



# SESSIONS DESCRIPTION



# PATHWAYS TO DE-ESCALATION

Child Protection In Cyberspace. Session on latest developments, initiatives, and potential actions

## Plenary

In an increasingly interconnected world, Cyberspace stands as a critical domain in which nations, organizations, and individuals converge and collaborate. Cyberspace is a dynamic environment transcending geographical boundaries and playing a pivotal role in modern life and global connectivity. As inter-state tensions continue to strain the international order, it is essential to recognize the potential for conflict in Cyberspace which could disrupt economies, compromise national security, and diminish trust.

This session will highlight the implications of rising inter-state tensions in Cyberspace, as well as the key frontiers of opportunity including in terms of new diplomatic channels, evolving norms, and emerging technologies. The discussion will also focus on identifying the most viable pathways of collective action to de-escalate tensions and promote peace and security in Cyberspace.

### Key Questions:

- What are the primary implications of the current geopolitical dynamics on Cyberspace – in particular, for governments, the private sector, and individuals?
- In the current climate, how can international cooperation be strengthened to enhance cybersecurity and reduce the risk of full-blown cyber warfare?
- What are the highest strategic priorities for international organizations in addressing the challenges posed by inter-state tensions and conflicts in Cyberspace?
- What are the most significant trade-offs between national and collective security in Cyberspace given current geopolitical dynamics?
- What new diplomatic channels are emerging or are needed to mitigate geopolitical risk in Cyberspace?
- What are the most viable strategies for collective action to de-escalate conflicts and enhance the stability of Cyberspace?



# LEADERSHIP LAUNCHPAD

## Charting Paths to Leadership in Cybersecurity

### Panel Discussion

In today's cybersecurity landscape, the underrepresentation of women in senior leadership roles remains a critical issue. As the demand for diverse perspectives and strategic acumen grows, it becomes imperative to address barriers hindering mid-to-senior female cybersecurity professionals from advancing into executive positions. To bridge this gap, proactive initiatives should leverage global cybersecurity networks, developing effective strategies including targeted mentorship and sponsorship programs.

This session will explore the strategies to propel mid-to-senior female cybersecurity professionals into executive positions through tailored mentorship and sponsorship programs on a global scale. The session will also explore the role of global networks in supporting women's leadership in cybersecurity and how best to leverage and scale these networks.

### Key Questions:

- What are the primary barriers preventing mid-to-senior female cybersecurity professionals from advancing into executive roles?
- In what ways can global collaboration and networking initiatives be leveraged to scale mentorship and sponsorship programs for mid-to-senior female cybersecurity professionals internationally?
- What strategies should organizations adopt to foster inclusive cultures that empower women in cybersecurity, particularly in male-dominated subsectors or regions with traditional gender biases?
- How can sponsorship programs be tailored to help mid-to-senior female cybersecurity professionals achieve executive positions?
- How can global networks be leveraged and scaled to provide continuous support and opportunities for women in cybersecurity?



# PIONEERING PATHWAYS

## Unleashing potential in the Cybersecurity sector

### | Panel Discussion

In an era defined by rapid technological transformation and interconnectedness, cybersecurity is a critical pillar to support economic stability and growth. As technological reliance intensifies across sectors, so too does the need to safeguard these systems from evolving cyber threats.

Effective cybersecurity plays a crucial role in facilitating continued innovation and increased technological investments. In this context, harnessing the potential of cybersecurity as a driver for sustainable economic development is imperative.

This session will explore the multi-faceted economic contributions of the cybersecurity sector in tech-driven markets, covering the potential of the sector in times of major technological changes, the looming risks and opportunities in the development of the ecosystem. The session will also explore the most important pathways of action to harness the potential of this sector for sustainable economic growth.

### **Key Questions:**

- What are the key implications of increasing demand to ensure economic stability and growth in cybersecurity?
- What are the emerging opportunities at the intersection of cybersecurity and emerging technologies that drive future innovations and enhance overall ecosystem development?
- What are the most significant economic risks associated with the rapid advancement of technology in the cybersecurity sector? How can they be mitigated to ensure sustainable economic growth?
- How can governments and private sector entities collaborate to create supportive policy frameworks that support both economic growth and technological innovation in a competitive global market?
- What are the most important pathways of action to harness the potential of this sector for sustainable economic growth?



# CYBER STATECRAFT

## The new chessboard of geopolitics

### Fireside Chat

In an era where cybersecurity and geopolitics are increasingly intertwined, nations must navigate a complex landscape of cyber threats and strategic interests. As security risks loom large and geopolitical tensions rise, the importance of robust cybersecurity policies in national security planning and strategy development cannot be overstated.

Cyber statecraft has emerged as a critical component of modern diplomacy and defense, shaping the way countries protect their infrastructure and assert their sovereignty in Cyberspace.

This session will explore the strategic importance of cybersecurity in national security planning and strategy development in times of looming security risks and increasing geopolitical tensions. The session will also explore the key pathways of action to integrate cybersecurity measures into national defense strategies to enhance geopolitical advantage and ensure long-term security and stability.

### **Key Questions:**

- What are the most pressing cybersecurity threats that nations face today, and how do these threats impact national security and geopolitical stability?
- How might these threats evolve in the future given the rapid advancement of technologies?
- How can nations leverage advanced cybersecurity technologies to enhance national defense strategies?
- What are the most effective strategies for integrating cybersecurity into national defense planning amid escalating geopolitical tensions and security risks?
- In what ways can cybersecurity be integrated into broader national defense strategies to strengthen a country's geopolitical position and resilience against cyberattacks?



# THE MULTILATERAL FRONTIER

## Assessing the state of play and imperatives for collective action in cyber diplomacy



### Panel Discussion

In a global environment that is paradoxically both increasingly interconnected and structurally divided, cyber diplomacy has become ever more strategically central and challenging. No single nation can achieve cybersecurity alone, but pathways of collaboration have become dauntingly complex.

Finding pathways of productive, substantive inter-state collaboration on cybersecurity is thus a shared imperative. The effectiveness of cyber diplomacy in catalyzing multilateral cooperation will be decisive in shaping the future of Cyberspace.

This session will dive into the current state of UN negotiations, examining the significant progress to date as well as the persistent challenges in establishing robust international norms and frameworks for cyber governance. It will then consider the path forward, identifying actionable pathways for strengthening global cyber resilience and stability through enhanced international cooperation.

### Key Questions:

- What have been the key achievements to date of the cyber discussions at the UN and what have been the primary obstacles to collective progress?
- What will it take to find a viable balance among diverse interests given the fragmented geopolitical landscape that we face?
- What will ensure collective momentum in advancing cybersecurity?
- How can we accelerate progress in cybersecurity negotiations to keep pace with technology?
- What are the most promising pathways of action for strengthening global cyber resilience and stability through enhanced international cooperation?

#### SUBTHEMES:



Beyond Cyber Discard



Cyber Psychology



Cyber Social Fabric



Thriving Cyber Economy



New Cyber Frontier



# CTRL + INVEST

## Women shaping the future of cyber innovation

### Panel Discussion

The landscape of cyber innovation is currently undergoing a transformative shift, in which there is a growing recognition of the pivotal role that women-led ventures play in driving technological progress and economic prosperity. As the cybersecurity sector continues to expand, there is an increasing emphasis on the need for inclusivity. Emphasizing inclusivity not only strengthens workforce diversity but also enhances innovation. It boosts resilience to tackle evolving cyber threats in a rapidly evolving technological age.

This session will discuss the expanding and ever-important opportunities for investing in women-led cyber ventures driving innovation and economic growth while providing space for discussion on what each of the stakeholders can do to support inclusivity in this sector. The session will also explore the most promising actions the public and private sectors can take to support the innovation and growth of women-led startups.

### **Key Questions:**

- What are the most significant challenges women entrepreneurs face in the cyber industry, including systemic barriers, access to funding, and societal biases, and how can these challenges be effectively addressed?
- What are the most promising trends and emerging opportunities in the cybersecurity industry that can support and scale women-led cyber startups?
- What innovative funding models can investors and industry leaders introduce to support and promote inclusivity in the cyber sector, particularly for women-led ventures?
- What policies can the public sector introduce to foster greater inclusivity and investment in women-led cyber ventures?
- What are the most promising actions the public and private sectors can take to support the innovation and growth of women-led startups in cybersecurity?



# ECONOMIC SECURITY AND CRITICAL INFRASTRUCTURE

The imperative to build trust in an era of geopolitical competition

## Fireside Chat

In an era of heightened geopolitical competition, protecting economic security and critical infrastructure presents significant challenges. This session will highlight the crucial role of building and maintaining trust to effectively address these issues. It will explore how international cooperation can strengthen resilience, safeguard essential assets, and promote stability. This session will discuss approaches for enhancing trust and collaboration in managing the complexities of economic and infrastructure security in a competitive global environment.

### Key Questions:

- What are the primary challenges in protecting economic security and critical infrastructure in today's geopolitical climate?
- Why is building and maintaining trust crucial for addressing these challenges effectively?
- How can international cooperation contribute to strengthening resilience and safeguarding essential assets?
- What approaches can be taken to enhance trust and collaboration in managing economic and infrastructure security?
- In what ways can stability be promoted in a competitive global environment, considering the complexities of economic and infrastructure security?

#### SUBTHEMES:



Beyond Cyber Discord



Cyber Psychology



Cyber Social Fabric



Thriving Cyber Economy



New Cyber Frontier





# BEYOND THE FIREWALL

## Building a cyber resilient supply chain in a hyperconnected world

### Panel Discussion

The world is in a period of extensive technological integration, with global supply chains becoming more interconnected and reliant on advanced technologies. Simultaneously, the rise in cyber threats exploiting these dependencies significantly endangers the security and stability of supply chains worldwide.

The imperative to build cyber resilience extends beyond individual organizations to encompass entire supply chains, where vulnerabilities are amplified through technological interdependencies. This session will explore the growing need for cybersecurity in supply chain resilience in a hyperconnected world, exploring the trends impacting the supply chain such as advanced technologies, and potential mitigation mechanisms to drive stability and safety in the supply chain. The session will also consider the role of international cooperation in enhancing cyber resilience in global supply chains.

### Key Questions:

- What are the key cyber threats to supply chains today, and how are these threats evolving with technological advancements?
- How can emerging technologies such as AI, Internet of Things (IoT), blockchain, etc. be leveraged to enhance supply chain resilience against cyber threats – to strengthen security measures and mitigate vulnerabilities?
- In what ways can international standards and regulations be harmonized to ensure consistent cybersecurity policies across supply chains?
- How can partnerships between government, industry, and academia drive innovation in supply chain cybersecurity resilience?
- What are the most effective strategies for integrating cybersecurity into supply chain management amid rapid technological development and an expanding cyber threat landscape?



# BALANCING PROGRESS AND PERIL

## Understanding the challenges and opportunities of AI in Cybersecurity

### | Panel Discussion

The rapid advance of AI is creating a new frontier of cyber threats and vulnerabilities. At the same time, it is generating powerful new means of strengthening cybersecurity. The dual nature of AI creates new challenges and opportunities for cybersecurity policymakers and diplomats at the national and international levels. For many countries, addressing these challenges and capitalizing on these opportunities will require new forms of international collaboration.

This session will explore AI's dual nature, delving into the advancements in cyber threats powered by AI, and its potential to offer transformative solutions that can anticipate, detect, and mitigate threats more effectively than ever before. This session will also focus on identifying the most promising pathways of collaboration for advancing the responsible use of AI to address its risks and realize opportunities.

### **Key Questions:**

- How do AI-driven cyber threats differ from traditional threats, and what strategies can we employ to mitigate them?
- What opportunities does AI present to bolster cyber defense capabilities?
- What are the emerging best practices for integrating AI into existing cybersecurity protocols to enhance systemic resilience?
- How can nations balance the need for AI innovation with the imperative to safeguard against new cyber threats?
- What role should the private sector and international organizations play in developing and deploying AI solutions in cybersecurity?
- What are the most promising pathways of collaboration for advancing the responsible use of AI to address the risks and realize the opportunities that this transformative technology is generating?

#### SUBTHEMES:



Beyond Cyber Discord



Cyber Psychology



Cyber Social Fabric



Thriving Cyber Economy



New Cyber Frontier



# THE HISTORY OF CYBER DIPLOMACY FUTURE

Drawing insights from collaborative progress on trade, nuclear and climate

## Plenary

In this session, we delve into key global issues such as trade, nuclear policy, and climate change to analyze successful strategies and lessons learned from negotiations on these topics, with the aim to develop innovative approaches to cyber diplomacy. Participants will explore how the complexities and negotiations in trade agreements, nuclear disarmament, and climate accords can inform and shape effective approaches to cyber diplomacy. The session will provide a comprehensive understanding of how these diverse areas intersect and offer practical insights for applying these to enhance global cyber diplomacy.

### Key Questions:

- What specific strategies from past trade agreements can be adapted to strengthen cyber diplomacy efforts on a global scale?
- How can the principles of nuclear disarmament negotiations be applied to international cyber agreements to reduce the risk of cyber conflict?
- In what ways can the lessons learned from climate change accords be leveraged to foster international cooperation in cyberspace?
- What are the common challenges in trade, nuclear policy, and climate negotiations that are also present in cyber diplomacy, and how can they be effectively addressed?
- How can a multidisciplinary approach, incorporating insights from trade, nuclear, and climate discussions, enhance the development of global cyber diplomacy frameworks?



# PRINCIPLES OF STABILITY

## Applying the lessons of the past to the current and future challenges in Cyberspace

### Fireside Chat

The growing frequency and sophistication of cyber attacks demand more effective approaches to mitigation and response. It's crucial to understand your entire attack surface area and trace every possible path into your environment, then address security gaps and weaknesses. As we navigate this new landscape, it is imperative that we leverage the lessons from prior incidents to understand the potential risks that are emerging and develop effective strategies for increasing stability and resilience.

This session will explore how these issues are tackled through the Secure Future Initiative, a multiyear program to evolve the way Microsoft designs, builds, tests, and operates products and services to achieve the highest possible standards for security.

### Key Questions:

- What specific strategies are being employed through the Secure Future Initiative to address the most pressing cybersecurity threats facing businesses and governments today?
- How does the Secure Future Initiative integrated into with the broader cybersecurity ecosystem, including cloud services and AI capabilities?
- In what ways is the Secure Future Initiative fostering collaboration with other tech companies, governments, and organizations to build a unified approach to global cybersecurity?
- What measures are being taken through the Secure Future Initiative to ensure the protection of emerging technologies such as IoT, 5G, and quantum computing?
- How does the Secure Future Initiative plan to evolve in response to the rapidly changing cybersecurity landscape, and what are the long-term goals for this initiative?

#### SUBTHEMES:



Beyond Cyber Discord



Cyber Psychology



Cyber Social Fabric



Thriving Cyber Economy



New Cyber Frontier



# SHIELDING CONNECTIVITY

## Safeguarding future networks

### | Panel Discussion

In this session, we will explore the challenges and opportunities in safeguarding next-generation networks, including 6G. As these networks become the backbone of future communication and technological advancements, they will also introduce new vulnerabilities and threats. Participants will delve into the latest security strategies, technologies, and protocols designed to protect these advanced networks from cyber threats. The session will also highlight the importance of global collaboration and policy-making in ensuring the resilience and security of critical infrastructure, paving the way for a secure Cyberspace.

### **Key Questions:**

- What are the key security challenges specific to 6G networks, and how do they differ from those in 5G?
- How can emerging technologies be leveraged to protect 6G networks from evolving cyber threats?
- What role does international collaboration play in the development and implementation of security protocols for next-generation networks?
- What policies and regulations are essential to ensure the resilience of critical infrastructure as we transition to 6G?
- How can we balance innovation in 6G with the need to safeguard against potential security vulnerabilities?



# COGNITIVE RESILIENCE

## Building psychological defense against cyberattacks

### Panel Discussion

The world has entered an era in which technology permeates every aspect of human life, creating an environment of technological omnipresence. As we increasingly incorporate technology into our daily tasks, the pervasive nature of these advancements exposes us to a heightened risk of cyber attacks. Cyber threats now pose significant risks not only to data and infrastructure but also to the mental well-being of individuals, resulting in the psychological impact of cyberattacks becoming a critical concern.

This session will explore several key mechanisms to develop psychological resilience and individual preparedness against cyberattacks. The session will also explore the most promising pathways of action to implement these mechanisms to protect individuals from the psychological harms of cyberattacks.

### Key Questions:

- What are the primary implications of cyber attacks for psychological vulnerabilities of individuals facing cyberattacks?
- What are the most effective communication strategies for governments to employ in order to inform and reassure the public during and after significant cyber incidents to minimize psychological harm?
- What is the role of educational systems in preparing future generations for the psychological challenges posed by the increasing pervasiveness of technology and potential cyber threats?
- In what ways can interdisciplinary collaboration between cybersecurity experts, psychologists, and policymakers enhance the psychological resilience of populations against cyber threats?
- What are the most promising pathways of action to implement these mechanisms to protect individuals from the psychological harms of cyberattacks?

#### SUBTHEMES:



Beyond Cyber Discord



Cyber Psychology



Cyber Social Fabric



Thriving Cyber Economy



New Cyber Frontier



# THE PULSE OF SECURITY

## Securing the healthcare sector amidst technological disruptions

### | Panel Discussion

The healthcare sector is increasingly reliant on interconnected systems and online platforms to deliver essential services, making it more susceptible to cyber threats. The management of vast amounts of sensitive data within hospital information systems and electronic health records further compound the challenge, presenting potential vulnerabilities and security risks. To address these challenges, the healthcare sector needs to prioritize cybersecurity measures. This includes increasing awareness, implementing robust systems, and developing comprehensive guidelines governing health confidentiality.

This session will delve into the challenges faced by the healthcare sector in times of attack, looking into the critical impact on public health service delivery. The session will also explore essential strategies for healthcare providers to balance the need for robust cybersecurity with the demand for accessible and efficient public health services.

### **Key Questions:**

- What are the main implications of cyberattacks on public health service delivery and patient safety, including the potential loss of sensitive data?
- What are the key challenges and opportunities in securing the Internet of Medical Things devices and other connected healthcare technologies?
- How can interdisciplinary collaboration between cybersecurity experts, healthcare providers, and policymakers enhance the resilience of healthcare infrastructure against cyber threats?
- What are the essential strategies for healthcare providers to balance the need for robust cybersecurity with the demand for accessible and efficient public health services?

#### SUBTHEMES:



Beyond Cyber Discard



Cyber Psychology



Cyber Social Fabric



Thriving Cyber Economy



New Cyber Frontier



# NAVIGATING THE FUTURE

## Advancing the Global Cybersecurity Agenda to build confidence in cyberspace

### Fireside Chat

This session will explore the evolution from World Summit on the Information Society (WSIS) Action Line 5, which established the foundation for building confidence and security in ICTs, to the development of the ITU Global Cybersecurity Agenda (GCA). It will highlight how the principles and objectives of Action Line 5 have influenced and shaped the ITU's comprehensive approach to cybersecurity. The discussion will cover the broader implications for global cooperation and strategic advancements in securing our interconnected world.

#### **Key Questions:**

- What are the main objectives of the GCA?
- How does the GCA align with international efforts to improve cybersecurity?
- What key strategies and initiatives are outlined in the GCA to enhance global cybersecurity and contribute to Sustainable Development Goals (SDGs)?
- How does the GCA address the challenges of workforce shortage in cybersecurity?
- In what ways can member states and organizations contribute to achieving the goals of the GCA?





# FROM SHORTAGE TO STRENGTH

## Closing the Cybersecurity Skills Gap for a resilient cyberspace

### Panel Discussion

As cyber threats become more sophisticated, the need for a strong cybersecurity workforce is more critical than ever. This session explores the cybersecurity skills gap and offers actionable strategies to address it. Attendees will learn about challenges in recruiting and retaining talent and discover innovative training approaches to enhance cyber defenses. It will also consider how the shortage of skilled professionals can be turned into a chance for growth and resilience in Cyberspace.

#### **Key Questions:**

- What are the main challenges currently faced in recruiting and retaining cybersecurity talent?
- What practical strategies can be implemented to address the cybersecurity skills gap?
- How can innovative training and education approaches enhance cybersecurity defenses?
- In what ways can organizations and individuals work together to build a stronger cybersecurity workforce?
- How can the current shortage of skilled cybersecurity professionals be turned into an opportunity for growth and resilience?



# SECURING THE SPOTLIGHT

## Cybersecurity Roadmap for Mega Events

### Panel Discussion

Mega events, from international sports tournaments to large-scale and/or high-level gatherings, present unique cybersecurity challenges due to their scale and high profile. This session will outline a comprehensive roadmap for managing cybersecurity in these high-stakes environments. We will explore key considerations for securing large events, including risk assessment, threat detection, and incident response. The session will provide insights into effective planning, coordination, and implementation of cybersecurity measures tailored to the complexities of mega events.

### **Key Questions:**

- What are the unique cybersecurity challenges associated with mega events like the FIFA World Cup, G20, Hajj, and the Olympics?
- How can risk assessment be effectively conducted for large-scale and high-profile gatherings?
- What strategies are recommended for threat detection in the context of mega events?
- What are the best practices for incident response during high-stakes events?
- How can effective planning and coordination be achieved to implement cybersecurity measures tailored to the complexities of mega events?



# PERSPECTIVE REVERSAL

## Cognitive Strategies and Orientations of Attackers

### Participatory Track

In an era marked by increasingly sophisticated cyber threats, understanding the mindset of attackers has become crucial for effective defense. The complexity and ubiquity of cyberattacks are driven by attackers' use of cognitive strategies, psychological tactics, and exploitation of human biases. In this context, gaining insights into the cognitive orientations of attackers is essential for developing robust cybersecurity measures. Studying the cognitive strategies of attackers also provides valuable intelligence for improving incident response capabilities and mitigating the impact of cyber attacks.

This session will explore attackers' cognitive strategies and orientations, investigating their use of cyber vulnerabilities, psychological tactics, and human biases in designing and executing cyber offenses amid increasing attack complexity and ubiquity. The session will also explore key pathways of action to counteract these tactics through enhanced defensive measures and strategic planning.

### **Key Questions:**

- How do attackers leverage cognitive strategies and psychological tactics to exploit vulnerabilities in cybersecurity systems?
- In what ways can understanding the cognitive orientations of attackers enhance the development of robust cybersecurity measures?
- What are the most common human biases that attackers exploit in designing and executing cyber offenses? How can we mitigate these vulnerabilities?
- What are the most effective strategies for counteracting the cognitive strategies and psychological tactics of attackers through enhanced defensive measures and strategic planning?
- What are the key pathways of action to counteract these tactics through enhanced defensive measures and strategic planning?



# FROST GUARD

## Securing the vaccines cold chain to the last mile

### Participatory Track

In the face of global health challenges, securing the vaccine cold chain from cyberattacks is crucial. Maintaining the integrity of the cold chain ensures that vaccines remain potent from production through distribution to vaccination sites. Any lapse in the security measures can compromise vaccine effectiveness, and undermine efforts to combat diseases and protect public health on a global scale. Addressing these challenges requires robust cybersecurity strategies and multi-stakeholder collaboration to protect vital facilities and ensure supply chain integrity.

This session will provide insights into the risks involved in vaccine cold chain management, analyzing the cybersecurity strategies deployed for protecting vital facilities in the supply chain in times of major global health challenges. The session will also explore the most promising pathways to counter cyber threats to ensure the secure delivery of vaccines to the last mile.

### **Key Questions:**

- What are the primary cyber threats and vulnerabilities facing the vaccine cold chain, from production facilities to distribution networks and vaccination sites?
- How can cybersecurity strategies be effectively integrated into vaccine cold chain management to ensure the integrity and security of vaccines?
- What role do technological innovations such as blockchain and IoT devices play in enhancing the cybersecurity resilience of the vaccine cold chain?
- What are the most effective strategies for integrating robust cybersecurity practices into the vaccine cold chain management systems?
- What are the most promising pathways to counter cyber threats to ensure the secure delivery of vaccines to the last mile?



# CYBER (S)HEROES

## Breaking Stereotypes, Building Careers

### Participatory Track

In the global cybersecurity landscape, diversity is not just a moral imperative but a strategic advantage. Despite the growing demand for skilled cybersecurity professionals, the industry continues to be predominantly male, with women facing significant barriers to entry and advancement. This lack of diversity stifles innovation and limits the range of perspectives necessary to tackle increasingly sophisticated cyber threats. Addressing this imbalance requires confronting persistent gender stereotypes that deter women from pursuing careers in cybersecurity. Empowering women to break these barriers is essential for fostering diversity and innovation.

This session will explore the critical issues resulting in the underrepresentation of women in the cybersecurity workforce, with a specific emphasis on women's leadership across different sectors – public and private. The session will also explore the most important policy initiatives that can support and promote women in cybersecurity leadership roles.

### **Key Questions:**

- What are the primary barriers to entry and advancement for women in the cybersecurity industry?
- How do gender stereotypes impact the career choices of women in cybersecurity?
- What strategies can be implemented to challenge and change these perceptions?
- How can mentorship and sponsorship programs be structured to provide meaningful support and career advancement opportunities for women in cybersecurity?
- What policy initiatives would be most effective in increasing the representation of women in cybersecurity leadership roles, and what additional measures are needed?



# REDUCING CYBER CARBON FOOTPRINT

## Making Cybersecurity Sustainable

### Participatory Track

In today's world of fast-paced technological expansion and heightened risk of cyber threats, the interplay between cybersecurity measures and their carbon footprint is critical to shed light on. Addressing this issue is crucial not only for reducing environmental harm but also for ensuring sustainable development in this sector. Optimizing the operational and energy efficiency of cybersecurity solutions and exploring the usage of renewable sources is imperative to build a future and make cybersecurity sustainable, including through integrating green technologies.

This session will explore the environmental impact of cybersecurity solutions and explore strategies to enhance sustainability in cybersecurity. The session will also explore the most collaborative pathways of action to reduce energy consumption while maintaining high-security standards of evolving technologies.

#### **Key Questions:**

- What are the primary implications of the rising need for cybersecurity solutions for environmental sustainability?
- What are the key challenges and emerging opportunities in integrating sustainable technologies in cybersecurity solutions?
- What are the potential trade-offs between enhancing cybersecurity and maintaining environmental sustainability? How can these trade-offs be managed effectively?
- What strategies can international organizations play in strengthening and mandating actions to reduce cyber carbon footprint?
- What are the most collaborative pathways of action to reduce energy consumption while maintaining high-security standards of evolving technologies?



# CODE, CLICKS, AND CULTURE

## Social Transformation in the Technological Age

### Participatory Track

In today's interconnected world, the rapid evolution of technology is fundamentally reshaping how societies interact, communicate, and evolve. From the youngest to the oldest generations, technological advancements have permeated every aspect of daily life, profoundly influencing cultural norms and societal structures. Understanding this transformation and identifying ways to manage it is crucial to ensure the inclusion, ethical usage of technology, and the preservation of cultural identities amid globalization.

This session will explore the transformation led by technological advancements by analyzing the cultural shift driven by increasing interconnectedness and widespread use of technologies across all layers of the population, from children to the elderly. The session will also explore the most effective strategies for managing this transformation to foster inclusive and sustainable societal development.

### **Key Questions:**

- What are the key cultural shifts driven by the widespread adoption of technologies, and how do these shifts impact societal norms and values?
- How might these shifts further evolve with the advancement of technologies?
- What innovative technologies can be leveraged to enhance social inclusion and bridge the digital divide across diverse demographics?
- How can interdisciplinary collaboration between technologists, sociologists, and policymakers enhance the positive effects of technological advancements on cultural transformation?
- What are the most effective strategies for managing this transformation to foster inclusive and sustainable societal development?



# CURING THE GAP

## Promoting Cybersecurity solutions for vulnerable health

### Participatory Track

As we move into an increasingly interconnected future, healthcare systems worldwide are embracing advanced technologies to revolutionize patient care. However, this rapid technological integration brings significant cyber risks, especially for vulnerable health systems in developing countries. The future of global healthcare depends on robust cybersecurity measures to protect critical infrastructure from sophisticated cyber threats that could disrupt services, compromise sensitive data, and incur substantial financial losses. Ensuring the cybersecurity of health systems is imperative as we navigate an ever-evolving technological landscape.

This session will discuss the importance of cybersecurity for healthcare services, assess the need for such investments in developing countries, and identify strategies for inclusive capacity building. The session will also explore key pathways through which public-private partnerships can enhance cybersecurity for healthcare services.

### **Key Questions:**

- What are the key strategic priorities for investing in cybersecurity infrastructure to protect sensitive health data and ensure the resilience of healthcare services?
- What role do international organizations play in setting and harmonizing standards for cybersecurity in healthcare?
- How does multi-stakeholder collaboration contribute to developing and implementing robust cybersecurity frameworks for healthcare systems in developing countries?
- How can developing countries prioritize and justify investments in cybersecurity for their healthcare sectors amidst other pressing needs?
- What are the key pathways through which public-private partnerships can enhance cybersecurity for healthcare services?





# BREAKFAST

## Launch of 'Women Leadership in Cyber' global mentoring program



### Participatory Track

The 'Women Leadership in Cyber' Mentoring program will accelerate and help aspiring and current women professionals in building and sustaining meaningful careers in cybersecurity. The series will be catered around thought-provoking conversations with Women thought leaders and decision makers. The series of mentoring sessions will provide mid-management women in cybersecurity with best practices to sustain and advance their careers into leadership positions.

The 'Women Leadership in Cyber' Mentoring program is part of project "Develop a career development and leadership program for women in cybersecurity" of the Women Empowerment in Cybersecurity (WEG) global initiative.



# FORTIFYING THE FIELD

## Securing the operational technology of the oil industry in a hyperconnected world

### Participatory Track

In a hyperconnected world, the oil industry faces the dual challenges of leveraging technological transformation while managing heightened cyber threats. The convergence of Operational Technologies (OT) and Information Technologies (IT) brings efficiency and innovation but also exposes critical infrastructure to cyberattacks that can disrupt operations and cause significant financial and environmental damage. Ensuring the resilience and security of OT systems has never been more crucial for the global oil industry. To address these challenges, a comprehensive cybersecurity strategy tailored specifically for the oil sector is essential.

This session will explore the unique challenges, and emerging trends of OT cybersecurity in the oil industry against the backdrop of increasing connectedness to develop strategies and design innovative solutions for enhanced security. The session will also explore the most promising pathways for collaboration to enhance the security of OT in the oil sector.

### **Key Questions:**

- How has the increasing interconnectedness of the oil industry amplified cybersecurity vulnerabilities in OT systems? What are the most significant threats currently facing the sector?
- What solutions are being developed to address the unique challenges of securing OT systems in the oil industry?
- What are the key challenges and opportunities in integrating advanced technologies in securing oil industry infrastructure? How can these be addressed?
- How can international regulatory frameworks be aligned to ensure consistent and effective cybersecurity measures across the global oil industry?
- What are the most promising pathways for collaboration to enhance the security of OT in the oil sector?



# THE LAST MILE

## Turning talk into tangible results

### Participatory Track

The world's growing interconnectedness makes global collaboration and innovation in Cyberspace a paramount imperative. As geopolitical tensions and technological rivalries intensify, countries must unite to address global challenges effectively. Several multilateral and multi-stakeholder platforms, including the United Nations, facilitate essential discourse and are working to translate this discourse into tangible progress, for example through the UN Programme of Action to advance responsible State behavior in the use of ICT in the context of international security.

This session will explore the current state of cyber diplomacy discussions in various venues, and focus specifically on the challenge of converting these processes into practical action and tangible results.

#### **Key Questions:**

- What are the key obstacles to turning cyber diplomacy discussions into tangible results, and how can they be overcome?
- What emerging trends should be considered in future efforts to translate cyber diplomacy dialogue into tangible outcomes?
- What practical methodologies can be employed in the context of cyber diplomacy discussions, including at the UN, to ensure successful and accelerated translation into action?
- What are the key considerations while applying these methodologies, such as mini-lateral consensus, and what are the key success factors?
- What are the most productive pathways for translating dialogue into action at global forums to create meaningful impact?



# EQUIPPING THE DEFENDERS

## What law enforcement needs to win

### Participatory Track

The increasing integration of technology across all age groups is reshaping societal interactions and behaviors worldwide. This transformation brings unprecedented connectivity and convenience but also amplifies risks such as the proliferation of online child abuse cases. Geopolitical fragmentation further complicates international efforts to address these challenges, highlighting the urgent need for innovative approaches to protect vulnerable populations in an evolving digital environment.

This session will examine the need for law enforcement specialists to investigate online child abuse, address the talent shortage, analyze future skill requirements, and propose a plan of action. The session will also explore strategies to secure the expanding attack surface and ensure effective law enforcement responses in the fight against online child abuse.

### **Key Questions:**

- How has the widespread adoption of technology reshaped the landscape of online child abuse, and what emerging trends or patterns are being observed globally?
- What are the anticipated future skill requirements for law enforcement specialists regarding child exploitation, and how can training programs adapt to meet these demands?
- What is the role of international organizations in addressing the rise of online child abuse and strengthening law enforcement in this issue?
- In what ways can multi-stakeholder collaboration and information sharing be improved to combat online child abuse more effectively on a global scale?
- What are the most effective strategies to secure the expanding attack surface and ensure effective law enforcement responses in the fight against online child abuse?



# HACKING TRUST

## Cybercrime's Role in Transforming Social Norms

### Participatory Track

The technological era has ushered in a profound transformation where cybercrime profoundly impacts social trust, fundamentally reshaping decision-making processes, behaviors, consumption habits, and the very fabric of interpersonal trust. These advancements, while promising enhanced connectivity and efficiency, also introduce complexities that often fracture rather than unify societal norms. As online interactions become increasingly pervasive, preserving social trust and stability emerges as a paramount challenge.

This session will explore the impact of cybercrime on social trust amplified by the rise of technological advancement, delving into how these factors impact social decisions, behaviors, consumption patterns, and trust, transforming social norms. The session will also explore the most effective measures for strengthening cybersecurity and protecting social trust in the rapidly evolving technological age.

### **Key Questions:**

- What are the primary implications of cybercrime for societal trust dynamics?
- Amidst the evolving technological landscape, how can nations and international organizations collaborate more effectively to bolster cybersecurity frameworks and mitigate the disruptive impacts of cyber threats on societal trust?
- What are the key strategies and technologies that governments, businesses, and communities can adopt to bolster cybersecurity defenses and safeguard societal trust in digital interactions?
- What innovative approaches can be implemented to enhance public awareness and digital literacy regarding cyber threats?
- What are the most effective measures for strengthening cybersecurity and protecting social trust in the rapidly evolving technological age?

