UNITED NATIONS INFORMATION SERVICE

Vienna International Centre
PO Box 500, 1400 Vienna, Austria
Tel: (+43-1) 26060-4666
Fax: (+43-1) 26060-5899
Email: unis@unvienna.org
http://www.unis.unvienna.org

Taking action where we can to stop cybercrime

Yury Fedotov

Cyber. It is the inescapable prefix defining our world today. From the privacy of individuals to relations between states, cyber dominates discussions and headlines – so much so that we risk being paralyzed by the magnitude of the problems we face.

But we would do well to keep in mind that despite the many outstanding questions on the future of cybersecurity and governance, international cooperation is essential to tackle the ever-growing threats of cybercrime.

Online exploitation and abuse of children. Darknet markets for illicit drugs and firearms. Ransomware attacks. Human traffickers using social media to lure victims. Cybercrime's unprecedented reach – across all borders, into our homes and schools, businesses, hospitals and other vital service providers – only amplifies the threats.

A recent estimate put the global cost of cybercrime at 600 billion US dollars. The damage done to sustainable development and safety, to gender equality and protection –women and girls are disproportionately harmed by online sexual abuse – is immense.

Keeping people safer online is an enormous task and no one entity or government has the perfect solution. But there is much we can do, and need to do more of, to strengthen prevention and improve responses to cybercrime, namely:

• Build up capabilities, most of all law enforcement, to shore up gaps, particularly in developing countries; and

• Strengthen international cooperation and dialogue – between governments, the United Nations, other international as well as regional organizations, INTERPOL and the many other partners, including business and civil society, with a stake in stopping cybercrime.

Cyber-dependent crime, including malware proliferation, ransomware and hacking; cyber-enabled crime, for example email phishing to steal financial data; and online child sexual exploitation and abuse all have something in common besides the "cyber" aspect: they are crimes.

Police, prosecutors and judges need to understand these crimes, they need the tools to investigate and go after the criminals and protect the victims, and they need to be able to prosecute and adjudicate cases.

At the United Nations Office on Drugs and Crime (UNODC), we are working in more than 50 countries to provide the necessary training, to sharpen investigative skills, trace cryptocurrencies as part of financial investigations, and use software to detect online abuse materials and go after predators.

As a direct result of our capacity-building efforts in one country, a high-risk paedophile with over 80 victims — was arrested, tried and convicted. We delivered the training in partnership with the International Centre for Missing & Exploited Children and Facebook. This is just one example of how capacity building and partnerships with NGOs and the private sector can ensure that criminals are behind bars and vulnerable children protected.

Working with the Internet Watch Foundation, we have launched child sexual abuse reporting portals – most recently in Belize – so that citizens can take the initiative to report abuse images and protect girls and boys from online exploitation.

With partners including Thorn and Pantallas Amigas we are strengthening online protection and educating parents, caregivers and children about cyber risks through outreach in schools and local communities. Prevention is the key.

UNODC training – focused primarily on Central America, the Middle East and North Africa, Eastern Africa and South East Asia – is also helping to identify digital evidence in online drug trafficking, confront the use of the darknet for criminal and terrorist purposes, and improve data collection to better address threats.

A critical foundation for all our efforts is international cooperation. Our work – which is entirely funded by donor governments – has shown that despite political differences, countries can and do come together to counter the threats of cybercrime.

We are also strengthening international cooperation through the Intergovernmental Expert Group, which meets at UNODC headquarters in Vienna.

Established by General Assembly resolution, the Expert Group brings together diplomats, policy makers and experts from around the globe to discuss the most pressing challenges in cybercrime today. These meetings demonstrate the desire and willingness of governments to pursue pragmatic cooperation, which can only help to improve prevention and foster trust.

As a next step, we need to reinforce these efforts, including by providing more resources to support developing countries, which often have the most new Internet users and the weakest defences against cybercrime.

Tech companies are an indispensable ally in the fight against cybercrime. We need to increase public-private sector engagement to address common concerns like improving education and clamping down on online abuse material.

Countering cybercrime can save lives, grow prosperity and build peace. By strengthening law enforcement capacities and partnering with businesses so they can be part of the solution, we can go a long way in ensuring that the Internet can be a force for good.

Yury Fedotov is Executive Director of the United Nations Office on Drugs and Crime