GLOBAL
CYBERSECURITY
FORUM

ANNUAL MEETING
1-2 OCTOBER 2025

SCALING COHESIVE ADVANCEMENT IN CYBERSPACE

Riyadh, 1-2 October

Preliminary Program

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, society, 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.**

This preliminary program provides an initial set of topics corresponding to the GCF Annual Meeting 2025 theme and its five sub-themes. As such, it serves as a general guide to the final program for the GCF Annual Meeting 2025.

GCF ANNUAL MEETING 2025

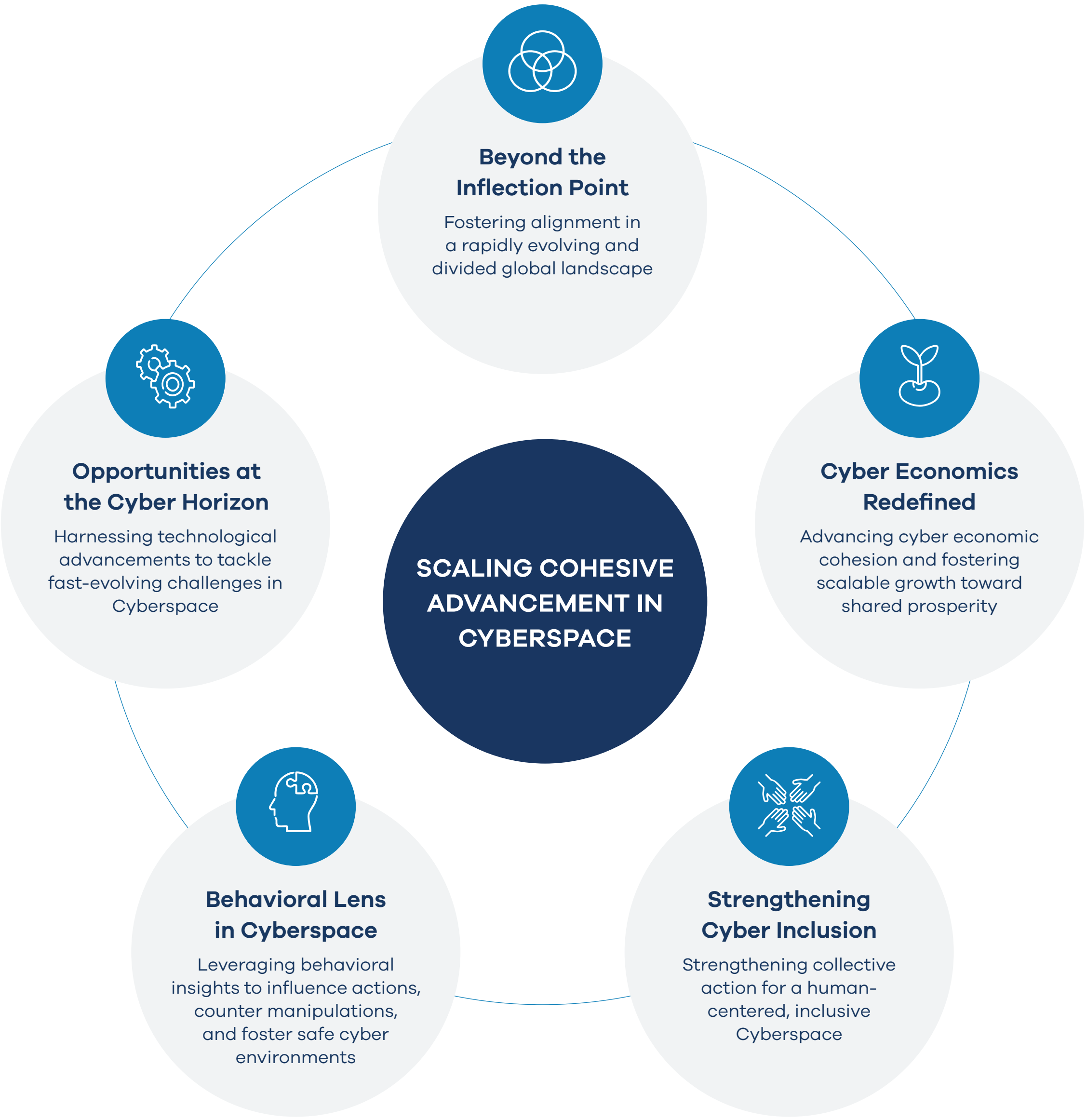
Scaling Cohesive Advancement in Cyberspace

The Ritz-Carlton, Riyadh **1-2 October**

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 global challenges and opportunities in Cyberspace.

The GCF 2023 theme of "Charting Shared Priorities in Cyberspace" built upon the conceptual foundation set by the 2022 theme of "Rethinking the Global Cyber Order." The 2024 edition continued this narrative movement to drive substantive action under the theme "Advancing Collective Action in Cyberspace." This year, the Annual Meeting aims to scale the cohesive advancements accomplished by the GCF community, with the aim of elevating their scope, capacity, and impact to advance a more secure and resilient Cyberspace for all.

The program for the GCF Annual Meeting 2025 will be structured around five main sub-themes:



SCALING COHESIVE ADVANCEMENT IN CYBERSPACE

Beyond the Inflection Point
Fostering alignment in a rapidly evolving and divided global landscape

Cyber Economics Redefined
Advancing cyber economic cohesion and fostering scalable growth toward shared prosperity

Strengthening Cyber Inclusion
Strengthening collective action for a human-centered, inclusive Cyberspace

Behavioral Lens in Cyberspace
Leveraging behavioral insights to influence actions, counter manipulations, and foster safe cyber environments

Opportunities at the Cyber Horizon
Harnessing technological advancements to tackle fast-evolving challenges in Cyberspace

BEYOND THE INFLECTION POINT

Fostering alignment in a rapidly evolving and divided global landscape

Amid an increasingly dynamic and divided global landscape, geopolitical tensions and technological advancements are reshaping the foundations of international cooperation. Nearly 60% of organizations state that geopolitical tensions have affected their cybersecurity strategy. Rapid technological transformation, coupled with shifting power dynamics and fragmented policy approaches, has created both challenges and opportunities for greater global alignment. At the same time, increased cyber resilience and strengthened governance have become more critical than ever, requiring innovative strategies to bridge divides and strengthen cross-border collaboration.

New Pathways for Global Cyber Resilience

The known number of cyberattacks has increased by approximately 75% over the past five years. As cyber threats continue to evolve, there is an opportunity to explore how broader and deeper collaboration—including among governments, the private sector, and other stakeholders—can complement and strengthen existing multilateral efforts.

How can nations and organizations across the private sector and civil society, in partnership with other stakeholders, advance global cyber resilience and foster trust through more inclusive cooperation?

Scaling Critical Infrastructure Protection in Cyberspace

Between January 2023 and January 2024, critical infrastructure worldwide sustained over 420 million cyberattacks – equivalent to 13 attacks per second. These attacks targeted essential services, including energy grids, healthcare systems, and financial institutions.

How can nations, critical infrastructure operators, and other private sector entities scale their cooperation to protect critical infrastructure from cyberattacks, particularly during times of conflict?

Global View: A Leading Country's Path to Cyber Resilience

Certain nations—beyond traditional great powers—have distinguished themselves as global leaders in cybersecurity, setting global benchmarks for cyber resilience by integrating public-private partnerships, national cybersecurity strategies, and cutting-edge research.

How does a nation emerge as a global cybersecurity leader across areas including cyber defense, threat intelligence, infrastructure security, and workforce development?

Reinventing Consensus in a Fragmented World

Recent successful multilateral efforts, such as the Convention on Cybercrime (ratified by 78 countries as of 2025) demonstrate that diplomatic mechanisms can provide effective channels for fostering cross-border cooperation and trust. Amid increasing fragmentation and division, achieving consensus in cyber diplomacy is more important than ever.

How can these success stories inform the future strategies of intergovernmental organizations, nations, and cybersecurity agencies as they seek to advance global cyber governance?

Supply Chain Cybersecurity in a Fragmenting Economy

Supply chain vulnerabilities are the primary barrier to cyber resilience for 54% of large organizations. Global manufacturing, energy, and consumer goods supply chains remain highly vulnerable due to ransomware, third-party vulnerabilities, and the increasingly interconnected nature of logistics and operations.

In what ways can greater international cooperation enhance supply chain resilience, mitigate cyber risks from protectionist policies, and foster alignment on security standards for networks critical to global commerce?

CYBER ECONOMICS REDEFINED

Advancing cyber economic cohesion and fostering scalable growth toward shared prosperity

As the cyber landscape evolves, its economic implications are becoming more profound, influencing everything from investment strategies to global stability. Rising cyber threats continue to reshape risk calculations, prompting organizations to reassess financial exposure and resilience. The economics of cybercrime remain a pressing challenge, with regulatory gaps and cross-border enforcement shaping the financial calculus of attackers. Meanwhile, the cybersecurity talent gap, particularly the underrepresentation of women, presents an opportunity to drive innovation and competitiveness.

Rethinking Cybersecurity as an Economic Imperative

As cyber threats grow in scale and sophistication, global spending on cybersecurity is projected to reach USD 400 billion by 2030. Yet, cybersecurity is often viewed as a technical challenge rather than an economic imperative. Exploring the broader financial implications of cyber risk—including financial losses, regulatory penalties, and reputational damage—can help highlight its significance as an economic imperative.

How can organizations strike the right balance between investment and resilience? What strategies ensure that cybersecurity budgets are spent wisely, maximizing protection without compromising growth?

Insuring an Era of Unpredictable Cyber Threats

As cyber threats evolve, businesses face mounting financial and operational risks, yet the role of cyber insurance in mitigating these risks remains complex. The cyber insurance market reached USD 14 billion in value in 2023 and is projected to double to USD 29 billion by 2027, reflecting its growing importance. However, a critical gap remains—87% of companies still lack coverage, leaving them vulnerable to devastating cyber incidents. Shifting policy limitations, pricing trends, and the challenges of underwriting an ever-changing threat landscape raise questions about its effectiveness as a risk management tool.

How can cyber insurance be structured to provide meaningful protection while keeping pace with emerging threats?

Unlocking the Economic Power of Women in Cybersecurity

With only 72% of cybersecurity roles filled and women representing just 24% of the workforce, the sector faces an urgent challenge in building a future-ready workforce. Closing the gender gap in cybersecurity is not just a matter of equity—it's an economic necessity. Greater diversity has been linked to stronger innovation, resilience, and problem-solving, yet barriers to entry and advancement persist, from limited access to STEM education to workplace cultures that hinder inclusion.

How can targeted investments in education, mentorship, and inclusive policies unlock the full potential of women in cybersecurity and drive global economic growth?

Disrupting the Cybercrime Economy by Shifting Incentives

Cybercrime thrives on financial gain, exploiting gaps in regulation, enforcement, and cross-border coordination. With global cybercrime damages estimated to reach USD 10.5 trillion in 2025, the financial incentives fueling cyberattacks are staggering. In this context, governments, businesses, and law enforcement agencies can consider new collaborative approaches to disrupt cybercriminal operations, increase penalties for perpetrators, and reduce the profitability of cybercrime.

How can the financial calculus of cybercrime be reshaped to turn the tide in this ongoing battle?

Cyber Investments Shaping the Next Decade of Security

With 76% of global CEOs agreeing that cybercrime and insecurity will negatively impact their organization's prosperity over the next three years, the urgency for stronger cybersecurity investment has never been clearer. There are a number of potential collaborative avenues to advance cyber innovation by bringing together governments, private investors, and technology leaders to reduce risk and expand funding opportunities.

What are the most productive pathways for governments, cybersecurity providers, and small and medium-sized enterprises (SMEs) to collaborate strategically, accelerate investment, and support long-term growth?

Bracing for an Era of Quantum-driven Economic Transformation

Quantum computing is poised to redefine cybersecurity, challenging existing encryption methods while introducing new opportunities for defense. With the global quantum computing market projected to grow from USD 1.16 billion in 2024 to USD 12.62 billion by 2032, at a CAGR of 34.8%, its rapid expansion will reshape the cybersecurity landscape. As this technology advances, the economic dynamics of cybersecurity will shift, influencing everything from risk exposure to investment strategies.

How can governments and private sector organizations mitigate financial risks and leverage quantum-driven innovations to stay ahead in an evolving threat landscape?

STRENGTHENING CYBER INCLUSION

Strengthening collective action for a human-centered and inclusive Cyberspace

As technologies continue to shape societies worldwide, the challenge of ensuring an inclusive and human-centered Cyberspace grows more urgent. Vulnerable populations—including children, the elderly, and those in developing nations—face heightened cyber risks. At the same time, accessibility barriers persist, preventing millions from enjoying the full benefits of Cyberspace. Through concerted, collective action between governments, industry leaders, educators, and civil society, the global community has an opportunity to scale cyber inclusion efforts and build a more secure and equitable online environment for all.

Reimagining Online Safety for the Next Generation

72% of children below age 12 on social media have experienced a cyber threat, and 48% feel unsafe online. As online platforms become increasingly central to education, socialization, and entertainment, children remain particularly vulnerable to risks such as cyberbullying, exploitation, and data privacy breaches.

How can governments, the private sector, educators, and civil society scale cyber inclusion initiatives that protect children, foster cyber literacy, and create a safer, more inclusive online environment?

Driving Systemic Inclusion through Cybersecurity Solutions

Across a sample of one million home pages hosted on the global internet, 56,791,260 distinct accessibility errors were detected—an average of 56.8 errors per page. As a result, disabled people are over 50% more likely to face internet access barriers than non-disabled people.

In what ways can inclusive design increasingly meet the diverse needs of all users, including the disabled?

Bolstering Cyber Capacity for Inclusive Security in LDCs

ITU cybersecurity capacity scores for the highest income countries are more than four times better than those of least developed countries (LDCs), and malware infection rates in high income countries are four to five times lower than those in LDCs. Many LDCs face significant barriers to building robust cybersecurity frameworks, including limited technical expertise, resource constraints, and gaps in policy implementation. Collaborative efforts can help bridge these gaps and create a more resilient global cyber ecosystem.

How can governments, the private sector, and international organizations work together to scale capacity-building initiatives and ensure all nations, including LDCs, have the tools needed to strengthen cybersecurity resilience?

Engineering Security to Think Like Humans, Not Hackers

Around 85% of people reported encountering an online scam attempt in 2023, underscoring the ongoing threat of phishing, fraud, and deception. While traditional cybersecurity measures play a crucial role, many approaches rely heavily on users to identify and prevent threats. There is growing interest in security solutions that better align with human behavior, making protection more intuitive and effective.

In what ways can cybersecurity be designed to complement human behavior rather than work against it?

Adopting Proactive Protection for Seniors in Cyberspace

Older internet users are almost twice as likely to be targeted by phishing attacks than younger users (53.46% compared to 26.37%). As the global population ages, there is a clear opportunity to explore new ways in which cybersecurity strategies can be adapted to protect senior users from scams, identity theft, and online fraud.

What are the most promising pathways of collaborative action to enhance protections for seniors in Cyberspace?

BEHAVIORAL LENS IN CYBERSPACE

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

As online interactions increasingly shape society, the intersection of human behavior and cybersecurity has never been more critical. Improving trust requires a deep understanding of psychological vulnerabilities, behavioral science, and the impact of Cyberspace on decision-making. From designing intuitive security measures that empower safe behavior to leveraging gamification for engagement, human-centered strategies play a decisive role in fostering cyber resilience.

Restoring Human Resilience and Trust in Cyberspace

In an era of evolving cyber threats and shifting media landscapes, strengthening trust in Cyberspace is of paramount importance. In an era of misinformation, manipulation, and cyber threats, trust in Cyberspace is more fragile than ever. Organized online manipulation campaigns have been detected in 81 surveyed countries and, worse, misinformation has become a common communication strategy, with 93% of these countries witnessing its use. Understanding human psychology is key to rebuilding confidence and societal resilience. By leveraging behavioral insights, leaders can increase their organizations' cyber awareness, foster critical thinking, and promote responsible online behavior in Cyberspace.

What are the most productive pathways of shaping a more secure and trustworthy online world in order to safeguard human resilience?

Shaping Healthier Decision-Making and Well-Being Online

While Cyberspace is supporting the growth of new communities and social interaction, frequent exposure to social media has been positively associated with a higher risk of a combination between depression and anxiety. From disinhibition to cyberchondria, online interactions are reshaping how people think, feel, and behave. The subconscious effects of prolonged internet exposure influence everything from decision-making to emotional well-being, raising critical questions about the psychological impact of technology.

What strategies are required for individuals and societies to collectively cultivate healthier habits online?

Designing Security to Fit into Daily Life

Security should work for people, not against them. When cybersecurity measures are cumbersome or unintuitive, users often bypass them—a reality acknowledged by 65% of office workers who admit to circumventing company security measures, often without realizing the potential consequences. Identifying new ways to seamlessly integrate security into workflows without disrupting productivity can help increase both efficiency and security.

How can we create intuitive, human-centered security systems that integrate easily into daily workflows and empower users to protect themselves effortlessly?

Turning the Human Factor into Cybersecurity's Strongest Defense

Cybercriminals don't just exploit technology—they exploit people. Estimates suggest that 84% to 98% of cyber hacks rely on exploiting psychological vulnerabilities rather than technical flaws, highlighting the critical role of human behavior in cybersecurity breaches. By leveraging cognitive biases and social engineering tactics, attackers manipulate human behavior to bypass even the strongest security measures. Understanding these psychological vulnerabilities is key to designing more effective cybersecurity awareness programs, improving trust, and preventing human-targeted attacks.

How can behavioral science be applied to turn people, rather than technology, into the first line of defense?

Gamifying Cybersecurity to Build a More Resilient Workforce

Engagement is the key to effective learning, and gamification is transforming how individuals develop cyber skills and threat awareness. Gamified cybersecurity awareness programs have been shown to boost employee engagement by 60% and productivity by 43%, making them a powerful tool for improving cyber resilience. From Capture-the-Flag (CTF) competitions to interactive simulations, competition is proving to be an effective method for increasing the effectiveness of cybersecurity education.

How can organizations, educators, and security professionals harness gaming mechanics to develop a more cyber-resilient workforce?

Redefining Online Identity to Secure Privacy and Build Trust

86% of internet users have tried to be anonymous online and taken at least one step to try to mask their behavior or avoid being tracked. In an era where online interactions shape personal and professional lives, managing online identities is more complex than ever. While anonymity can foster free expression, it also enables identity fraud, misinformation, and security risks. Innovations in identity verification, behavioral biometrics, and authentication technologies are redefining how trust is built in Cyberspace.

How can governments and private sector entities alike balance user autonomy and privacy with security?

OPPORTUNITIES AT THE CYBER HORIZON

Harnessing technological advancements to tackle fast-evolving challenges in Cyberspace

While innovations such as artificial intelligence (AI), blockchain, and autonomous security systems offer powerful tools to advance cyber resilience, they also introduce new vulnerabilities that can be exploited by cybercriminals and state actors. Global cybercrime is projected to cost USD 10.5 trillion annually in 2025, underscoring the urgent need to advance proactive and adaptive security measures. Additionally, as AI-driven cyber threats become more sophisticated, 70% of Chief Information Security Officers (CISOs) believe AI currently gives an advantage to attackers over defenders. From safeguarding healthcare systems against ransomware to securing the expanding cyber frontier in space, governments, businesses, and technology, leaders must harness innovations while mitigating emerging risks. The challenge ahead is to strike a balance between rapid technological progress and responsible governance, ensuring that Cyberspace remains a secure and resilient domain for all.

Transforming Tech Disruption into a Cybersecurity Advantage

A recent survey of Chief Information Security Officers (CISOs) found that 70% believe that AI gives an advantage to attackers over defenders. However, AI and automation also have the potential to revolutionize cybersecurity defenses, enabling real-time threat detection, automated incident response, and predictive risk modeling.

How can governments, businesses, and tech leaders turn disruptive innovation into smarter, faster, and more adaptive cyber resilience?

Weighing the Ethics of Autonomous Cyber Defenders

Emerging technologies are increasingly making autonomous cybersecurity decisions. In 2024, over two-thirds of IT and security professionals worldwide had already tested AI capabilities for security, while 27% were planning to do so.

What are some potential frameworks for governing emerging tech-powered cybersecurity while maintaining transparency, trust, and ethical integrity?

Blockchain’s Billion-Dollar Potential to Reinvent Cybersecurity

Blockchain technology is transforming cybersecurity by enhancing transparency, data integrity, and financial security. In the finance sector alone, blockchain implementation could save companies at least USD 12 billion annually, with banks reducing infrastructure costs by 30%.

How can governments and organizations leverage blockchain technology to increase transparency, secure financial systems, and build trust across borders?

Shaping the Future of Cyber Threat Intelligence in Healthcare

36% of healthcare facilities reported increased medical complications due to ransomware attacks in 2024, as cybercriminals increasingly target hospitals, clinics, and medical research institutions. Disruptions to patient data access, medical devices, and critical systems can lead to life-threatening consequences.

What are the most productive, collaborative pathways of scaling cybersecurity intelligence to identify threats in the healthcare sector?

Balancing Security and Sustainability for Data and the Planet

By 2030, AI could account for up to 3.5% of global electricity consumption — twice the energy demand of France. While cybersecurity infrastructure is essential for protecting data, its environmental impact cannot be ignored.

How can governments and private sector actors collectively advance innovative approaches that balance security, performance, and sustainability in the era of AI?

Strengthening Global Strategies for Securing Space Assets

Today, space systems play an increasingly critical role for our national security, economy, and way of life. The global space economy was valued at USD 630 billion in 2023, with estimated growth to USD 1.8 trillion by 2035. As reliance on space technology grows, so do threats from cyberattacks on satellite networks, GPS spoofing, and the misuse of space-based infrastructure.

How can international collaboration and technological innovations in space be harnessed to secure critical space assets, foster global policy alignment, and protect our expanding cyber frontier?

PARTICIPATORY TRACK

In addition to discussions oriented around the five GCF Annual Meeting 2025 sub-themes, collaborative dialogue will also take place during high-level roundtables and across several areas of cohesive advancement:

HIGH-LEVEL ROUNDTABLES

Cyber CxO Meeting

The Cyber CxO Meeting, established to convene each year at the GCF Annual Meeting, leverages GCF's unique value and global reach to bring together the C-suite of globally reputed companies. Representatives discuss challenges and emerging trends in cybersecurity, implications for private sector entities, and productive pathways for collaborative action.

Cyber Chiefs Roundtable

The Cyber Chiefs Roundtable was established to convene senior-level representatives of national government cyber authorities to share perspectives, discuss key cybersecurity challenges, and explore productive pathways for addressing them.

Other invite-only roundtables and meetings will include:

GCF Knowledge Communities

GCF Impact Network

Centre for Cyber Economics (CCE)

OT Cybersecurity Center of Excellence (OTC-CoE)

AREAS OF COHESIVE ADVANCEMENT

Child Protection in Cyberspace (CPC)

GCF is committed to creating a safer and more inclusive online environment for children by addressing cyber risks and empowering young users. Through multistakeholder collaboration, GCF is working to enhance online safety, online literacy, and policy frameworks. Primary focus areas include advancing a secure and beneficial Cyberspace for children, driving progress on the Child Protection in Cyberspace Index, and Gaming for Good.

Capability Building for Cyber Resilience

GCF is dedicated to improving global cybersecurity capacity by addressing critical capability gaps through a collaborative, multistakeholder approach. By leveraging expertise from UN entities, governments, the private sector, and cybersecurity organizations, GCF aims to strengthen cyber resilience through targeted training, knowledge-sharing, and technical assistance programs.

Cybersecurity in Healthcare

With the increasing interconnectedness of healthcare systems, GCF seeks to fortify the cybersecurity posture of the sector to protect patient data, medical devices, and healthcare infrastructure from cyber threats. By advancing security frameworks, incident response mechanisms, and industry-wide collaboration, GCF is prioritizing enhancing the resilience of healthcare institutions against cyberattacks.

Cyberpsychology

GCF seeks to explore the intersection of human behavior and cybersecurity, examining how online environments influence individuals' actions, mental health, and decision-making. By understanding the psychological factors behind cyber threats—such as social engineering, manipulation, and online addiction—GCF aims to inform policy development and awareness campaigns that promote safer online behaviors.

Women Empowerment in Cybersecurity (WEC)

GCF seeks to bridge the global talent gap in cybersecurity by fostering gender inclusion, professional development, and leadership opportunities for women. By equipping women with the necessary skills and resources, GCF aims to strengthen cyber resilience, innovation, and economic growth.

Protection of Critical Infrastructure

GCF aims to safeguard essential services and assets—such as energy, transportation, finance, and communications—from cyber threats. By promoting best practices, developing risk mitigation strategies, and fostering cross-sector collaboration, GCF aims to ensure that critical infrastructure remains resilient against emerging cyber risks.

Cyber Diplomacy

GCF's focus on cyber diplomacy aims to foster international cooperation, dialogue, and policy development to address cyber threats and promote a stable cyber ecosystem. GCF aims to advance productive pathways for collaboration in the governance of Cyberspace, while mitigating risks related to cyber conflicts and cybercrime.

Cyber Economics

GCF's focus on cyber economics aims to investigate the economic dimension of cybersecurity, focusing on the costs of cyber threats, the impact of cybercrime on global economies, and investment strategies that promote cyber resilience. By analyzing market trends, regulatory frameworks, and economic incentives, GCF aims to increase understanding around the economics of Cyberspace and help decision-makers shape policies that promote sustainable cybersecurity investments and economic stability.

SELECT FORMATS AND PRELIMINARY AGENDA

The GCF Annual Meeting 2025 will feature new session formats to foster dynamic discussions and drive greater participant engagement, alongside regular formats such as panel discussions, townhalls, and fireside chats. The new formats will include:

- **Solution Design Session:** An interactive session that engages in hands-on activities and discussions to co-create solutions for shared challenges.

- **Practitioner Case Study:** As an in-depth exploration of a significant cybersecurity event, this session will provide firsthand accounts from cyber leaders, revealing key moments of discovery, critical decision-making processes, and lessons learned.

- **Global View:** Exploring cybersecurity success stories from around the world, discussions during this session will highlight how countries and organizations effectively address cyber threats, offering valuable lessons and actionable insights that can inform strategies in different contexts.

Preliminary High-Level Schedule

Wednesday 1 October			Thursday 2 October		
Open Forum	**Participatory Track**	**Roundtables**	**Open Forum**	**Participatory Track**	**Roundtables**
Room G	**Room Cs**	**Room F**	**Room G**	**Room Cs**	**Room F**
	9:00 – 12:00 **Invite Only Sessions**	9:00 – 12:00 **Invite Only Sessions**		9:00 – 12:00 **Invite Only Sessions**	9:00 – 12:00 **Invite Only Sessions**
10:00 – 10:30 **Opening Ceremony**			10:00 – 10:45 **Opening Plenary**		
10:30 – 11:45 **Opening Plenary**			10:45 – 12:00 **Open Forum Sessions**		
11:45 – 13:00 **Open Forum Sessions**			12:00 – 13:00 **Lunch**		
13:00 – 14:00 **Lunch**			13:00 – 14:45 **Open Forum Sessions**	13:00 – 18:00 **Invite Only Sessions**	13:00 – 18:00 **Invite Only Sessions**
14:00 – 15:30 **Open Forum Sessions**	13:00 – 18:00 **Invite Only Sessions**	13:00 – 18:00 **Invite Only Sessions**			
			14:45 – 15:30 **Closing Plenary**		
			16:00 – 17:00 **Closing Ceremony**		
	19:00 – 21:00 **Gala Dinner**				

ABOUT GCF

The Global Cybersecurity Forum is a global, non-profit organization that seeks to strengthen global cyber resilience by advancing international collaboration, purposeful dialogue, and impactful initiatives. It serves as a platform where the global community comes together to exchange knowledge and collaborate in tackling critical issues regarding Cyberspace. By uniting decision-makers and thought leaders from around the world, GCF aligns with international efforts to build a secure Cyberspace that enables prosperity for all nations and communities.