THE PERMANENT MISSION
OF MALTA TO THE UN NEW YORK

Malta
2023-2024
UNITED NATIONS
SECURITY COUNCIL

Security Council briefing on Threats Posed by Ransomware Attacks Against Hospitals and other Healthcare Facilities and Services, 8 November 2024

Malta Statement delivered by Mr Darren Camilleri
Deputy Permanent Representative of Malta to the United Nations, New York

---

Thank you President, and I also thank Dr Ghebreyesus and Mr Conrado for sharing their valuable insights.

The evolution of ransomware tactics represents a severe escalation in the cybersecurity threat landscape. These attacks have become increasingly damaging, making recovery without succumbing to the demands of malign actors more challenging.

This is why Malta joined the call for this meeting.

The World Health Organisation has identified ransomware as the primary digital threat to healthcare, a situation worsened by COVID-19-driven digital transformation.

244 East 48th Street, New York, N.Y. 10017
T +1 (212) 725 2345 **E** malta-un.newyork@gov.mt

www.foreign.gov.mt

These attacks do not only jeopardise access to essential medical services. They also violate the fundamental right of privacy of the individual, and threaten the overall well-being and security of citizens and their fundamental human rights.

The OEWG's Annual Progress Report highlights the growing concern among states regarding ransomware, noting the increasing frequency and severity of these attacks. The rise of ransomware-as-a-service has broadened the range of malicious actors involved. The report underscores the necessity for a comprehensive approach to counter the ransomware threat, which includes targeting the illicit financing of these activities.

During the Security Council's high-level debate on cyber threats during the Republic of Korea Presidency in June, several delegations recognised the potential of ransomware to destabilise governments, and disrupt essential public services. They also underscored the increasing intensity of ransomware and state-sponsored cyberattacks targeting critical infrastructure.

These concerns were also underlined in the final report of the Panel of Experts, which reported on investigations of 58 suspected cyberattacks between 2017 and 2023, valued at approximately $3 billion. Reportedly, these helped the DPRK circumvent sanctions and continue develop weapons of mass destruction.

Malta acknowledges the rapidly evolving nature of technology-driven threats, and emphasises the need for a comprehensive response. It is vital for member states to ensure that the IT workforce, particularly in healthcare, possesses up-to-date cybersecurity skills. Additionally, raising awareness at the executive level about the potential of cyberattacks to serve as public health emergencies is crucial.

Investment in human capital, the establishment of robust incident response processes, and training clinical staff to maintain service quality during cyberattacks are essential. Developing strong communication pathways within healthcare entities for coordinated responses, potentially across borders, is also important.

National efforts alone can only go so far. They must be complemented by international cooperation, also to ensure adherence to international law. Cross-border ransomware attacks pose increasing risks to public health, with implications that extend far beyond mere technical disruptions. The availability of ransomware online has lowered the barriers for attackers, including transnational organised crime groups, making it easier for malicious actors to launch their operations globally.

President

Gender mainstreaming in cyber norm implementation and gender-sensitive capacity building are needed. Women's involvement and participation in cyber decision-making is crucial, especially in conflict and post-conflict contexts. Ensuring gender responsiveness in our cybersecurity strategies is essential for developing comprehensive and effective solutions.

In closing, President, we look forward to continuing our discussions on cybersecurity, and commend efforts made to highlight the vital role of the Security Council.

We reaffirm our support for a programme of action guided by the UN. We believe that the agreed Framework for Responsible State behaviour in cyberspace is essential for fulfilling our shared responsibilities and aligning our common interests.

I thank you.