Organization of the Interactive Program

While the highlighted plenary speakers will offer visions for the future of international collaboration for cyber security, the bulk of the Summit will be a highly interactive format. This interactive part of the program gives participants unique opportunities to work with professional peers from around the world. Its structure has two main lines: there are 8 *sectors* and under each sector there are one or more *breakthrough groups.* The 8 sectors span both the fabric of cyberspace (i.e. the ICT sector) and the most critical sectors depending on it. Participants can expect to be able to work on issues pre-identified as critical international stalled policy areas, or on those that are participant-proposed at the Summit. Some of the identified topic areas that breakthrough groups may form around are outlined in Figure 1. The success of the Summit is measured by the breakthroughs made by these groups both during the Summit, and in the follow-up activities.

Figure 1. Relationship Between Critical Sectors and Breakthrough Topics, *with examples*

Breakthrough Groups	Critical Sectors							
	ICT	Financial Services	Energy	Transport-ation	Essential Gov't. Services	National Security	Media	Small and Medium Enterprises
GUCCI Reliability Measurements for Stakeholder Due Diligence	██	██						
ICT Standard for the International Financial Services Sector	██	██						
Rules of Engagement for Peaceful Co-Existence						██		
Protecting Youth in Cyber Space							██	
Use of ICT for Humanitarian Aid	██				██			

Figure 2 indicates that each topic discussion begins at one of three basic levels of maturity. The first level is one in which the nature of the problem and initial solution space are being *explored*. The second level is where possible *recommendations are being developed*. The third level of maturity is where the *implementation of a consensus recommendation* is the work at hand. This is designed to facilitate breakthroughs at each of these levels.

Figure 2. Maturity of Discussion Entry Points

Specific Focus Areas

The specific focus areas of the First Worldwide Cybersecurity Summit will be primarily of three levels of maturity:

ICT Development Supply Chain Integrity

Maturity Level: *LOW-MODERATE*
Sectors: *All*
Abstract: *The integrity of ICT supply chains is essential for the trusted operation of our critical infrastructures – communications, financial, energy, government, transportation, etc. The hardware and software that are so vitally depended upon are created in less developed regions due to the benefits of lower cost structures. However, the risk of exposure from malicious design insertion is profound. The re-use of ICT development environments and processes are multifarious and highly complex, making integrity assurance exceedingly difficult. Because the development supply chains and dependencies crisscross international borders, international collaboration is imperative.[1] Existing solutions are not sufficient to address the present or future challenges of our dependencies upon outsourced ICT.[2]*
Challenges: The full range of vision, incentives and policies are lacking. The private sector and academia need to focus. Governments need to promote the implementation of innovative trust concepts to support the operation of these systems. International collaboration needed.

Payload Prioritization in Public Networks[3]

Maturity Level: *MODERATE*
Sectors: *ICT, Financial, National Security, Essential Government Services,*
Abstract: *The continuous availability of communications services is imperative to the operation of our critical infrastructures. The rapid shift from legacy, dedicated circuit switched to data switching network technology has introduced dramatic cost reductions in services. However, concomitantly, there is now new uncertainty about whether bandwidth will be available when needed for critical applications. Emerging bandwidth-intense applications such as video and gaming can deprive access to applications with even light bandwidth applications such as real-time financial transactions or emergency voice calls. While most societies around the world discern and assign more importance to some functions (e.g., hospitals, police, national security) that ensure economic and social stability, cyberspace is increasingly becoming undiscerning in its ability to reflect social values. The consequences are increased risk to society. Despite the fact that cyberspace is borderless and international standards have been developed, there is no coordination between nation-states to implement an international scheme.*
Challenges: Begin coordination of international priority services using existing international standards.

---

[1] *An Intrinsic Vulnerability Approach Component for Total Integrity Management of Information and Communications Technology Development and Delivery*, Rauscher, K. F., Bell Labs, USA, IEEE Globecom 2009 International Workshop on Telecommunications Infrastructure Protection and Security, December 2009.

[2] EC Availability and Robustness of Electronic Communications Infrastructures (ARECI), March 2007.
[3] IEEE ROGUCCI Recommendation 11, Mechanisms for Overload Control

GUCCI Reliability Measurements for Stakeholder Due Diligence[4]

Maturity Level: *HIGH*
Sectors: *ICT*
Abstract: *Throughout the world, many stakeholders are depending on the reliability of Global Undersea Communications Cable Infrastructure (GUCCI). One such stakeholder is the financial sector. In similarity to vital dependence of the transportation sector on fuel, and agriculture on rain, the modern financial sector cannot operate without GUCCI. As the financial services sector continues to evolve on a global basis, increased reliance on ICT translates directly into increased reliance on undersea cable infrastructure. Those responsible for overseeing their institutions' exposure to operational risk cannot perform due diligence because there is insufficient information available. Some of the fundamental information that is needed includes statistically based expectation of downtime for international connectivity, geographic route information for purchased circuits and bandwidth, and equipment and service supplier information that can contribute to common failure modes.*
Challenges: Private sector-led, voluntary outage sharing and analysis within a trusted environment. Development of a statistical framework for supporting stakeholders' due diligence.

Prioritization for Timely Repairs[5]

Maturity Level: *HIGH*
Sectors: *ICT*
Abstract: *Damaged undersea cable repairs have extended durations due to government permitting processes for access to sovereign waters. The repair of a damaged undersea communications cable is a process that involves coordination between the cable system owner, a specialized repair vessel operator and the nation-state government in whose waters the repair operation needs to be performed. Because of variations across nation-state governments' policies and procedures that grant access for repair operations, there is wide variation in permitting approval times – from 24 hours to well over 2 months. On one hand, there are governments whose process is proactive and streamlined. In these cases, speedy restoration of service has been prioritized and coordination planning for responses to anticipated outages includes pre-approval for repair operations in designated waters. Such coordination and planning keeps the approval process on the order of only days. On the other hand, there are governments whose approval approach is reactive, uncoordinated among divisions, or otherwise ineffective in prioritizing the restoration of service over damaged cables. In these cases, outage durations are unnecessarily extended by additional weeks. Regarding the special case of disputed territorial waters, the undersea cable industry continues to expend considerable effort to promote ratification of the UNCLOS as a means of establishing international laws protecting the rights of cable owners in international waters. The industry is encouraged that the UNCLOS provides special status to undersea communications cables, but also recognizes that confusion is caused by the differences between legal regimes under the UNCLOS territorial seas, Exclusive Economic Zone (EEZs) and Continental Shelves with regard to submarine cables. Very long duration outages are a major concern regarding the reliability of GUCCI because they contribute significantly to overall widespread downtime or impairment.*
Challenges: Nation-state governments must conduct advance planning in anticipation of cable damage and must prioritize the restoration of undersea communications cables by committing to providing an efficient and appropriately-speedy process for granting authorized repair vessels access to their sovereign waters. Cable ship operators and cable infrastructure owners must

---

[4] IEEE ROGUCCI Report Recommendation No. 7, *Measurements for Stakeholder Due Diligence.*

[5] IEEE ROGUCCI Report Recommendation No. 4, Best Practices and Information Sharing

cooperate with government requirements for information, onboard inspections, escorts and other requests, particularly when opportunities for pro-active engagement are presented. Nation-state governments must be willing to compare themselves to best-in-class benchmarks for efficient permitting time durations.

Rudimentary Geographic Diversity for Cable Infrastructure[6]

Maturity Level: *HIGH*
Sectors: *Financial Services, ICT*
Abstract: *The world's undersea communications cable infrastructure performs at a level of reliability such that it's availability and operation are taken for granted by countless users. However, the dramatically increasing dependence upon this infrastructure evokes a sense that ever-increasing diligence is needed to ensure its reliability performance is commensurate. The fundamental principle of avoiding single points of failure is compromised in the world's global undersea communications cable infrastructure due to the aggregation of cables at certain "choke points". These locations include the Luzon Strait, the Suez Canal-Red Sea-Mandab Strait passage, and the Strait of Malacca, among others. Single points of failure are latent design weaknesses, whether or not they are ever exposed. Recent history has provided instances where this susceptibility has been exploited. Contributing factors to the current situation include real and perceived geographic and nation-state political barriers to preventing private sector investment in alternate routes to avoid existing choke points. Hindrances include the initial access to explore and invest in these locations, and then uncertainty regarding access to these cables for maintenance. In addition, economic incentives motivate undersea network installations to re-use existing paths.*
Challenges: Stakeholder advocacy is needed to promote the deployment of geographically separate cable paths that will avoid current single points of failure. Nation-states controlling the lands and waters for potential alternative, diverse paths need to demonstrate new flexibility and support new network deployments.

Preparedness for Hostile Maritime Crisis[7]

Maturity Level: *MODERATE - HIGH*
Sectors: *National Security, ICT*
Abstract: *Increased hostile activity around the world requires the undersea communications cable industry to enhance its preparedness for attacks on its specialized cable ships and critical infrastructure. In addition to the obvious danger to lives to property, such activity could cause long-term service outages.*
Challenges: The effective implementation of this Recommendation requires the commitments of governments and the private sector. Nation-state governments must cooperate in establishing intergovernmental agreements, participating in planning, and periodic simulated crisis exercises. Owners of cable ships must support effective planning and exercises by making vessels and critical personnel available. Finally, Nation-state governments and cable ship owners must establish agreements on cooperation procedures for maritime crisis response.

---

[6] IEEE ROGUCCI Report Recommendation No. 1. *Rudimentary Geographic Diversity for Cable Infrastructure*
[7] IEEE ROGUCCI Report Recommendation No. 3, *Preparedness for Hostile Maritime Crises.*

Best Practices and Trusted Information Sharing for International Critical Infrastructure[8]

Maturity Level: *MODERATE - HIGH*

Sectors: *ICT*

Abstract: *With the enormous challenge of protecting and advancing the reliability of GUCCI, there are compelling reasons for ensuring that industry peers are well informed, as better awareness can be critical in optimizing strategies for protection and reliability assurance. This information sharing is needed on an international basis, as inter-continental undersea cables are by definition international critical infrastructure.*

Challenges: Private sector companies that own and operate undersea communications infrastructure must jointly establish a trusted environment for sharing information to improve the protection and rapid restoration of GUCCI. The private sector must be willing to share threat and outage information within a trusted environment within the industry for the common good. Nation-state governments must be wiling to share threat and other sensitive information with owners and operators of GUCCI and safeguard information provided by the industry. Nation-state governments must be willing to share information that will improve the protection and rapid restoration of critical infrastructure with other nation-states as well as the owners and operators of that infrastructure within the other nation-states.

New Private Sector Governance for International Critical Infrastructure[9]

Maturity Level: *MODERATE*

Sectors: *ICT*

Abstract: *The IEEE ROGUCCI Report establishes the need for dealing with individual undersea cable systems as an aggregate, i.e. global level. The need is based on the limited focus of commercial interests that manage individual systems, the difficulty stakeholders have in performing due diligence in managing their operational risk and the extremely high level of importance that this infrastructure plays in the world. Some groups are re-examining their charters to determine how they might addresses some of the new or more critical issues of the nature discussed at ROGUCCI Summit. Observations from financial sector stakeholders were that the undersea communications industry would benefit from a "system-wide" view, more inclusive participation in industry collaborative programs, more structured governance, better coordination and a unified voice. Specific mission areas for new governance would ideally include defining expectations for the industry, engaging representative stakeholders and articulating ASPR that would advance GUCCI resilience.*

Challenges: Stakeholders must maintain a proactive posture in engaging this critical international infrastructure partner. Existing industry fora must evaluate their charters, membership and commitments, in light of the stakeholder and internal industry needs. Existing industry fora must, as appropriate, be either willing to make charter and membership representation adjustments, or be supportive of sister organizations playing new complimentary roles. Private sector companies must provide expert and leadership resources to champion new governance functions.

---

[8] IEEE ROGUCCI Report Recommendation No. 4, Best Practices and Trusted Information Sharing
[9] IEEE ROGUCCI Report Recommendation No. 5, New International Governance

ICT Standard for the International Financial Services Sector[10]

Maturity Level: *MODERATE*
Sectors: *Financial Sector*
Abstract: *The world's international undersea communications cable infrastructure continues to operate at highly reliable levels and continues to provide tremendous service to the financial services sector. Recommendations 4 and 7 position the communications industry to better share information and provide needed information to the financial sector, respectively. Correspondingly, this Recommendation calls on the financial sector to better define its needs and expectations, and to develop a structure to organize operational risk guidance that allows both providers and users to manage their growing global dependency on GUCCI.*
Challenges: The international financial sector must recognize GUCCI reliability as a strategic priority for the stability of its operations. The international financial institutions must commit operational risk managers to developing the details of global guidelines. The financial sector and international communications industry must commit to a partnership to develop a core standard that both can agree on. The financial sector members must voluntarily implement the developed core standard. The world's international financial authorities must utilize these standards in their determination of ratings and other stability-related decisions.

Recognize Catastrophic Loss of GUCCI Grand Challenge

Maturity Level: *LOW*
Sectors: *ICT, Essential Government Services*
Abstract: *Nearly 100% of the world's inter-continental electronic communications traffic is carried by the undersea cable infrastructure. Terrestrial based routes would leave continents in isolations. The probability of such a failure is very low, however, it is not zero. The impact of such a failure on international security and economic stability could be devastating. The pace at which technology has been adopted and then depended upon is unprecedented in history. It is unclear if civilization can recover from the failure of a technology that has been so rapidly adopted without a backup plan. Without GUCCI, the world's economic financial market would immediately freeze. But what would happen next? What are the options? What can be done to best prepare for this unlikely, but possible event?[11]*
Challenges: Governments and other stakeholders must encourage academic and private sector research to ensure appropriate resources are focused on this global challenge. Scientists and engineers must be devoted to developing alternatives. Stakeholders must conduct planning scenarios that consider true worst-case scenarios. The finance sector can play a lead role.

Internet Governance

Maturity Level: *MEDIUM*
Sectors: *ICT*
Abstract: *What role do nation-states, global corporations and civil societies have in shaping the Internet? The UN's Information Society initiative has begun to define governance, however, control is sharply contested by diverse political and ideological perspectives.[12] Organizations*

---

[10] IEEE ROGUCCI Report Recommendation No. 6, International Communications Infrastructure Standard for the Financial Sector
[11] IEEE ROGUCCI Report Recommendation No. 12, Recognize Catastrophic Loss of GUCCI Failure as Grand Challenge.
[12] United Nations-initiated World Summit on the Information Society (WSIS), 2005.

such as the Internet Society (ISOC), and its Internet Engineering Task Force (IETF); the Internet Corporation for Assigned Names and Numbers (ICANN) and its Internet Assigned Numbers Authority (IANA) and the World Wide Web Consortium (W3C) provide structure,, standards and policy for the Internet . and world wide web. The United States has been the incubator for most of the early development of the Internet and currently retains disproportionate influence over its governance. Arguments are made that due to the continued rapid development of the Internet, that the needs of the global community can best be served with a governance model that ensures streamlined decision-making and efficiency. Others insist that given the importance of the Internet to societies around the world, a more international representation and influence is needed.

Challenges: Dialogue is needed to better understand what needs are not being met with the current governance. Other considerations are what representation is appropriate and how efficiently can such representation operate.

Protecting Youth in Cyber Space

Maturity Level: *LOW-MEDIUM*

Sectors: *Media*

Abstract: *The Internet offers countless benefits but can have a downside. The protection of youth remains an unmet challenge of the digital age. Parents around the world are worried about the changed behaviors they observe from Internet addictions – not just to pornography and gaming, but to the general obsession for being up to date with an array of social networking expectations. Schools observe rising obesity rates, families complain of anti-social behavior, students neglect studies, and children are exposed to offensive content. With advanced 3G+ mobile technologies, mobile phones are now another avenue for concern.*

Challenges: *Online youth protection can have a health approach, given the cyber bullying, obesity and anti-social behaviors that are being observed around the world. Existing rating systems can be used to offer options. Need better leadership to champion.*

Use of ICT for Humanitarian Aid

Maturity Level: *LOW*

Sectors: *Essential Government Services*

Abstract: *One of the fundamental challenges of international cooperation in cyberspace is the understandable lack of trust among parties. However, international cooperation in the use of ICT for humanitarian aid is a trust-building measure with tremendous benefits to the people around the world. This cooperation can take many forms. Examples include the IEEE Humanitarian Technology Challenge (HTC) that promotes rural health office connectivity, mutual aid agreements that enable the resources of one country to be available as "insurance" to another in a catastrophe,[13] and the many innovative private sector initiatives such as cyber awareness and education, emergency mobile ad hoc networks and search and rescue support using advanced wireless technology.*
These and other efforts make an important difference, yet because the application types and needs are endless, the impact is for only a sliver of the opportunities that abound.

Challenges: *The opportunities for international cooperation in the use of ICT for humanitarian aid needs further exploration. Consideration should be given for the protocols for providing assistance in catastrophes, developing the market forces for sustainable private sector*

---

[13] See Formal Mutual Aid Agreements, Recommendation No. 3, European Commission *Availability and Robustness of Electronic Communications Infrastructure (ARECI).* 2007.

investment and respect for the cultural values of the people being served.

Privacy and Data Mining

Maturity Level: *LOW*
Sectors: *Media*
Abstract: *Swift progress is being made in many aspects of society as a direct result of the use of ICT. There are many benefits from the dramatic breakthroughs in access to education, efficiencies in productivity, new opportunities and many other areas. However, at a personal level, a trade-off for being an active netizen can be vast exposure of personal information and loss of privacy. Often this information is offered willingly, though perhaps ignorantly. In other cases information is aggregated with data mining technique and subsequently privacy is violated. But even for official business new exposure is created. Both governments and commercial enterprises repeatedly promise secure transactions and protections, but the protection they offer is relative and not absolute. Further, companies that have access to your online behavior can exploit it in the marketplace, accelerating the compromise of personal information protection. Data mining has become a tool for national security, commerce and crime.[14] Cyberspace lacks international policies that define, track and prevent privacy violations.*
Challenges: *Netizens need to be aware of the implications of their online activities. Nation-states would benefit from coordination in policy and practice.*

---

[14] 2008 Report to Congress *Data Mining: Technology and Policy* The DHS Privacy Office, December 2008.