Strengthening regional cyber norms guidance through practice-based approaches: the case of ransomware

OEWG Side Event

**Date:** Monday, 8th July 2024, 1315 - 1445 pm  
**Location:** Permanent Mission of Estonia to the UN  
*Three Dag Hammarskjöld Plaza, 6th Floor, 305 East 47th Street, New York, N.Y. 10017*  
**Registration:** RSVP by sending an email to LouiseH@rusi.org

In July 2023, States recognised for the first time that ransomware is an emerging threat to international peace and security as part of the Annual Progress Report of the OEWG. A year later, the question remains as to what the next step for a practice-oriented dialogue is on how norms connect with emerging threats such as this.

Throughout the past years, countries in Latin America and Caribbean have been dealing with an increasing number of ransomware incidents. While most of the public and international attention has revolved around specific incidents, such as Costa Rica, other States such as Dominican Republic, Brazil, Peru, Colombia, Chile, and many others have experienced the disproportionate impact of ransomware incidents against government and other critical national infrastructure.

How can States better leverage their experience in responding to specific cyber threats such as ransomware with the operationalisation of the framework of responsible state behaviour in cyberspace?

With the aim of enhancing a practice-based and regionally sensitive norms guidance, RUSI, Estonia, EU Cyber Net/LAC4, Chile and the Dominican Republic would like to invite States from the region for a closed workshop on Monday **8th July 2024 from 1315 – 14:45**. The side event will focus on responses to ransomware incidents in Latin America and the Caribbean and invite representatives to share experiences and collectively map how a cross-cutting regional concern, such as ransomware, can inform regional norms guidance.

The side event will be divided into two parts. The first part of the event will consist of an open moderated dialogue. Chile and the Dominican Republic will share their views on how lessons learned from responding to such incidents can inform the operationalisation of the framework. This will be followed by an open discussion with other State representatives in the room. All participants will be sent a set of guiding questions in preparation for the workshop. In the second part, participants will be separated into breakout groups, where they will be invited to outline the connection between specific norms and their experiences.
This is an interactive discussion, and we **encourage representatives to come prepared to engage in the discussion and share their experiences on the topic.**

The event will be followed by a short summary of the discussions to be shared with participating Member States. Inputs will also support RUSI’s ongoing project on [Responsible Cyber Behaviour](#) which seeks to advance the mapping of practical understandings of responsible cyber across different regions.

For any questions, please contact Louise Marie Hurel ([LouiseH@rusi.org](mailto:LouiseH@rusi.org))