FOR IMMEDIATE RELEASE

March 1, 2022

Media Contact

Natalie Monsanto, monsanto@law.ucla.edu

The Promise Institute for Human Rights at UCLA School of Law

*****PRESS RELEASE*****

CYBER ATTACKS CAN QUALIFY AS WAR CRIMES AND CRIMES AGAINST HUMANITY

As the Russian invasion of Ukraine continues, concerns and headlines have increasingly turned to the threat of cyberwarfare. This April marks the fifteenth anniversary of Estonia becoming the first victim of a recognized state cyber attack, and yet in the intervening years the international criminal law framework governing cyberwarfare remained obtuse - until now.

The Promise Institute for Human Rights at UCLA School of Law gathered leading international legal experts to demystify cyberwarfare and address pressing questions related to cyber operations, including things like ransomware attacks on civilian infrastructure and dual cyber/armed forces efforts.

To understand how international criminal law applies to cyberwarfare, the panelists discussed how all four crimes in the Rome Statute could be committed through cyber means. The most likely crimes to be applied to cyber operations are War Crimes and Crimes Against Humanity because they aren't as narrowly defined as Genocide and Crimes of Aggression. While War Crimes governs acts committed during armed conflict, a Crime Against Humanity can be committed in time of war or peace. Cyber activities which amount to torture, persecution or other inhumane treatment, for example, could be prosecuted on this basis, as part of a widespread or systematic attack on a civilian population.

As a result, it is clear that cybercrimes can already be prosecuted under international criminal law - meaning no new law specific to the technology we're seeing used today needs to be written to address cyberwarfare.

As Promise Institute Executive Director Kate Mackintosh noted, “There has been a lingering and pervasive sense that cyber operations existed in a legal gray area. Part of the fog surrounding cyber operations is that perpetrators are difficult for the average person to identify and can literally be anywhere in the world. However, international criminal law already has the tools to address many of these issues - our job now is to raise awareness.”

In response to questions about identifying attackers, Lindsay Freeman said “Attribution is a big issue. However, as there is no statute of limitations for international crimes, investigators can take whatever time they need to not only be certain of a cyber operation’s technical attributions, but also to connect other evidence including witnesses when relevant, and ultimately build a very strong case.”

Cases like the Florida water treatment plant whose lye (often used as liquid drain cleaner) levels were raised to 100 times their normal amounts by cyber attackers who had been quietly monitoring the computer system for months, and other attacks on critical civilian infrastructure like hospitals and pipelines, illustrate the importance of more robust legal responses.

Charles Jalloh stated “There is a question at the heart of cyber operations conversations about the maintenance of international peace and security on a global scale. Cyber security implications for society go well beyond any one particular technology and include the integrity of democracy itself.”

Cyberattacks are nothing new to Ukraine, but cyber operations targeting the nation are of particular relevance to international law. Ukraine has submitted to the jurisdiction of the International Criminal Court under two declarations, meaning that although it is not a formal state party itself, the court has authority over crimes committed on its territory since February 2014.

One example which may reach the ICC is the stunning December 23, 2015, power grid hack which left some 230,000 Ukrainians without power as Russian troops simultaneously massed on their border. Whether Ukraine will become the first situation to see accountability for international cybercrimes remains to be seen, but given pervasive global cyber operations it seems clear that a case will emerge in the near future.

Many of the panelists were participants in drafting “*The Council of Advisers Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare”* an analysis spearheaded by the Permanent Mission of Liechtenstein to the United Nations.

The Promise Institute for Human Rights is the innovative home for human rights at UCLA, combining focus areas like technology, accountability and human rights to help generate global impact like that seen with our analysis of cyberwarfare and international criminal law. Speakers at our event included Richard Dicker of Human Rights Watch, Charles Jalloh of Florida International University, Ambassador Christian Wenaweser of Liechtenstein, Lindsey Freeman of UC Berkeley's Human Rights Center, and Promise Institute Executive Director Kate Mackintosh.

###