unicri

United Nations
Interregional Crime and Justice
Research Institute

Statement of the Director of the United Nations Interregional Crime and Justice Research Institute Antonia Marie De Meo

International Festival of European Geopolitics

Cybersecurity, cybercrime and cyberterrorism

Venice, Italy
11 May 2023

Excellencies, Ladies and Gentlemen,

It is a pleasure to join you today on behalf of the United Nations Interregional Crime and Justice Research Institute (UNICRI), based in Torino. I am grateful to the City of Venice and each of the co-organizers for the kind invitation to participate in this International Festival of European Geopolitics.

UNICRI is a United Nations research and training institute focused on crime prevention, justice, security, and the rule of law. Within this broad mandate, one topic particularly relevant today is cyber.

Indeed, given the immense social, political, and economic consequences, cybercrime and cybersecurity have become increasingly important for Europe and the world. Malicious actors are launching evermore complex attacks and continue to adapt their techniques to evade detection and exploit vulnerabilities. New technology, such as artificial intelligence, is helping to automate attacks, make them more effective, and even better tailor attacks to victims.

In recent years, Europe – its institutions, critical infrastructure, and citizens – has found itself the target of notable major cyberattacks, such as WannaCry and the SolarWinds supply chain attack. And even when Europe has not been the direct target, cyberattacks on other countries have affected Europe. Such is the interconnected reality of cyberattacks in our digital age.

The European Union Agency for Cybersecurity estimated that the annual cost of cybercrime to the EU economy was around €265 billion in 2018 alone. On the global level, the World Economic Forum estimated that the cost of cybercrime may reach $10.5 trillion annually by 2025. That's less than two years away.

From UNICRI's perspective, one of the most relevant developments is the rise of the 'crime-as-a-service' model. This is a criminal business model that involves cyber-criminals providing their services to potential customers on the dark web for a fee. The model potentially allows any malicious actor with even the most basic cyber capabilities to launch a cyber-attack by facilitating access to the necessary expertise and tools.

UNICRI is further exploring this phenomenon from the perspective of cyber-terrorism. Terrorist groups such as ISIL and Al-Qaida have demonstrated tremendous capabilities to use the internet and social media. However, they have not succeeded to carry out effective and sophisticated cyber and technology-based attacks – yet. The cybercrime-as-a-service model could be a game changer for cyber-terrorism. And it challenges us to consider whether we may see terrorist groups leveraging more advanced cyber tools and techniques in the future, such as AI-enabled ransomware attacks or AI-powered decryption techniques.

Another notable development is evolution in the types of cybercrimes, in particular as a result of the COVID-19 pandemic. One of the most disturbing developments has been the significant rise of online child sexual exploitation and abuse. During the pandemic lockdowns, children and adults increasingly spent a large part of their day at home online, and we have seen a concurrent increase in concerning activities like online grooming, online risk-taking by minors, and live streaming of abuse materials.

We are also sensitive to the enabling role of new technology. Consider, for example, ChatGPT – a powerful language model that can generate human-like responses to prompts – which has taken the world by storm in little over 5 months. While we are still deciphering the beneficial uses to facilitate communication and enhance human productivity, cyber-criminals have already started to exploit ChatGPT.

And the malicious potential is tremendous. So-called generative AI can be used to create phishing emails, social engineering attacks, and even impersonate legitimate entities to steal sensitive information. It can create deepfake content, which can be used to spread disinformation and propaganda, leading to social and political unrest. Tellingly, shortly after the release of ChatGPT, dark web hits spiked.

As we continue to navigate the complexities of our increasingly digital world, cyber threats loom large. We must be vigilant and work collaboratively to develop new strategies and tools to prevent, investigate, and prosecute cyber-criminals.

It is crucial for Europe, and for the world, that we prioritize the safety and security of critical infrastructure, institutions, and citizens in our digital age. At UNICRI, we are committed to working with our partners in law enforcement agencies, international organizations, and the private sector to address these complex challenges and to promote a safer and more secure digital environment for all.

Thank you.