



Press Corps/The Economist

Press Corps

Reporters: Daniel Harper and Kai Cortadellas

Topic: SOCHUM/Countering the use of information and communications technologies for criminal purposes

United Nations takes action against cybercrime

Less than 40 years ago, when people thought of falling victim to a crime, they thought of their wallet being stolen. They thought of things like pickpocketing and shoplifting. In the worst case, most just prayed not to be caught in the middle of a bank break. But 40 years ago, computers were still primitive, and nobody knew what the word ‘internet’ meant. Our recent technological advancements have caused a stronger reliance on these things than ever before. It has gotten to a point where, whenever our computers fail, so do we.

“Today, wars are not fought with bombs and bullets,” Graeada Cooperman, a delegate for Venezuela, says. “They are fought with electrical signals.” And today, instead of jumping in the getaway van to rob a bank, criminals take to their computers. As a 2021 article from The Economist puts it, “Why would you walk into a bank with a sawn-off shotgun to steal £30,000 when, if you’ve got some money to invest, you can go on the dark web and start a ransomware campaign and make millions?” However, these attacks have gone beyond simple robberies. Now, crimes like this are used to wage war, and most worryingly, can go on to threaten international order and peace.

“Cybercrime causes tension across borders,” says Chloe Hurcula, an Israeli delegate. Tension that threatens peace. The world now turns to the United Nations to solve this international problem. The middle school SOCHUM committee, made up of just over 100 delegates, met on

March 21st in an effort to prevent cybercrime. They now believe that they have the answer, but after they worked together to find a solution, the delegates have decided that the course of action is more complicated than many would think.

Chloe Hurcula, the Israel delegate, recognizes that the first step to change is worldwide cooperation between nations. She points out hostility between the world's countries and sees the greater issue: the world needs to work together to prevent digital crimes. Another delegate from Nigeria agrees and encourages larger and more technologically advanced nations to send aid to more developed countries in the form of technology experts and equipment. One of the things this aid will be used for is education, one of the most important components of the solution. The majority of the victims of small-scale cybercrimes are either children or senior citizens; groups that lack the knowledge to protect themselves. But the victims of high-profile cybercrimes are corporations, who have proved unable to protect themselves. This is where the state needs to assist. Delegates proposed a wide range of methods to prevent cybercrime better. One method of protecting the victims is via firewalls, Virtual Private Networks, and more, as well as stopping the attacks from commencing in the first place, by investigating how to detect cybercriminals early and learning from research done on prior attacks.

Intergovernmental cooperation is needed. And when it comes to the safety of people's identities and lives, why should politics be involved? Other delegates also suggest that nations should share information about cyber protection and known criminals amongst themselves. Moreover, it is clear that our world coming together and working to solve this problem as a collective is very important for achieving our goals, but it goes beyond that. The very next step is to consider what goes on *within* these same nations.

Mexican delegate Aria Pungara brings up the suggestion that countries spend less on salvaging and recovering from cybercrimes, leaving more funds for the actual prevention of the issues. And it is true. In 2023, ransomware attacks cost the world 1 billion dollars altogether. On top of this, several delegates from other countries thought about the rapidly developing technology that is AI, "We need to fight tech with tech," one delegate said. And that is exactly what they plan to do. Several proposals were made concerning this topic of AI, whether it be used to aid biometric security or assist with cybersecurity defenses. It is a useful new technology, and it will only continue to develop.

People in the past couldn't have imagined multi-million dollar heists that don't even involve a weapon, but now, as a British delegate said, "We are in a never-ending age of cybercrime." High-profile cyber attacks happen now more than ever. Today, with enough skill, anyone can log onto their computer, go online, and steal millions of dollars. All without ever leaving their room. As more time goes by, billions of dollars will continue to be stolen every year. Cybercriminals can freely conduct international attacks with little consequences. Now, more than ever, governments take more offense from these attacks. And now, more than ever, we cannot wait. Delegates must take action. Together, they will take their proposals further; off of paper and into the real world, to create a place where we can all benefit from the technological advancements of our world.