WSIS FORUM 2026 | 6-10 July 2026 Geneva, Switzerland

Session Outcome Document

The Global Shield: Collaborative Cyber Resilience for global e-Commerce and logistics

Universal Postal Union

Monday 06 July 2026 – 11:00 am CEST, Room K1, ITU HQ

https://www.itu.int/net4/wsis/forum/2026/Agenda/Session/324

Key Issues discussed:

- **The Interconnected Vulnerability of Global E-Commerce:** The session highlighted how modern e-commerce depends entirely on an invisible, deeply digital, and borderless engine of logistics and postal networks. Because these systems are interconnected, a cyber vulnerability in one single national operator or logistics node presents a systemic risk to the entire global supply chain.
- **Industrialized Cybercrime and Malicious AI:** Panelists discussed how modern cyberattacks are no longer random; they are orchestrated by highly structured criminal networks operating an industrial-scale corporate supply chain. Furthermore, malicious AI acts as a massive threat multiplier, enabling even low-skilled attackers to rapidly discover infrastructure weaknesses and launch complex, automated campaigns.
- **Filtering Threat Intelligence for Niche Vulnerabilities:** The discussion focused on how operators can manage the overwhelming volume of generic threat data. Because the postal sector uses unique vertical technologies—such as automated mail and parcel sorting systems—a coordinated response allows the sector to filter out the noise and deliver highly curated, relevant threat intelligence specific to logistics infrastructure.
- **Diagnosis of Global Cyber Maturity:** Findings from the comprehensive UPU Cybersecurity Survey (compiled from 152 member-operator responses) were analyzed. While basic measures like web encryption show strong global adoption, critical operational areas—such as formal incident-response and crisis-management plans—remain severely underdeveloped across multiple regions.
- **The "Capacity Gap" vs. Awareness:** Data demonstrated that global postal operators are overwhelmingly aware of cybersecurity risks and existing secure platforms. However, the true binding constraint facing vulnerable operators is a significant lack of operational capacity, dedicated funding, and technical training, especially as cyber workloads heavily outpace current budget growths.
- **Translating High-Level Policy into Inclusive Resilience:** The panel examined how global policy frameworks, such as the Universal Postal Union's Dubai Congress mandates,

provide the necessary legal and strategic foundation to build secure digital environments. These frameworks ensure that developing countries are not left digitally vulnerable, promoting equitable global economic inclusion.

- **Operationalizing Threat Intelligence via POST-ISAC:** Panelists discussed the practical deployment of platforms like the UPU's POST-ISAC. It was emphasized that moving from abstract threat awareness to real-time, cross-border intelligence sharing requires building a strong culture of trust and shared data protocols among sovereign postal operators.
- **Securing Digital Space via .POST Infrastructure:** The role of the .POST top-level domain and SECURE.POST platforms was highlighted as a concrete mechanism to turn international policies into a functional, highly secure digital ecosystem, shielding final-mile delivery and transactions from exploitation.
- **Strategic UPU Action Points for the Future:** The discussion concluded with five concrete strategic pathways for international organizational support: bridging the capacity gap through direct funding relief, productizing standardized cyber-hygiene training, brokering cross-border incident-response and recovery layers (e.g., CERT networks), prioritizing aid by residual risk outliers rather than just standard development tiers, and validating self-reported maturity scores with practical readiness checks.

Key Outcomes of the session

- **key insights and findings:**
    - **The Capability Paradox:** Data from 152 member-operators confirmed that while basic awareness and web-encryption adoption are exceptionally high globally (66%), practical operational defense is severely lacking—with only 41% of operators possessing formal incident-response plans and only 35% affiliated with an active national response team.

    - **The Shift to "Collective Defense":** The session established a unified consensus that modern, interconnected e-commerce logistics cannot be protected using siloed national security models; a cyber vulnerability in a single node threatens the entire global supply chain, necessitating a shift toward shared, borderless ecosystem defense.
    - **Niche Operational Security Capabilities:** A key insight from the front lines showed that the postal sector's widespread physical and digital footprint gives it a unique tactical advantage. National operators have deep, vertical expertise in specialized automated transit technologies, making them uniquely capable of spotting, identifying, and escalating emerging supply-chain threat scenarios with much higher precision than general cybersecurity frameworks.
    - **The True Constraint is Capacity:** The primary barrier to global postal cyber-resilience is not a lack of risk awareness, but a severe capacity deficit. 69% of operators face a rapidly growing cyber workload, yet only 49% see corresponding budget growth, creating a "capacity scissors" gap that disproportionately leaves developing nations vulnerable.

- **announcements, launches, or new initiatives presented during the session**

- **The UPU Cybersecurity Position Paper Framework:** The session served as the formal presentation platform for the UPU's forthcoming Cybersecurity Position Paper, establishing the 5 strategic pillars for future global postal defense (Direct Cyber-Hygiene Funding, Productized Training Curriculums, Shared SME Pools, Cross-Border Response/Recovery Layers, and Risk-Outlier Triaging).

- **Operationalizing POST-ISAC Capabilities:** A roadmap was highlighted for expanding the UPU's POST-ISAC platform from an information-sharing repository into a live, real-time threat-intelligence-sharing network capable of pushing active alerts directly to national operators' front lines.

- agreements, collaborations, or commitments made
    - **Commitment to WSIS Action Line C7 (E-Business):** The UPU re-affirmed its institutional mandate as a co-facilitator of Action Line C7, committing to actively bridge the technical divide between high-maturity operators and vulnerable, developing-market digital economies.
    - **Leveraging Economies of Scale through POST-ISAC:** Participants committed to utilizing the POST-ISAC platform to break the traditional, "island-based" model of isolated national defense. By collaborating globally, operators agree to leverage the network's massive scale to drastically reduce the cost of cybersecurity threat-hunting and technical training, ensuring that even under-funded, smaller operators can access high-quality protective barriers.

Key Recommendations and Forward-Looking Actions

- International organizations and stakeholders should redirect technical assistance resources to target the operational "capacity scissors" gap. Future initiatives must prioritize direct financial support and technical budget relief for cyber-hygiene execution rather than redundant, high-level risk awareness campaigns.
- To address the severe global deficit in technical staff skills, a standardized, universally accessible cyber-hygiene training curriculum must be institutionalized. This should be backed by a shared pool of international Subject Matter Experts (SMEs) to provide targeted operational training to vulnerable operators on demand.
- Global frameworks must expand their focus beyond mere attack prevention to embrace active resilience. Stakeholders should collaborate to broker mutual-assistance, CERT-style regional networks and publish shared, standardized incident-response and disaster-recovery playbooks to handle active ransomware and systemic supply chain threats.
- Digital development assistance should move away from rigid, purely geographic or standard macroeconomic development tiers. Strategic aid and intervention resources must be dynamically prioritized and triaged toward "high residual risk outliers"—specifically identifying mid-development nations that report near-zero technical cyber-maturity.
- To ensure true structural resilience heading toward WSIS 2035, the international community must treat self-reported security scores as a foundational baseline rather than a final verdict. Frameworks must integrate mandatory, hands-on digital assessments and incident-readiness pressure tests to validate the real-world defense capabilities of highly ranked networks.