Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare | TLP:WHITE | Alert ID : 1df5544a | Oct 11, 2023, 10:13 AM

This week, *Hacking Healthcare*™ takes a look at a set of rules for civilian hackers taking part in armed conflicts that the International Committee of the Red Cross has published in response to the ongoing Russian invasion of Ukraine. We take a look at why this came to be, what affect the rules are and may have, and what Health-ISAC members should consider doing as a result.

Welcome back to *Hacking Healthcare*.™

Health-ISAC European Summit

The Health-ISAC would like to remind members that there is still time to register for the upcoming 2023 European Summit. The event will be held in Dubrovnik, Croatia, from October 17 to October 19. For those interested in learning about responsible artificial intelligence or getting an update on NIS2, please consider registering before the deadline on October 12.

Link: https://web.cvent.com/event/3e5fb53c-28a0-4d5d-ad1b-7b82eb63d4ce/summary

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 who wish 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

Rules for Civilian Hackers in Armed Conflicts?

The Russian invasion of Ukraine has been a chance to see how state and non-state actors have chosen to employ cyber capabilities in the context of a modern and open armed conflict. One aspect that has drawn considerable attention is the degree to which non-state actors, many of whom are not even

geographically proximal to the conflict, have found ways to engage in the conflict through cyberspace. Responding to their involvement, the International Committee of the Red Cross (ICRC) has published a blog post that details eight rules for "civilian" hackers and highlighted the responsibilities of states towards them.[i]

Who is the ICRC?

The ICRC is a non-governmental organization that was established in 1863 and describes itself as "an independent, neutral organization ensuring humanitarian protection and assistance for victims of war and armed violence.[ii] It takes action in response to emergencies and promotes respect for international humanitarian law and its implementation in national law." It is funded through voluntary contributions from states, international organizations like the European Commission, and private donations.

Context

The ICRC blog post notes a "worrying trend" of growing numbers of civilian actors "[becoming] involved in armed conflicts through digital means."[iii] Sometimes termed hacktivists or patriotic hackers, these individuals are carrying out cyber operations of their own volition and not as part of a state government's military or intelligence apparatus, although the degree of their separation from any kind of government coordination can be blurry.
The ICRC notes that while Ukraine may be the most prominent, there are a wide range of geographically dispersed examples and that these civilians can be found carrying out both offensive and defensive operations in support of their cause or chosen side. In many cases, these are not isolated individuals, but semi-coordinated groups with tools and instructions being shared.[iv]

The ICRC stresses that while these civilian operations are unlikely to cause the kind of harm a dedicated nation state actor might be able to, they do create significant problems. First, they disrupt civilian services and functions that can cause harm, such as to transportation, healthcare, and banking. Second, their involvement blurs the line between military combatants and civilian non-combatants. This distinction is critical for minimizing civilian harm and collateral damage during conflicts and the ICRC points out that while members of the armed forces enjoy some level of legal protection for "lawful" acts of war, civilians do not enjoy these same protections for carrying out similar actions.

Rules for Civilian Hackers

The eight rules the ICRC have come up with are:[v]

1. Do not direct cyber attacks against civilian objects.

2. Do not use malware or other tools or techniques that spread automatically and damage military objectives and civilian objects indiscriminately.

3. When planning a cyber attack against a military objective, do everything feasible to avoid or minimize the effects your operation may have on civilians.

4. Do not conduct any cyber operation against medical and humanitarian facilities.

5. Do not conduct any cyber attack against objects indispensable to the survival of the population or that can release dangerous forces.

6. Do not make threats of violence to spread terror among the civilian population.

7. Do not incite violations of international humanitarian law.

8. Comply with these rules even if the enemy does not.

Obligations of States

As we have noted in past editions of *Hacking Healthcare*, little of this matters if states do not take good faith actions to police their own citizens from engaging unlawful cyber actions. This is not lost on the ICRC, as they do remind states that they have responsibilities to regulate civilian hacking through the adoption and enforcement of adequate laws. Furthermore, the ICRC reminds states that their use of civilian hackers ultimately makes them responsible for their actions, and that states have an obligation to prosecute civilian cyber operations that cross into the territory of war crimes and to suppress activities that otherwise violate international humanitarian law.

Action & Analysis
Included with Health-ISAC Membership

Congress
Tuesday, October 10
No relevant meetings

Wednesday, October 11
No relevant meetings

Thursday, October 12
No relevant meetings

International Hearings/Meetings
No relevant meetings

[i] https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/
[ii] https://www.icrc.org/en/who-we-are

[iii] https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/
[iv] https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/
[v] https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/
[vi] https://www.icrc.org/en/document/icrc-cyber-attack-analysis
[vii] https://www.bbc.com/news/technology-67029296
[viii] https://www.bbc.com/news/technology-66998064

Report Source(s)

Health-ISAC

Reference | References

BBC
icrc
icrc
cvent
Health-ISAC
Health-ISAC
BBC
icrc

Tags

Rules, Hobby Exercise, Hacking Healthcare, Red Cross, International Law, hacktivism, Hacktivist, law

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.

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP "Share Threat Intel" Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

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.

For Questions or Comments:

Please email us at toc@h-isac.org