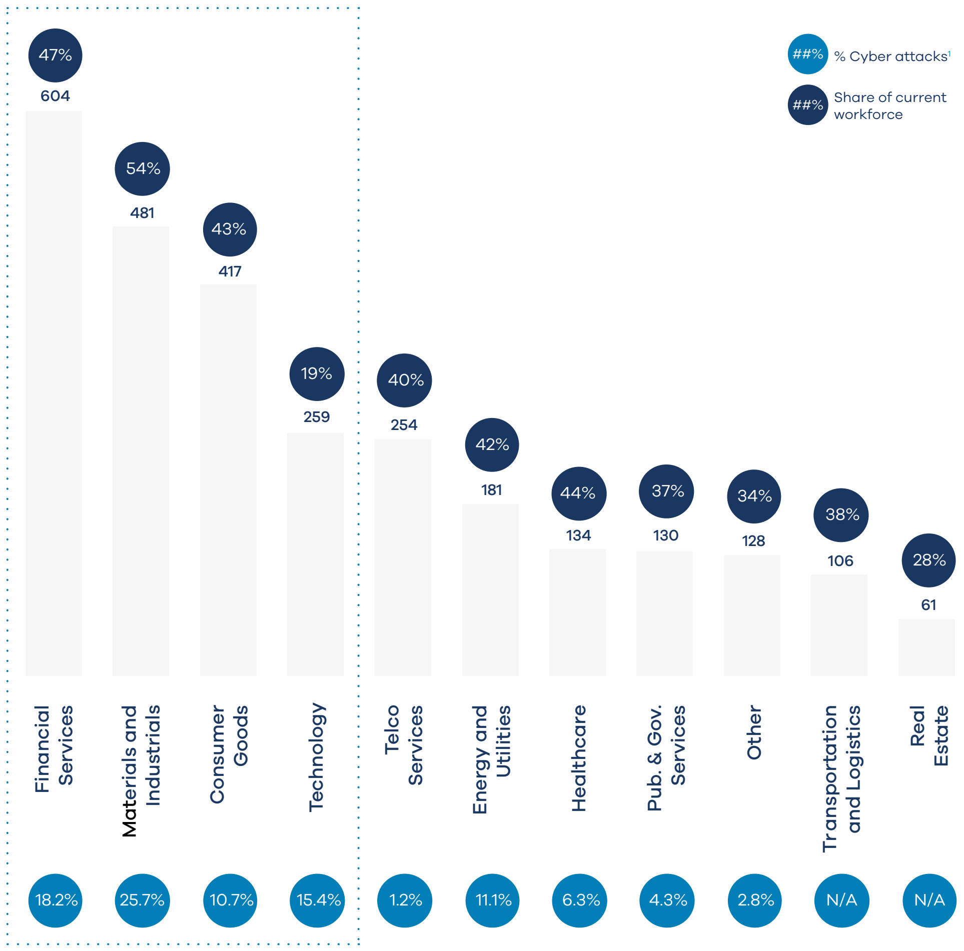
Regional view of current cybersecurity workforce shortage



🟦 Shortage as share of workforce

Source: Survey results

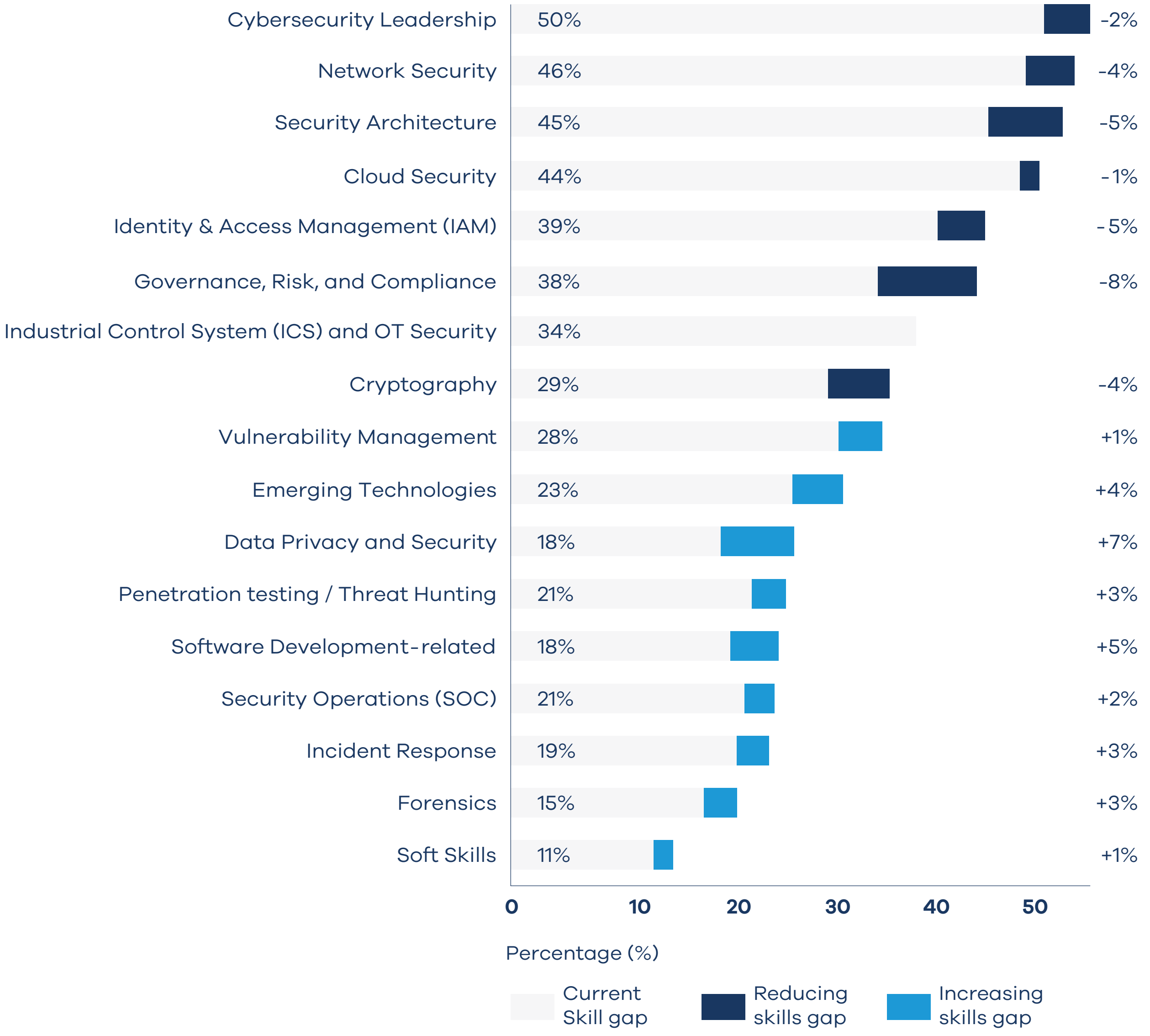
Shortage of cybersecurity workforce per industry



[1] Adapted from IBM

Source: IBM, Survey results

Expected skill gap change in 5 years



Source: Survey results

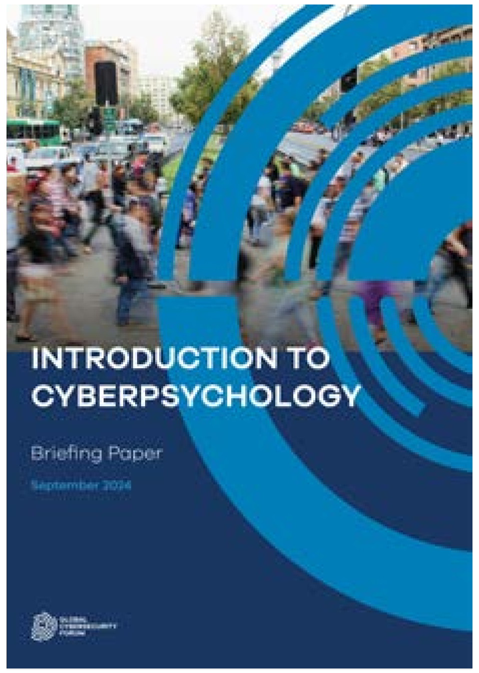
The report concludes with a set of recommended actions, anchored to the World Economic Forum's Cybersecurity Talent Framework:

Attracting talent into cybersecurity

Educating & training cybersecurity professionals

Retaining cybersecurity professionals

Recruiting the right cybersecurity talent



INTRODUCTION TO CYBERPSYCHOLOGY

SCAN HERE

DR. MARY AIKEN

Professor and Chair of the Cyberpsychology Department at Capitol Technology University

Authored by Dr. Mary Aiken, this briefing paper discusses the origins of cyberpsychology as a discipline, and the key concepts associated with the study of human behavior in cyber contexts.

Examining its applications in different sectors and industries reveals how cyberpsychology intersects with cybersecurity and safety, and can help us to understand human motivations, behaviors and cognitive processes that influence security outcomes, as part of fostering a safer Cyberspace.

BRIEFING PAPER CONTENTS

- Origins of cyber
- Psychology of Cyberspace
- Application of cyberpsychology
- Intersection of cybersecurity, cybercrime and cyber safety
- Future of cyberpsychology

GCF ANNUAL MEETING

Launched in 2020, the GCF Annual Meeting is a platform for multistakeholder dialogue on the most pressing priorities in Cyberspace. The event, held in Riyadh, Saudi Arabia, aims to catalyze action year-round, and offers the global cybersecurity community:

- A two-day program of substantive sessions with world-class speakers and experts
- Insights and perspectives from the foremost thought leaders in the sector
- Opportunities to network with global experts and decision makers

The GCF Annual Meeting 2024 built on the strong foundations established by GCF 2022, 'Rethinking the Global Cyber Order' and GCF 2023, 'Charting Shared Priorities in Cyberspace,' to address the theme of 'Advancing Collective Action in Cyberspace.' GCF looks forward to welcoming participants from around the world to our next Annual Meeting in Riyadh on October 1st-2nd, 2025.

CHILD PROTECTION IN CYBERSPACE (CPC) GLOBAL SUMMIT

In conjunction with the Annual Meeting 2024, GCF held the first Child Protection in Cyberspace (CPC) Global Summit in Riyadh in collaboration with the International Telecommunication Union (ITU), United Nations Children's Fund (UNICEF), DQ Institute, and WeProtect Global Alliance.

The summit convened key stakeholders from around the world to identify pathways for collaboration and collective action towards safeguarding children in Cyberspace. Participants established key recommendations for collective action on child cyber safety, with a view to sustaining action beyond the event.

MEET GCF

Meet GCF events are being held in cities across the world, raising awareness of GCF and convening global stakeholders to work collaboratively to address key cybersecurity topics.

Events in 2024

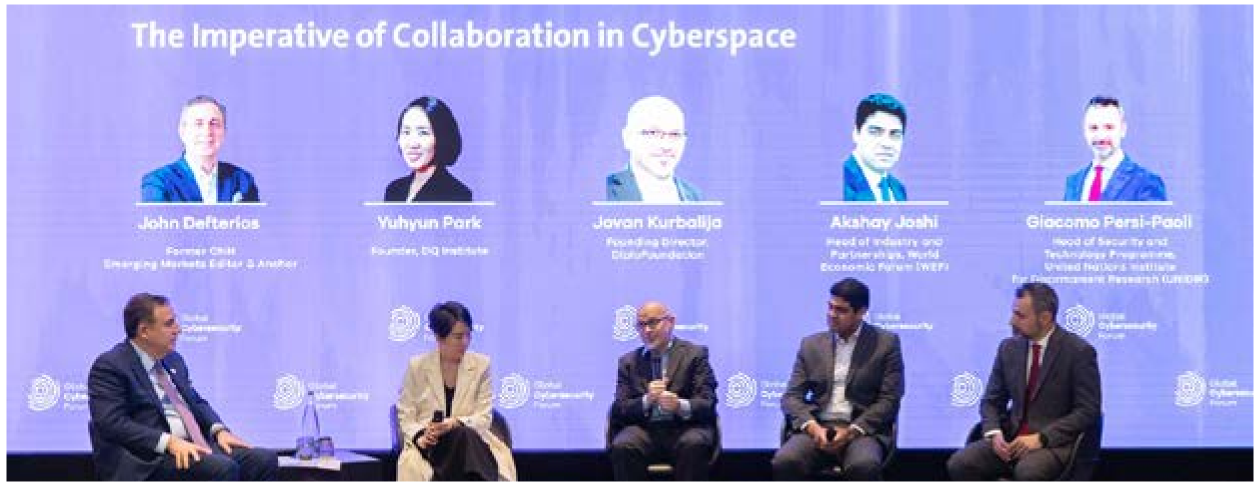
Geneva, Switzerland

- Co-hosted with Saudi Arabia's Permanent Mission to the UN
- Attended by diplomats, policymakers, experts, and NGO and IGO representatives
- Panel discussion held on 'Securing Tomorrow: The Imperative of Collaboration in Cyberspace'

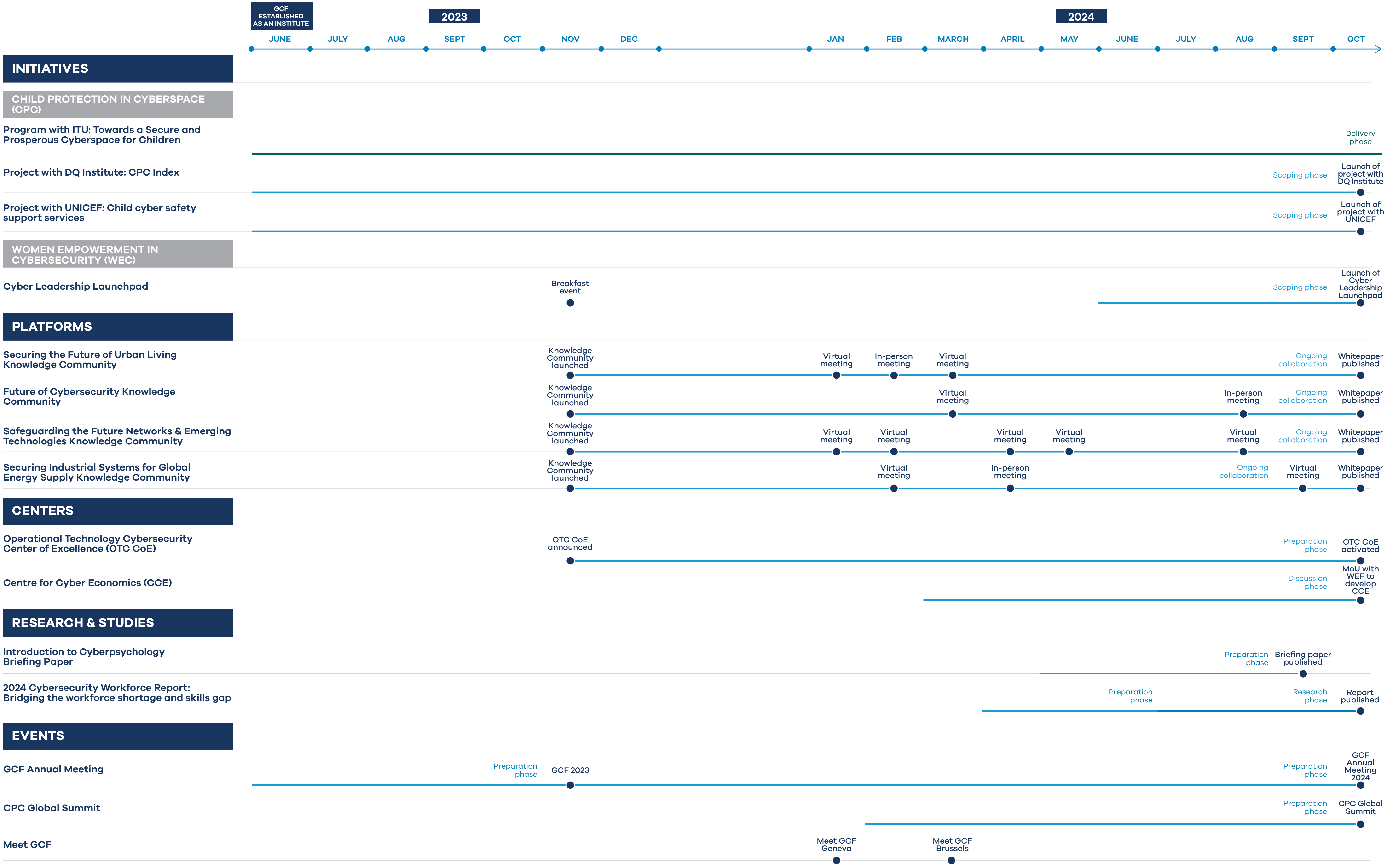
Brussels, Belgium

- Co-hosted with Saudi Arabia's Mission to the European Union
- Attended by representatives from government, the private sector, IGOs, NGOs, and academia
- Panel discussion held on 'Collaborative Pathways: Transforming Cybersecurity Challenges into Strategic Opportunities'.

Meet GCF is coming to new cities around the world in 2025.


The Imperative of Collaboration in Cyberspace
John Defterios
Former CNN Emerging Markets Editor & Anchor
Yuhyun Park
Founder, DQ Institute
Jovan Kurbalija
Founding Director, DiploFoundation
Akshay Joshi
Head of Industry and Partnerships, World Economic Forum (WEF)
Giacomo Persi-Paoli
Head of Security and Technology Programme, United Nations Institute for Disarmament Research (UNIDIR)

GCF ACTIVITIES TIMELINE 2023/24



GCF ESTABLISHED AS AN INSTITUTE

2023

JUNE JULY AUG SEPT OCT NOV DEC

2024

JAN FEB MARCH APRIL MAY JUNE JULY AUG SEPT OCT

INITIATIVES

CHILD PROTECTION IN CYBERSPACE (CPC)

Program with ITU: Towards a Secure and Prosperous Cyberspace for Children

Delivery phase

Project with DQ Institute: CPC Index

Scoping phase

Launch of project with DQ Institute

Project with UNICEF: Child cyber safety support services

Scoping phase

Launch of project with UNICEF

WOMEN EMPOWERMENT IN CYBERSECURITY (WEC)

Cyber Leadership Launchpad

Breakfast event

Scoping phase

Launch of Cyber Leadership Launchpad

PLATFORMS

Securing the Future of Urban Living Knowledge Community

Knowledge Community launched

Virtual meeting

In-person meeting

Virtual meeting

Ongoing collaboration

Whitepaper published

Future of Cybersecurity Knowledge Community

Knowledge Community launched

Virtual meeting

In-person meeting

Ongoing collaboration

Whitepaper published

Safeguarding the Future Networks & Emerging Technologies Knowledge Community

Knowledge Community launched

Virtual meeting

Virtual meeting

Virtual meeting

Virtual meeting

Virtual meeting

Ongoing collaboration

Whitepaper published

Securing Industrial Systems for Global Energy Supply Knowledge Community

Knowledge Community launched

Virtual meeting

In-person meeting

Ongoing collaboration

Virtual meeting

Whitepaper published

CENTERS

Operational Technology Cybersecurity Center of Excellence (OTC CoE)

OTC CoE announced

Preparation phase

OTC CoE activated

Centre for Cyber Economics (CCE)

Discussion phase

MoU with WEF to develop CCE

RESEARCH & STUDIES

Introduction to Cyberpsychology Briefing Paper

Preparation phase

Briefing paper published

2024 Cybersecurity Workforce Report: Bridging the workforce shortage and skills gap

Preparation phase

Research phase

Report published

EVENTS

GCF Annual Meeting

Preparation phase

GCF 2023

Preparation phase

GCF Annual Meeting 2024

CPC Global Summit

Preparation phase

CPC Global Summit

Meet GCF

Meet GCF Geneva

Meet GCF Brussels

05

CONCLUSION

CONCLUSION

This book summarizes the key outcomes of the GCF Annual Meeting 2024 and first ever Child Protection in Cyberspace (CPC) Global Summit, while also reflecting on GCF's year-round efforts to advance purpose-driven dialogue, impactful initiatives, and collaborative priorities among the global Cyberspace community.

From engaging dialogue to action-oriented discussions, the Annual Meeting 2024 and CPC Global Summit brought together participants from a varied range of perspectives and backgrounds, including government, the private sector, international organizations and academia, setting out to drive forward collective action and strengthen cybersecurity efforts across borders and sectors.

Discussions brought to the fore the need for multistakeholder collaboration to address challenges and harness opportunities across the social, economic, geopolitical, and behavioral dimensions of Cyberspace. Speakers reinforced the opening message from His Royal Highness Prince Mohammed bin Salman bin Abdulaziz, Crown Prince and Prime Minister of Saudi Arabia, agreeing on the need to prioritize a safe, empowering Cyberspace, particularly for vulnerable groups, such as children, while strengthening collective resilience and balancing the vast opportunities created by emerging technologies with responsible innovation.

Key outcomes of the Annual Meeting included the launch of new strategic projects under GCF's leadership. The projects will focus on enhancing knowledge on the economic dimensions of Cyberspace, closing the cybersecurity skills gap, advancing mentorship and capacity building to empower more women in the sector, and ensuring that Cyberspace is safe for children. The new projects will continue driving impactful collaboration with GCF's various partners in the months ahead, while also advancing the goals of GCF's two global initiatives - Child Protection in Cyberspace (CPC) and Women Empowerment in Cybersecurity (WEC).

Both form part of GCF's year-round program of activities beyond the Annual Meeting and reflect GCF's mission to strengthen Cyberspace safety and resilience for all nations and economies, championing actions that address the most pressing challenges while maximizing the opportunities in Cyberspace. This includes the work of GCF's four Knowledge Communities, which guide collaboration between globally diverse organizations; GCF's specialized centers, including the Operational Technology Cybersecurity Center of Excellence activated during the Annual Meeting 2024, and the new Centre for Cyber Economics; the evidence-driven research and studies published by GCF; as well as events which gather stakeholders in cybersecurity hubs all around the world throughout the year.

Through these activities, carried out in collaboration with local and international partners, GCF is committed to its mandate as a global platform for action-oriented collaboration in line with its strategic goals:

- Advancing dialogue and pushing knowledge boundaries
- Driving social impact and opportunities for investment
- Integrating cybersecurity stakeholders as a single global community

GCF extends thanks and utmost appreciation to its esteemed partners, who have been integral to the GCF journey and share a vision to strengthen Cyberspace safety and resilience. GCF looks forward to building on these accomplishments to advance global development and prosperity for all.

GLOBAL
CYBERSECURITY
FORUM