YUNMUN
Yeshiva University National Model UN

Yael Polotsky
UNODC: Topic #2 - Combatting Cyber-Extortion Networks
YUNMUN XXXVI

The United Nations Office on Drugs and Crime works to stop transnational organized crime in all its forms, including those that are emerging in today's digital age. In recent years, ransomware and cyber-extortion have become some of the most serious and quickly changing threats to global security. These attacks involve criminals locking or stealing important data and demanding payment, often in cryptocurrency. These digital blackmail schemes have affected government agencies, hospital technology systems, multibillion-dollar corporations, and even school networks.

Cybercrime networks operate across borders, taking advantage of weak rules and lack of coordination between countries. To tackle this crisis, international agencies need to work together to improve cryptocurrency tracing, build stronger cyber defense systems, and share information more effectively.

The UNODC is already taking steps to address these challenges through its Global Programme on Cybercrime, which helps countries strengthen their defenses against digital threats. The program focuses on building technical skills, improving legal frameworks, and encouraging international cooperation to prevent and respond to attacks like ransomware. By training law enforcement and promoting global collaboration, the UNODC works to create safer and more resilient digital systems worldwide.[1]

We will aim to tackle this crisis with the following goals:

- Strengthening international frameworks for cyber cooperation and information sharing in order to track and dismantle ransomware networks.
- Expanding the capacity for tracing and regulating cryptocurrency to identify and intercept illegal payments.

[1] UNODC Home

- Supporting national cyber defense programs and public awareness campaigns to prevent attacks and improve resilience.

When preparing your position papers, keep these guiding questions in mind:

- What cybersecurity measures and digital defense systems does your country currently have in place to prevent ransomware attacks?
- How does your country regulate or monitor cryptocurrency transactions used in cybercrime?
- What role should international cooperation and intelligence sharing play in fighting cyber-extortion networks?
- Propose specific practices the international community can take to reduce this global threat of cyber-extortion.

These are merely starting points, and I encourage you to explore other avenues related to ransomware and cyber-extortion. Remember that you are representing your country's views, not your own.

While researching, remember that YUNMUN has a zero-tolerance policy for plagiarism. All position papers must be submitted through Turnitin and AI detectors.

Feel free to reach out to me with any questions, comments, or concerns. I can be reached at ypolotsk@mail.yu.edu. I look forward to reading your position papers and delving into these matters at the YUNMUN XXXVI conference!

All the best,

Yael Polotsky

Chair, United Nations Office on Drugs and Crime

YUNMUN XXXVI