The Marconi Society

marconisociety.org

Submission on the WSIS+20 Zero Draft

The Marconi Society's Internet Resilience Institute welcomes the Zero Draft and strongly supports its emphasis on digital inclusion, multistakeholder cooperation, and alignment with the Global Digital Compact (GDC). Building on the IGF 2025 Workshop "Internet Resilience: Securing a Stronger Supply Chain"[1], we respectfully submit the following observations and suggested improvements to strengthen the text's treatment of Internet resilience.

Key Paragraphs of Relevance

Para. 16 (Confidence, security, and trust in ICTs)

Strength:	Recognises the importance of enabling environments and trust.
Shortfall:	Lacks explicit reference to resilience of core Internet functions and infrastructures (e.g., routing, DNS, IXPs) and their interdependence.
Improvement:	Add language underscoring the need for cross-sectoral collaboration to secure and maintain resilience of these foundational systems.

Paras. 33–35 (Digital economy, supply chains, market concentration)

Strength:	Acknowledges supply chains and risks of concentration of capacity/market power.
Shortfall:	Does not highlight digital supply chain dependencies (hardware, software, services) that can undermine resilience.
Improvement:	Emphasise transparency and diversity of digital supply chains, consistent with global development and security aims.
Paragraph 35:	*Current text* : "…tackle concentrations of technological capacity and market power…"

[1] https://intgovforum.org/en/content/igf-2025-ws-139-internet-resilience-securing-a-stronger-supply-chain

	Proposed edit: Insert after "market power": "…and strengthen the transparency and diversity of digital supply chains, recognising their role in ensuring resilience and trust…"

Paras. 47 & 49–54 (Disaster response, environment, sustainability)

Strength:	Recognises ICT roles in disaster response and environmental monitoring.
Shortfall:	Overlooks dependencies between digital infrastructure and other critical sectors (energy, transport, finance) that are essential for resilience.
Improvement:	Call for integrated risk assessments across sectors, leveraging WSIS Action Lines, to ensure continuity of connectivity and services.
Paragraph 47:	*Current text*: "…address risks associated with natural disasters and facilitate humanitarian assistance…" **Proposed edit**: Add at the end of the paragraph: "We further recognise the critical interdependence of digital infrastructure with other essential sectors such as energy, transport, and finance, and the need for integrated risk assessments across sectors to ensure continuity of connectivity and services."

Paras. 62–65 (Cybersecurity capacity-building)

Strength:	Affirms multistakeholder cooperation for security.
Shortfall:	Needs stronger recognition that resilience is not only about cybersecurity but also continuity of operations and recovery from disruptions.
Improvement:	Encourage IGF intersessional work (BPFs, DCs) to continue surfacing good practices on resilience, incident response, and cross-sectoral coordination.

Paras. 113–118 (Internet Governance Forum)

Strength:	Establishes the IGF as permanent.
Shortfall:	The IGF's role in supporting resilience through multistakeholder cooperation and technical community expertise is not sufficiently noted.
Improvement:	Highlight the IGF as the central platform to advance multistakeholder dialogue on Internet resilience, including hyperscaler engagement, SMEs' continuity, and cross-border dependencies.
Paragraph 113:	*Current text*: "…enhanced multistakeholder discussion of relevant issues…" **Proposed edit**: Insert after "relevant issues": "…including resilience of Internet infrastructures, supply chains, and engagement of major platforms and hyperscalers in supporting continuity and security of the digital ecosystem…"

Paras. 126 & 129 (WSIS Forum and Action Lines)

Strength:	Calls for continued WSIS Forum and roadmaps.
Shortfall:	Misses an opportunity to link Action Lines to resilience priorities (e.g., C2: Information infrastructure, C5: Building trust and security, C6: Enabling environment).
Improvement:	Ensure Action Line roadmaps integrate resilience, mapping of dependencies, and sectoral interlinkages in their targets and indicators.

Paras. 140–145 (Follow-up and review)

Strength:	Calls for convergence with GDC, role of CSTD and ECOSOC.
Shortfall:	Risks fragmentation of resilience discussions if IGF outcomes are not systematically channelled.

Improvement:	Reaffirm that IGF outputs on resilience, supply chains, and hyperscaler engagement should directly feed into UNGIS, CSTD, and ECOSOC reviews.
Paragraph 145:	*Current text (para. 145)*: "…requests the Commission further to review and assess progress made in implementing the Global Digital Compact commitments…" **Proposed edit**: Insert after "…Global Digital Compact commitments": "…including specific consideration of Internet resilience, supply chain dependencies, and cross-sectoral cooperation…"

Conclusion

The Zero Draft provides a strong basis for reaffirming the WSIS vision. However, to ensure a safe, secure, and resilient digital future, the text should more explicitly reference resilience of Internet infrastructures, cross-sectoral dependencies, supply chains, and hyperscaler engagement, while embedding these themes in the mandates of the IGF and WSIS Action Lines. These improvements require no new structures, only clearer linkages within the existing UN and WSIS architecture.