Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : b0e98766 | May 03, 2023, 05:16 PM

This week, *Hacking Healthcare* takes a look at developments in the international community. Specifically, we examine new developments related to the United Nations (U.N.) Cybercrime Treaty and analyze what the healthcare sector should expect from this international process.

Welcome back to *Hacking Healthcare*.

What Could Be Expected from a U.N. Cybercrime Treaty?

The U.N. commenced negotiations for a Cybercrime Treaty in 2017 but recent developments have brought this proposed legislation into the spotlight. The current draft of the treaty would have a significant impact on criminal laws with the potential to add 30 criminal offenses and expand police powers for domestic and international investigation.[i] However, the fifth session of the Cybercrime Convention which commenced in Vienna in early April 2023 has sparked concerns that the proposed treaty lacks strong protections of human rights and may not actually be focused on cracking down on cybercrime as it is generally interpreted by the U.S. and its allies.

In 2019, the UN General Assembly adopted a resolution on "countering the use of information and communication technologies for criminal purposes" and introduced an ad hoc committee to work towards the creation of a new international treaty on cybercrime.[ii] This resolution was met with skepticism by many for two reasons.

First, there were concerns that the creation of a new treaty would result in legislative fragmentation considering the existence of the Budapest Convention on Cybercrime, which is a widely accepted, comprehensive cybercrime treaty already in existence.[iii] The Budapest Convention reconciles effective criminal justice and human rights safeguards with narrowly defined restrictions, only investigating and prosecuting specific criminal offenses.[iv] 80% of states worldwide have used the Budapest Convention as a guide for their own domestic cybercrime litigation and it has driven essential norms of behavior in cyberspace since its inception.[v]

Secondly, there were concerns that authoritarian states such as China and Russia would attempt to transform the treaty into a mechanism of information control and brandish it to crack down on internet

freedoms and human rights.[vi] In essence, a revisionist take on the Budapest Convention that would bifurcate global opinion. Based on the draft language, these fears were not entirely misplaced.

The content of the proposed draft is unique in that it does not focus on traditional cybercrimes like network intrusions or computing system interferences. Instead, the treaty focuses on content-related crimes and includes clauses that could make it a crime to humiliate a person or group, or to post legitimate content currently protected under international law like the Universal Declaration of Human Rights.[vii] During negotiations, a number of provisions were proposed to expand surveillance powers of states to include real time collection of traffic data, interception of content, and "special investigative techniques." These expansive surveillance provisions and the focus on content-related crimes could likely result in overly broad laws to crack down on free speech and privacy rights.[viii]

The draft Cybercrime Treaty also puts forth vague provisions that would encourage states to pass laws authorizing the use of broadened spying powers without the necessary safeguards in place to protect the right to a fair trial.[ix] Current negotiations have seen member states such as Russia, China, and Iran proposing to remove Article 5 which emphasizes respect for human rights and references international human rights obligations. Furthermore, other states have lobbied to remove modest limitations on government spying powers in Article 42. Critics have raised concerns in the past regarding anti-cybercrime laws being used to prosecute minority communities and stifle free speech.[x] As a result, the treaty's negotiation process will continue to be scrutinized by those focused on the protection of rights and ensuring the document will not be exploited once finalized.

At a time where cybercrime is already rampant, many are worried about the implications of a treaty with vague and expansive components that don't appear to actually address the issue as its conceived of by the United States and other likeminded governments. The connection of autocratic states to this treaty is also troubling due to the sheer number of cyberattacks perpetrated by actors residing within those countries. So, what does this mean for international forums as a place for progress on cybercrime? Can the international community rely on multilateral negotiations to make progress on these cybersecurity issues, or are alternative methods of collaboration likely to remain the answer?

Action & Analysis
Included with Health-ISAC Membership

Congress
Tuesday, May 2
No relevant hearings

Wednesday, May 3
No relevant meetings

Thursday, May 4
No relevant hearings

International Hearings/Meetings

No relevant meetings

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

[i] https://www.eff.org/deeplinks/2023/04/decoding-uncybercrime-treaty
[ii] https://unric.org/en/a-un-treaty-on-cybercrime-en-route/
[iii] https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights
[iv] https://www.coe.int/en/web/cybercrime/key-facts
[v] https://www.coe.int/en/web/cybercrime/key-facts#{%22105028002%22:[0]}
[vi] https://www.lawfareblog.com/un-cybercrime-convention-should-not-become-tool-political-control-or-watering-down-human-rights
[vii] https://www.un.org/en/about-us/universal-declaration-of-human-rights
[viii] https://www.eff.org/deeplinks/2023/04/decoding-uncybercrime-treaty
[ix] https://www.eff.org/deeplinks/2023/04/decoding-uncybercrime-treaty
[x] https://www.eff.org/deeplinks/2023/04/decoding-uncybercrime-treaty
[xi] https://subscriber.politicopro.com/newsletter/2023/04/russia-china-aim-to-twist-meaning-of-cybercrime-00094368
[xii] https://subscriber.politicopro.com/newsletter/2023/04/russia-china-aim-to-twist-meaning-of-cybercrime-00094368
[xiii] https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights
[xiv] https://www.washingtonpost.com/politics/2023/04/28/perilous-path-new-cybercrime-treaty/
[xv] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
[xvi] https://home.treasury.gov/news/press-releases/jy1256

Reference | References

unric
US Department of Justice
politicopro
EFF
coe
Health-ISAC
treasury
un
Lawfare Blog
Washington Post
hrw

Report Source(s)

Health-ISAC

Tags

Hacking Healthcare, International Law, Cybercrime, United Nations

---

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.