“Securing Access to the Internet and Protecting Core Internet Resources in Context of Conflicts and Crises”

- **Contribution from:** Dino Cataldo DELLACCIO: IGO Representative to the MAG of the UN-IGF, and Co-Lead of the Dynamic Coalition on Emerging Technologies and Dynamic Coalition on Blockchain Assurance and Standardization

- **Date:** June 11th, 2025

Question 1: Refinements to the Problem Statement

The current problem statement provides a solid foundation but could benefit from several clarifications and additions to enhance its scope and precision.

Suggested Refinements

- Temporal Scope Clarification: The statement should explicitly address both prevention and response phases, specifying that roles and responsibilities apply during pre-crisis preparedness, active crisis management, and post-crisis recovery.
- Stakeholder Categories: The term "multistakeholder Internet community" is a familiar concept to the members of the UN-IGF. However, new members and/or other stakeholders could benefit from explicitly naming the key categories: governments, private sector entities, technical community, civil society organizations, academia, and international organizations.
- Geographic Considerations: The statement should acknowledge that "conflicts and crises" encompass both localized incidents and global disruptions, as well as different types of conflicts including armed conflicts, natural disasters, and cyber warfare.
- Human Rights Framework: The statement would benefit from explicitly referencing the human rights dimension, particularly the right to freedom of expression and access to information during crises.

Proposed Revised Statement

"There is a clear and pressing need to clarify the roles, responsibilities, and coordination mechanisms of the multistakeholder Internet community—including governments, private sector, technical community, civil society, academia, and international organizations—in securing core Internet resources and ensuring civilian access to the Internet before, during, and after conflicts, crises, and emergency situations, while upholding human rights and international law."

Question 2: Defining Core Internet Resources

The Global Commission on the Stability of Cyberspace (GCSC) has provided what is considered the most comprehensive and authoritative definition of critical Internet Resources/Infrastructure through its concept of the “Public Core of the Internet”. This definition has been adopted by the OECD and other international organizations as a standardized framework.

The GCSC defined the Public Core of Internet to include:

(i) Packet Routing and Forwarding (i.e., equipment, facilities, information, protocols, and systems that facilitate transmission of communications; Internet Exchange Points; Peering and core routers of major networks; Systems for routing authenticity and network defense);

(ii) Naming and Numbering Systems (i.e., Domain Name System operations including registries and name servers; DNSSEC cryptographic signing infrastructure; WHOIS information services for domain registration data; IP address allocation and management systems);

(iii) Security and Identity Infrastructure (i.e., Cryptographic mechanisms that enable secure communications; Digital certificate authorities and public key infrastructure; Authentication systems that verify identity across networks); and

(iv) Physical Transmission Media (i.e., Submarine cables, fiber optic networks, and terrestrial infrastructure; Data centers and network facilities that house critical equipment; Hardware supply chains for networking equipment).

Question 3: Key Challenges in Protection During Crises

Technical Vulnerabilities: Infrastructure Fragility: BGP Security Weaknesses: Single Points of Failure.

Governance and Coordination Challenges: Jurisdictional Complexity: Multi-stakeholder Coordination: Information Sharing Barriers.

Conflict-Specific Challenges: Weaponization of Internet Shutdowns; Targeting of Civilian Infrastructure; Economic and Humanitarian Impact.

Question 4: Relevant Existing Norms and Agreements

International Legal Frameworks: International Humanitarian Law (The Geneva Conventions and Additional Protocols); UN Charter and Sovereignty Principles; Law of the Sea Convention (i.e., for submarine cables).

Cybersecurity Norms and Agreements: UN GGE 2015 Consensus Report; Paris Call for Trust and Security in Cyberspace; Regional Cybersecurity Frameworks.

Technical Standards and Best Practices: ISO Standards **(**27001; 22301; 27032; 22320; 27033; and 31000)**;** NIST Cybersecurity Framework; Internet Engineering Task Force (IETF) Standards.

Question 5: Effectiveness and Notable Gaps: Norm Implementation Challenges; Attribution Difficulties; Rapid Technology Evolution; Civilian Protection Mechanisms; Enforcement Mechanisms; Technical Capacity Disparities; Private Sector Integration; Real-time Coordination.

Question 6: Successful Practices and Approaches

Technical Resilience Measures: "Anycast" Implementation; Internet Exchange Point Development; Diversified Connectivity.

Governance Innovations: ICANN's Multistakeholder Model; Emergency Response Coordination; Regional Cooperation Frameworks:

Crisis Response Examples: Ukraine Conflict Digital Resilience; Post-Disaster Recovery.

Question 7: Background Materials and Resources

Academic Research and Analysis

- Internet Governance Research Project Case Studies - Comprehensive analysis of multistakeholder governance models: https://publixphere.net/i/noc/page/Internet_Governance_Research_Project_Case_Studies
- Multistakeholder as Governance Groups: Observations from Case Studies - Detailed examination of governance group effectiveness: https://itsrio.org/wp-content/uploads/2017/01/2015-NoC-Multistakeholder-as-Governance-Groups-SSRN-id2549270.pdf
- Strategic Monitor 2019-2020: Conflict in Cyberspace - Analysis of cyber conflict dynamics: https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/conflict-in-cyberspace/

Policy and Legal Analysis

- Safeguarding Civilian Internet Access During Armed Conflict - Legal analysis of international humanitarian law applications: https://journals.library.columbia.edu/index.php/stlr/article/view/8056
- Internet Governance in an Age of Conflict - Analysis of governance challenges: https://www.linkedin.com/pulse/internet-governance-age-conflict-models-power-adelino-machado-won0f
- European Parliament Internet Governance Brief- Comprehensive policy overview: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766272/EPRS_BRI(2024)766272_EN.pdf

Reports and Best Practices

- IGF 2021 Best Practice Forum Cybersecurity Submission - UN analysis of cybersecurity norms: https://documents.unoda.org/wp-content/uploads/2022/01/IGF2021-BPF-Cybersecurity-Submission-OEWG.pdf
- Best Practice Forum Cybersecurity (IGF 2024) - Latest capacity building findings: https://cybilportal.org/publications/igf-2024-best-practice-forum-cybersecurity-mainstreaming-capacity-building-for-cybersecurity-trust-and-safety-online/
- The Internet Under Attack- Chatham House analysis of Internet resilience: https://www.chathamhouse.org/2024/08/internet-under-attack

Technical Infrastructure Resources

- Dive Deep into Protecting Submarine Cables - Comprehensive infrastructure protection analysis: https://www.diplomacy.edu/blog/dive-deep-into-protecting-submarine-cables/
- Creating Accountability for Global Cyber Norms - CSIS analysis of norm implementation: https://www.csis.org/analysis/creating-accountability-global-cyber-norms
- Cyber Stability and Critical Infrastructure - Analysis of conflict impacts: https://www.secdev.com/RMCS/2024_06_26-Critical-Infrastructure-EN.pdf

Implementation Frameworks

- NIST Cybersecurity Framework 2.0 Implementation Examples - Practical implementation guidance: https://www.nist.gov/document/csf-20-implementations-pdf

- Emergency Services Sector Cybersecurity Framework - Sector-specific guidance: https://www.cisa.gov/resources-tools/resources/emergency-services-sector-cybersecurity-framework-implementation-guidance

Crisis Response and Monitoring

- 2023 Was the Worst Year for Internet Shutdowns - Comprehensive shutdown monitoring: https://time.com/6978512/internet-shutdowns-india-report/
- Why Shutting Down the Internet in Wartime Is a Humanitarian Failure - Humanitarian impact analysis: https://pulse.internetsociety.org/blog/why-shutting-down-the-internet-in-wartime-is-a-humanitarian-failure
- Access to Internet Infrastructure is Essential - EFF analysis of wartime access: https://www.eff.org/deeplinks/2024/03/access-internet-infrastructure-essential-wartime-and-peacetime