World Health
Organization

WHO Information Session - Update on WHO deliberate Event Preparedness and Response

10 December 2024 | 9:00–9:45 AM | Palais des Nations Room V

The Fifth Session of the Working Group on the Strengthening of the BWC
02–13 December 2024

Concept Note

Introduction: In the increasingly fragmented and polarized world in which we live, the public health service carries an important responsibility to protect its people from deliberate events with intention to harm. In the past decade, with the creation of the WHO Health Emergencies Programme, WHO has significantly enhanced its capacity to respond to major events with rapid, agile, and scalable actions under a 'No-regret' policy. Our strength lies in our presence in countries where we maintain close working relationships with the Ministries of Health and their emergency coordination mechanisms. Additionally, our strategic three-level structure supports our countries effectively.

Overview: In line with WHO mandates set by its Constitution, International Health Regulations, and more recently by the 14th General Programme of Work, our strategic approach spans around the three main pillars: 1) Development of WHO deliberate event response and surge capacity, 2) country capacity building, 3) Deliberate event preparedness and readiness and interagency response coordination. The areas of work seek advice from the Health-Security Interface Technical Advisory Group (HSI-TAG).

1) Development of WHO deliberate event response and surge capacity
- Development of WHO response and surge capacity: Based on its conceptual framework, the development of a CBRN surge capacity roster from the WHO workforce is achieved through the formal WHO deployment mechanism and specialized training by partner agencies. Operationalization involves developing standard operating procedures (SOPs) and conducting simulation exercises. This includes engaging Emergency Medical Teams, Standby Partners, and other international agencies.
- Establishment of the WHO Deliberate Event Task Force: WHO functions are seamlessly integrated across the organization to ensure rapid risk assessment, activation of the Incident Management system, and scalable response as outlined in WHO's Emergency Response Framework.

2) Country capacity building
- Raising awareness: WHO raises awareness through the International Health Regulation's Joint External Evaluation, web and social media-based advocacy, standard-setting by guidance, factsheets, and frequently asked questions (FAQ).

- Training and Exercises: WHO develops, conducts, and supports simulation exercises and training programs to enhance national preparedness.
- National Self-Assessment Tool: WHO enhancement of the health and security interface involves identifying and addressing gaps in national readiness through the National Self-Assessment Tool (NSAT). This tool is designed to complement the Joint External Evaluation and the IHR State Parties Self-Assessment Annual Report.

3) Deliberate event preparedness and readiness and interagency response coordination

- Early detection, verification and assessment: WHO strengthens detection of potential signals and collection of information through International Health Regulation, open source (AI-powered EIOS platform) and other channels.
- International partnerships and networks: WHO strengthens inter-agency preparedness and response through the United Nations agencies coordinated by UN Biorisk working group co-led by WHO and UNODA, international agencies and intergovernmental mechanisms, networks, partnership and WHO Collaborating Centers.
- Ukraine Examples: WHO trains public health and frontline responders and distributes personal protective equipment, decontamination facilities and medical countermeasures.
- Foresight: WHO utilizes strategic foresight to anticipate and prepare for potential deliberate events.

Addressing the new challenges: The pandemic has highlighted gaps in our preparedness and response capacities. The rapid spread of misinformation and disinformation has further complicated efforts to manage the crisis, undermining public trust and compliance with health measures. This necessitates a robust approach to countering false information and ensuring accurate, timely communication. Moreover, cyberattacks pose an additional threat to health security, requiring robust cybersecurity measures to protect sensitive health data and ensure the integrity of health systems, especially when they are stretched and most needed during health crises. WHO tackles these emerging threats in addition to the traditional CBRN threats.

- WHO reports that outline responses to cyber-attacks on health care and the rise of disinformation in public health emergencies

- The WHO Director-General's remarks at Meeting of the UN Security Council on threats posed by ransomware attacks against hospitals and other health-care facilities and services

- Questions and answers: Disinformation and public health

- Online Training OpenWHO: Infodemic Management: Addressing health misinformation and disinformation

- Questions and answers: Cyber-attacks on critical health infrastructure