Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ ○ TLP:WHITE Alert ID : 2dc7bdbf Sep 21, 2023, 03:49 PM

This week, *Hacking Healthcare*™ examines the International Criminal Court's (ICC) willingness to investigate and prosecute malicious cyber acts that fall within their jurisdiction. We briefly summarize what the ICC is, where this change in policy comes from, and what it may mean for the healthcare sector.

Welcome back to *Hacking Healthcare*™.

The Health-ISAC Hobby Exercise 2023

The Health-ISAC is pleased to announce the fourth iteration of our Hobby Exercise Americas on October 25th in Washington DC. The Hobby Exercise is an annual Healthcare and Public Health (HPH) event designed to engage the healthcare sector and strategic partners on significant security and resilience challenges. The overarching objective is to inform and provide opportunities for continuous organizational improvement while increasing healthcare sector resiliency.

Members wishing to know more or express an interest in participating should visit the following registration link: https://portal.h-isac.org/s/community-event?id=a1Y7V00000VJ560UAD

International Criminal Court Prosecutor Signals Intent to Investigate Malicious Cyber Acts

In late August the Prosecutor of the International Criminal Court (ICC), Karim A. A. Khan KC, published an article reiterating his belief that the ICC should pursue malicious cyber acts that meet the threshold for ICC investigation and prosecution.[i] Since then, the ICC has confirmed that this is now the official position of the ICC.[ii] Let's breakdown what Khan said, how it might affect cyberattacks against critical infrastructure sectors like healthcare, and discuss the challenges the ICC will face in making a difference.

What is the ICC?

Understandably, many readers may be not be fully familiar with the ICC, so we'll begin by briefly describing what the ICC is, how it came about, and what its mandate is.
In simple terms, the ICC is a permanent intergovernmental organization born out of the adoption of the Rome Statute in 1998. It would formally be established in 2002, and is based in The Hague, Netherlands.

The ICC acts as an international court that investigates and prosecutes individuals for a narrow scope of especially grave crimes such as genocide and war crimes, and it describes its mission as “help[ing] put an end to impunity for the perpetrators of the most serious crimes of concern to the international community as a whole.”[iii]

While technically independent from the United Nations, and entirely distinct from the United Nation’s International Court of Justice, it often cooperates with the United Nations, and relies on funding from a variety of public and private sources to operate. Over 120 member countries have voluntarily agreed to be party to Rome Statute and accept the court’s jurisdiction. Notably, the ICC has not traditionally pursued malicious cyber actions or cybercrimes.

What Was Said?

Now that we’ve established the background, lets explore what Khan said, which appears to be the basis for the ICC’s policy going forward.

Khan outlined that cyberspace should be treated the same as any other domain in terms of its relation to the law. He cited that tangible impacts that malicious cyber acts can have, and specifically called out the impacts of attacks on medical facilities. While acknowledging that the ICC plays a complementary, rather than a leading role in addressing crimes, Khan highlighted how the ICC’s new position on malicious cyber acts could be a benefit to deterrence. Additionally, the ICC could help member states with their own legal proceedings on cyber issues. Khan also stressed how the ICC would work with the private sector to take collective action against cybercrime.

With that said. What might we expect in terms of impact on the broader international community and specifically with regards to healthcare cybersecurity.

Action & Analysis

****Included with Health-ISAC Membership****

Conclusion

Maybe we will be surprised at what the ICC is able to accomplish over the next few years, but Health-ISAC members probably shouldn’t be holding their breath that this kind of policy shift will amount to much in the way of deterrence. The states most likely to be affected by the ICC’s efforts have little incentive to cooperate and the ICC’s jurisdiction and enforcement capabilities cannot compel intransigent governments to comply.

The ICC might even find itself targeted by the kinds of governments it is likely to consider investigating for malicious cyber acts. Just this week, the ICC admitted that its own systems had been breached, potentially resulting in sensitive evidence of ongoing cases being exfiltrated.[vii] While no culprit has been publicly identified, “The Dutch intelligence agency (AIVD) said in its 2022 annual report that the ICC was "of interest to Russia because it is investigating possible Russian war crimes in Georgia and Ukraine"”. [viii]

Congress

Tuesday, September 19

No relevant meetings

Wednesday, September 20

No relevant meetings

Thursday, September 21

No relevant meetings

International Hearings/Meetings

No relevant meetings

EU

[i] https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/

[ii] https://arstechnica.com/information-technology/2023/09/the-international-criminal-court-will-now-prosecute-cyberwar-crimes/

[iii] https://www.icc-cpi.int/sites/default/files/Publications/understanding-the-icc.pdf

[iv] https://www.icc-cpi.int/about/how-the-court-works

[v] https://www.icc-cpi.int/about/how-the-court-works

[vi] https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/

[vii] https://www.reuters.com/world/international-criminal-court-reports-cybersecurity-incident-2023-09-19/

[viii] https://www.reuters.com/world/international-criminal-court-reports-cybersecurity-incident-2023-09-19/

Report Source(s)

Health-ISAC

Reference | References

Reuters
digitalfrontlines
icc-cpi
Health-ISAC
Health-ISAC
icc-cpi
Ars Technica

Tags

War Crime, ICC, International Criminal Court, Hobby Exercise, Hacking Healthcare, Cybercrime, Europe

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

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

Hacking Healthcare™:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has 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.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC’s annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC’s monthly Threat Briefing.

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