COMMENTARY

The Proposed UN Cybercrime Treaty and a Path Forward

Critics are deeply skeptical and have expressed fears that the Russian proposal is a smoke screen to help allow it and others to further their totalitarian propaganda aims and block dissent at home and abroad, a former prosecutor writes.

May 25, 2023 at 02:07 PM

Commentary

By John Bandler | May 25, 2023 at 02:07 PM

In April, further meetings occurred regarding Russia's proposed and controversial United Nations Treaty on Cybercrime. The treaty ostensibly aims to improve the prevention, investigation and prosecution of cybercrime around the globe and facilitate cooperation between nation-states.

Many critics, however, are deeply skeptical and have expressed fears that the Russian proposal is a smoke screen to help allow Russia and others to further their totalitarian propaganda aims and block dissent at home and abroad.

The draft treaty is now enormous because of all the proposed additions and deletions. There's little consensus and changes will continue. There's also little agreement on what cybercrime is and what conduct should be criminalized and covered by the treaty.

Russia originally proposed this cybercrime treaty in 2017. It stated concern about "threats posed by crimes in the sphere of information and communications technologies … to the stability and security of society … democratic institutions and values, ethical values, and justice, and … the rule of law" and included a provision protecting the "sovereignty of nations."

The three most important chapters dealt with criminalization, prevention and cybersecurity, and international cooperation. The criminalization provisions indicate what conduct each nation should criminalize as part of the treaty, including typical cybercrimes, theft and child pornography. It had some uncertain language protecting “state secrets” and as to copyright.

At the outset, there was high skepticism about this proposal and the underlying motives of Russia. It was not supported by the United States or the European Union. Before 2016, Russia had developed a reputation for protecting cybercriminals within its borders, so long as those criminals targeted victims in other countries, such as the U.S.

Aside from suspicions, other international treaties already existed that relate to cybercrime, though their application to various countries and conduct is far from comprehensive.

Before its 2017 treaty proposal, Russia had been credibly accused by the U.S. of cybercrime attacks, including data breaches against U.S. targets. Russia offered “assistance” to investigate the allegations and promote cybersecurity, which few took seriously. Then came this treaty proposal, which was viewed by some as a cynical follow-up.

In 2019, Russia, China, Iran and others proposed a resolution to move this treaty forward in the U.N. approval process. The U.S. and EU opposed the resolution, but the U.N. approved it nevertheless, and a committee was formed to develop the new agreement, resolve differences, and eventually bring it to the U.N. General Assembly.

Many negotiation sessions have occurred over the years. The sixth session will commence in August, then a concluding session starts in January. After that a draft treaty is scheduled to go for consideration and vote by the U.N. General Assembly.

Focus on Theft

The path to building common understanding and then treaties to fight cybercrime is a focus on the heart of the criminal activity, which is theft and trespass. Most cybercrime is just about theft. Computers and the internet allowed theft to became international. That is the problem and why international treaties and cooperation are needed.

Measures that focus on theft can fight the vast majority of cybercrime more effectively. Most technical cybercrime attacks are motivated by greed with a goal to steal and this includes spam, data breaches, network intrusions, malware, ransomware, email hijacking, impersonation and more. Within this theft category we have extortion, identity theft, and a host of other crimes committed to facilitate it, including money laundering and all sorts of “cyber” actions.

Electronic trespass and tampering is the next priority focus. We all know and understand the criminal laws against physical trespass and burglary. Do not go into someone’s property, home or building without permission and authorization. Do not steal from someone’s house or property, do not vandalize the contents or interior.

These concepts apply in the digital realm too and many federal and state criminal laws prohibit unauthorized entry into a computer device or network. Essentially, the law says, do not go into a network, computer or system without authorization. Do not steal data from the system, do not damage the system.

The wording might be different. Some of the terms used might be: computer fraud and abuse, computer trespass, computer tampering, unauthorized use or access, denial of service, ransomware, malware and more.

While most electronic trespasses are committed in the furtherance of another theft, cybercrimes are not *always* for theft, and sometimes the financial aspect is hard to see and harder to prove. Therefore, these electronic trespasses need to be specifically criminalized and part of an international cybercrime treaty.

Criminalizing Speech and Expression

A common criticism is that the treaty in its present form could be used to cudgel and suppress speech and expression, especially by countries that do not value it. It would allow repressive countries to obtain evidence and coerce legal cooperation to investigate speech that is protected by international law and the law of most countries.

To build consensus and protect human rights for speech, international treaties could stop at child sex abuse content (e.g., images and videos) when addressing speech and content.

Child sex abuse content (sometimes called child pornography) needs to be a part of international cybercrime cooperation. Children need protection. Any crimes involving the creation, possession, trafficking or profiting from child sex abuse images need domestic criminal prohibitions and international cooperation.

Beyond that, international cybercrime laws should avoid speech and content crimes to gain consensus and protect human rights. Otherwise, some countries will be further empowered to oppress dissent.

The proposed treaty has no force of law yet, the text will continue to evolve, and if it ever passes, it will look different. Good international treaties that advance the rule of law, help investigate and prosecute cybercrime, and that respect individual rights will aid with the fight against cybercrime.

John Bandler *is a lawyer, consultant, author and adjunct professor at Elisabeth Haub School of Law at Pace University, who previously investigated international cybercrime as a prosecutor. He can be reached at JohnBandler@JohnBandler.com.*