GLOBAL HUMANITARIAN POLICY FORUM 2021

UNITED NATIONS FOUNDATION

OCHA

The Humanitarian Implications of Cyber Threats

Friday, December 10, 2021 | 10:30 – 11:45 am EST

Virtual Session – Register Here

Overview:

Harmful cyber operations ('cyber-attacks') have become a critical security threat. As the global digital transformation forges ahead, so too do the risks associated with our ever-more interconnected and digitised world. Along with much of the rest of the world, humanitarian functions are moving into the digital space, and in doing so are helping to unlock the societal and economic benefits of modern information technologies. But humanitarian operations are increasingly coming under cyber-attack, and evidence suggests that they are not adequately prepared to meet many of the cyber threats of today – let alone tomorrow. From disabling ransomware attacks on hospitals to shutdowns of electrical grids, electoral interference campaigns, and the stoking of geopolitical tensions through targeted human influence operations, the impacts of harmful cyber operations, can be devastating.

For humanitarians, cyber threats come in three contexts: to critical infrastructure that serve our communities, in the political and social environment where we work, and in the context of our own organization readiness and preparedness for attacks. The opportunities of new technologies and the growing digitalization of essential services is accompanied by a stark rise in cyberthreats against critical infrastructure sectors that provide services to the public, such as energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications, and electoral processes.

While vulnerabilities are growing, cybersecurity preparedness, organizational readiness and digital literacy remain limited. Poor 'cyber hygiene' continues to characterize many institutions active in the humanitarian space, ranging from NGOs to government agencies, and IT professionals across sectors are becoming increasingly pessimistic about their organizations' cyber resilience. Meanwhile, global divides in cybersecurity maturity levels risk placing vulnerable populations at even greater exposure to the damaging impacts of cyber threats.

The panel will consider how the humanitarian system can more effectively combat cyber threats. Experts from across sectors and disciplines will discuss the myriad of threats posed by today's cyber landscape to humanitarians, their organizations and operations, and to people affected by humanitarian crises. They will reflect on the avenues pursued by various actors to build trust and stability in cyberspace. And they will highlight gaps and possible ways forward for the humanitarian sector to mitigate and respond to cyber threats, including legal, technical, organizational, capacity-building and cooperation measures.

Guiding Questions:

- What are the main cyber threats to humanitarian action, and what is their impact?
- How prepared are humanitarian organizations to face cyber-security challenges?

- How has the COVID-19 pandemic contributed to the cyberthreat landscape for humanitarian action?
- How can humanitarians mitigate and respond to cyber threats more effectively?

Moderator:

Kristen Eichensehr, Director, National Security Law Center at the University of Virginia School of Law

Panelists:

- **Nemanja (Neno) Malisevic,** Director of Digital Diplomacy at Microsoft
- **Delphine van Solinge,** Adviser on Digital Risks for Populations in Armed Conflicts in the Protection Division of the International Committee of the Red Cross (ICRC)
- **Sara Wahedi,** CEO & Founder of Ehtesab, Afghanistan's first civic-technology startup, and the Ehtesab app, which provides near real-time alerts on security and city-service issues in Kabul, Afghanistan
- **Robert Young,** Legal Counsel at Global Affairs Canada, international lawyer on cyber issues and international law, and humanitarian/protection specialist
- **Jonas Belina**, PhD, Diplomatic Officer, Humanitarian Diplomacy