

November 14, 2024

The Honorable Antony Blinken
Secretary of State
U.S. Department of State
2201 C Street NW
Washington, DC 20520

The Honorable Samantha Power
Administrator
U.S. Agency for International Development
1300 Pennsylvania Avenue NW
Washington, DC 20004

The Honorable Merrick Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20500

Dear Secretary Blinken, Attorney General Garland, and Administrator Power:

HackerOne is writing to voice concern about the failure of the UN Convention Against Cybercrime to protect good faith security research and those who engage in this critical practice to enhance our cybersecurity. We respectfully encourage the United States to continue to work at the UN to incorporate protections into the treaty language, if possible, and to work with other countries to encourage the incorporation of protections for such research into national law or law enforcement policies and practices.

While the UN Convention Against Cybercrime aims to enhance international cooperation to combat malicious cyber criminals, the Convention raises serious concerns for those involved in security research to strengthen cybersecurity and protect people. The treaty's provisions related to security research fail to align with best practices encouraged by the U.S. government and federal policies adopted by the Department of Justice that protect good faith security research from prosecution.

Though this treaty will not directly alter existing computer crime laws, nations with less developed cybercrime laws may pass regulations that mirror the text of the UN's Convention, and authoritarian governments may use the flawed text of the Convention to justify suppression and censorship of security researchers and others.

Security researchers operating in or collaborating with entities in countries with fewer protections for good faith security research may find themselves at heightened risk of potential legal consequences for activities that are both ethical and essential to maintaining global cybersecurity.

The treaty encourages signatories to recognize the contributions of legitimate security researchers, provided their activities are intended to strengthen and improve security to the extent permitted by law. While this acknowledgment is a positive step, it falls far short of encouraging signatories to establish legal protections for legitimate security research. Because recognition of security researchers' vital work is not consistently reflected in the treaty's restrictions on computer access and use and translated into meaningful protections for researchers, it will be up to member countries to do so in national laws or through policies and guidelines that companies and law enforcement officials can follow.

If the United States is unable to advance a protocol to the convention that adequately provides these protections, our country can and should contribute its knowledge and experience in protecting security research and strongly encourage the adoption of similar practices in other countries. For example, the U.S. Agency for International Development and the State Department should incorporate policy best practices for protecting security researchers into their cybersecurity capacity building programs. Alternatively, they should condition digital capacity building funds on the condition that recipient governments do not prosecute good faith security researchers. The U.S. should also partner with nongovernmental capacity building organizations and like-minded governments to develop and disseminate best practices for implementing the treaty that recognize the importance and benefits of security research and differentiate ethical research from cybercrime.

Taking these and other steps to protect good faith security research will help ensure that policymakers around the world are aware of the treaty's implications for security research and encourage them to adapt their legal frameworks to support, rather than hinder, ethical hacking. By doing so, nations can foster a cooperative environment where the essential work of security researchers is valued and encouraged, ultimately strengthening our collective defenses against cyber threats.

Sincerely,

Ilona Cohen

Ilona Cohen
Chief Legal and Policy Officer
HackerOne

Cc: The Honorable Linda Thomas-Greenfield
The Honorable Nathaniel Fick

Mailing Address

548 Market Street
PMB 24734
San Francisco, CA 94104-5401