Responsible State Behaviour in Cyberspace

Introduction

In today's interconnected world, states face an escalating array of malicious ICT incidents that threaten critical infrastructure, disrupt essential services, and undermine national security. The international community has developed a framework for responsible state behaviour in cyberspace—comprising voluntary norms, international law, confidence-building measures (CBMs), and capacity building. This framework provides states with guidance on managing cyber threats, fostering international cooperation, and responding to incidents effectively.

However, implementation remains uneven. Many states, particularly small and developing nations, lack the institutional mechanisms, technical expertise, and procedural frameworks to operationalize these commitments.

For this challenge, we will examine the fictional state of "Mini-Garous," a small developing nation that recently completed the UN's survey on norms implementation (Attached). Mini-Garous has demonstrated commitment by documenting its cyber posture and existing legal frameworks. However, the government explicitly noted its inability to implement the norm 13H on "*response to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at another State's critical infrastructure emanating from their territory, taking into account due regard for sovereignty*". This honest assessment creates an opportunity: targeted capacity building that can bridge the gap between political commitment and operational capability.

Background Information: Mini-Garous

Mini-Garous is a small landlocked nation with a population of 850,000. The country has one of the best Constitutions, in the world with wide and progressive protections for citizens and inhabitants. It has recently digitized several government services and expanded internet connectivity and taken steps to address the gender digital divide, with critical dependencies including hydro power management systems, banking infrastructure connected to international financial networks, and a new identity card.

Mini-Garous established a National Cyber Coordination Centre (NC3) in 2023, operating with 12 personnel—only three with technical incident response training, and all three being men belonging to the same majority demographic grouping in Mini-Garous. The government endorsed the UN framework on responsible state behaviour and has taken concrete steps toward implementation, though significant gaps remain.

Critical Implementation Gap Identified:

Mini-Garous explicitly noted its inability to implement **the norm on states responding to appropriate requests for assistance from other states**.

Mini-Garous's honest self-assessment in the UN survey creates a clear mandate for capacity building.

Objective and Key Tasks

Serve as capacity building providers for Mini-Garous. Utilize your understanding of the UN framework on responsible state behaviour in cyberspace, and guidance for incident response to demonstrate its application through analytical skills, showcasing your insights and conclusions based on the findings regarding Mini-Garous's capacity needs and the international assistance request challenge.

In your presentation, please cover the following questions:

1. **How does Mini-Garous's existing legal and institutional framework (Cybercrime Act, National Key Point Strategy, Department of State Security mandates) create a foundation for implementing international assistance request capabilities, and what additional elements are needed?** Identify how existing structures can be leveraged and what gaps remain.
2. **What specific guidelines and procedures should Mini-Garous establish to request international assistance following malicious ICT incidents?** Identify the core elements of an assistance request framework, including when to trigger requests, which domestic agencies must coordinate, what information to include (technical, diplomatic, legal), and how to balance transparency with human rights, data privacy and sovereignty concerns.
3. **What are Mini-Garous's critical capacity gaps that prevent effective assistance requests, and what concrete capacity building interventions will address each gap?** Based on Mini-Garous's self-identified lack of expertise, map specific technical, institutional, legal, diplomatic, and human capacity deficiencies to targeted solutions.
4. **What is your structured capacity building programme, including specific training components, target audience, institutional support, legal assistance, technical tools, and implementation timeline?** Provide detailed, actionable recommendations showing how each component directly enables Mini-Garous to operationalize the norm, avoiding generic suggestions.
5. **How will your programme help Mini-Garous build international cooperation mechanisms and relationships necessary for effective assistance requests?** Address how Mini-Garous will identify potential assistance providers, establish communication protocols, participate in confidence-building measures, and leverage existing cooperation frameworks (regional organizations, bilateral partners, technical communities).
6. **In conclusion, evaluate whether Mini-Garous will be positioned to implement the norm on requesting international assistance following your capacity building programme, and recommend specific next steps for implementation and testing.**

5th November 12:00 CET / 16:30 IST is the deadline for you to hand in a video of max. 3min to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the final submission moment and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Contributor

Contributor for this challenge is the United Nations Institute for Disarmament Research (UNIDIR). UNIDIR generates knowledge and promotes dialogue on disarmament and security challenges, supporting states in implementing the UN framework on responsible state behaviour in cyberspace through research, convenings, and capacity building initiatives. UNIDIR's Cyber Policy Portal provides resources on norms implementation, legal frameworks, and confidence-building measures, while facilitating regional dialogues that enable states to share experiences and coordinate approaches. Through this challenge, UNIDIR seeks to identify innovative, practical approaches to operationalizing international cyber cooperation—particularly for small and developing states navigating complex technical and diplomatic landscapes.