In wake of ‘WannaCry’ attacks, UN cybersecurity expert discusses Internet safety

19 May 2017 – A United Nations cybersecurity expert says that cybercrime is ultimately preventable, and that the internet – even the hidden so-called ‘dark net’ – has very good elements to it.

That may seem difficult to believe for people in the 150 countries hit by the ‘WannaCry’ ransomware, some of whom have had to pay hundreds of dollars in digital currency, Bitcoin, to get back photos of their families and other files on their laptops, or the families unable to board a train in Germany or see a doctor in the United Kingdom.

“Law enforcement and diplomats have been warning people of ransomware for some time, but this is really the first time that we’ve seen an attack of this size,” said Neil Walsh, Chief of Cyber and Emerging Crime at the UN Office on Drugs and Crime (UNODC).

Last Friday’s attack was due to a strain of Windows ransomware – which like the name suggests, encrypts files and holds them ransom. It entered individual systems as a compressed zip file through a security loophole in the Windows operating systems, and went on to scramble information in hundreds of thousands of machines belonging to hospitals, banks and other organizations around the world.

Mr. Walsh told *UN News* that the attack attributes its success to the fact that the operating systems used by those companies were old and did not have a security patch.

His advice boils down to clicking yes to software updates, using an up-to-date antivirus system, and backing up data into a device separate from the computer.

“If you weren’t expecting an attachment from someone, or it looks strange, don’t open it,” Mr. Walsh added.

Neil Walsh, UNODC’s Chief of Cyber and Emerging Crime, at a cybercrime training in East African. Photo: Credit UNODC

Headquartered in Vienna, and with teams in Guatemala, El Salvador, Tunisia and Thailand, Mr. Walsh’s role is to help create an inter-governmental response to cybercrime. That involves, in part, public outreach about internet risk, including to children and their parents, and working with police, prosecutors and judges around the world to improve how cases are investigated and tried.

Despite the increased number of cybercrimes in the past several years, some governments do not understand cyber risk, he said.

“It still never fails to amaze me that some governments say we don’t have cybercrime in our country, we don’t see any threat here,” Mr. Walsh noted. “And technically that means that they don’t have the capability to identify, to look for and to respond to it. So my role, and the role of my people, is to help governments understand that and to help them put strategies in place to minimize that risk to them.”

His teams also work with victims, to make sure that they have avenues to report crimes to the police, and sometimes seeking redress from a non-governmental organization or charity.

“There’s no such thing as a victimless crime, and that’s the same in cyberspace as in crime committed in the physical world,” he added.

From ‘I Love You’ to Botnets

Cybercrime has evolved since the “Melissa” and “I Love You” computer worms in 1999 and 2000, becoming more common and more destructive.

“If we look back on some of the attacks we’ve seen over even in the past six months, one of the most common threats outside of ransomware that we’ve seen is called a botnet,” Mr. Walsh said.

Bots are malware that sneak into a person’s computer and quietly wait for commands. These zombie-like devices can then be used as part of a network, or botnet, for possible attacks.

Law enforcement experts from 22 countries and UNODC staff in a training course on cryptocurrencies, such as Bitcoin. Photo: Credit UNODC

“What that means is that cyber criminals have taken over lots of different devices that are connected to the internet. Now I don’t mean traditional computers or smart phones, I mean everything from refrigerators to CCTV cameras to TVs. By compromising these devices, it’s possible for a cybercriminal to cause real harm,” the UN expert said.

That means more than getting a shopping password or stealing a credit card number – it could be shutting down the telephone system in a country or compromising a nuclear plant.

“If we consider this sort of weaponization of cyberspace and the impact that that could have, especially on developing countries, it could be enormous. If you had a significant cyberattack on a country that had no real capability to respond to a threat to its critical national infrastructure, you could have an immediate and long-standing impact.”

Despite these threats, cybersecurity is still often viewed as the role of an

IT department. There is not even an agreed-on definition of cybercrime around the world.

“It’s one of those things that has become quite politically nuanced,” Mr. Walsh said. “Our role here at UNODC is to help those political and diplomatic discussions, but also to help the investigations happen, irrespective of the definition behind it, because the crime still happens irrespective of what we’re calling it.”

In that context, UNODC has advocated for a free and open internet that would only be used for good, the UN expert said.

“Cybercrime is ultimately preventable,” he said. “If you know what the risk is, you’re less likely to become a victim.”