



Cyber Volunteering during the COVID-19 Pandemic

 CyberPeace Institute

 [June 5, 2020](#)  [Blog, CyberPeace Lab](#)

Despite the WannaCry wake up call, healthcare cybersecurity still lags and COVID-19 is a stark reminder of this alarming situation. The [CyberPeace Lab#4](#) gathered healthcare practitioners and cybersecurity experts who discussed the reality on the ground, the challenges they face implementing cybersecurity in the midst of a pandemic, and how emerging volunteer cooperation models could be scaled and sustained over time.*

On the dark reality of cybersecurity and healthcare in many countries

The COVID-19 pandemic has brought about a new reality for hospitals all over the world. Beyond providing treatments to millions worldwide, there has been a stark increase in COVID-19 related phishing campaigns and ransomware attacks. In parallel, hospitals have had to increase access to telehealth and connect medical devices to the hospitals' networks hastily.

Most of hospitals around the world rely on technologies designed to be in place for a very long time and so security issues remain, if not increase due to the interaction with new systems. The very nature of critical infrastructures, such as hospital, is that systems should not be unavailable, which makes patching and updating particularly challenging.

Megan Stifel from the Global Cyber Alliance, underlined how small steps could have a significant impact, **implementing cyber hygiene and best practices**. Beyond these issues, hospitals also face a structural lack of adequate IT resources, a shortage of cyber talent exacerbated by low salaries, and a challenging prioritization of cybersecurity and patient safety.

"One of the major challenges that hospitals around the world face is that, unfortunately cybersecurity is yet not equal to patient safety, but it really needs to be." – Christopher Frenz, Interfaith Medical Center.

This makes for an explosive situation. On 13 March, Brno's University Hospital in Czech Republic faced a [major attack](#) that forced surgeries to be postponed as operational systems had to be turned off.

Professionals paint a dark picture of the cybersecurity reality in the healthcare sector. In many cases hospitals and medical facilities are neither compliant with basic regulations and guidelines, nor following best practice. In the last decade, due to the fast pace of tech developments, many hospitals have seen their technical debt increase.

As a result, a collective cyber awakening could be the most important lesson from the current crisis.

There is hope

Crises like Wannacry and COVID19 highlight the importance of cybersecurity in healthcare. Christopher Frenz from the Interfaith Medical Center in Brooklyn, New York, explained how his hospital didn't wait for the next crisis and regularly organizes cybersecurity exercises.

It was following such an exercise that his hospital adopted a zero-trust network; the exercise was instrumental in convincing senior leadership of the importance of segmentation. Cybersecurity is not a new priority in healthcare sector, but priorities need to be pushed up the agenda and crises, even if simulated, help.

Many government authorities are also helping their hospitals. At European level, Dimitra Liveri outlined that the European Commission, ENISA and other EU Agencies share with EU government authorities weekly incident response situation reports and technical guidance on COVID19 tracking applications. Large companies are also actively supporting healthcare organizations fend off cyber threats, as explained by Peter Spirik from PwC.

Volunteers increasingly play a role. I Am The Cavalry, represented by Beau Wood during the lab, is a group of volunteer cybersecurity researchers founded in 2013 around the vision of bringing computer security to public safety and human life. Such initiatives reveal a desire to help that pre-exist global events. The CTI League and COVID-19 Cyber Threat Coalition have emerged with the pandemic, bringing together several thousands of volunteers around the world, actively working with law enforcement to bring down malicious domains and botnets and containing many other cyber threats leveraging the current climate of uncertainty.

Scaling assistance up

The spirit of volunteerism precedes cybersecurity and its challenges too. The scaling up and sustainability of volunteer initiatives is a difficult problem to solve: how to avoid for instance the cannibalization of existing commercial services, or worse, in the present case, the deprioritization of IT budgets in healthcare? As reminded by Pierre Hayaert from Airbus, hospitals in many countries are considered critical infrastructure and as such, tightly supervised by governments. Bringing voluntary assistance may not be straightforward, but there are ways forward.

“As long as we make sure that everyone at every skills level knows that they are welcome, and we make sure they get value out of volunteering, such efforts will never slow down.” – Erick Galinkin, Cyber Threat Coalition.

For most healthcare entities there are no specific regulations *prohibiting* them to engage with volunteer initiatives. As the latter become more established and mainstream, their global reach and multidisciplinary nature could prove to be a great complement to existing governmental and commercial assistance schemes. In a complex environment where many actors are involved to build trust and there is not a one-size-fits-all approach, the cyber volunteer initiatives are succeeding in making themselves available almost anywhere, anytime.

Looking forward, Stifel suggested, it is also important to keep in mind some of the non-technical elements that are critical to the success of volunteering. These elements include trust, desire for transparency and engagement with existing actors in a complementary fashion. And indeed, long-term volunteering may require different processes, models, dynamics.

What now?

“After the crisis is over, we will do the analysis and share information about what worked and what didn't, and what we learnt. Then we will come up with sustainable models.” – Jen Ellis, Rapid7.

The priority today remains to support healthcare organizations in the fight against COVID19. When the pandemic is over, time will come to reflect upon all that happened. The CyberPeace Institute aims to harness such lessons to bring scalable and long-lasting solutions to vulnerable populations.

*Moderated by *Stéphane Duguin*, CEO of the CyberPeace Institute, the Lab featured the following experts:


- *Jen Ellis* – Vice President of Community and Public Affairs, Rapid7
- *Christopher Frenz* – AVP of Information Security, Interfaith Medical Center
- *Erick Galinkin* – Principal AI Researcher, Rapid7 and Volunteer, Cyber Threat Coalition
- *Pierre Hayaert* – Project Manager for Innovation, Airbus Defence & Space Innovation
- *Martin Konir* – CIO, Bulovka Hospital

- *Dimitra Liveri* – Network and Information Security Expert, ENISA
- *Petr Spirik* – Cyber & Privacy Leader, PWC
- *Megan Stifel* – Executive Director for Americas, Global Cyber Alliance
- *Beau Woods* – Co-founder, I Am The Cavalry
- ...

The CyberPeace Institute is an independent, non-profit organization with the mission to enhance the stability of cyberspace. It does so by supporting vulnerable communities, analysing attacks collaboratively, and advancing responsible behaviour in cyberspace.

Copyright: The CyberPeace Institute

COVID-19 Infodemic: Cyber Volunteers and Healthcare - State of Play



CATEGORY

Blog	(110)
Café	(18)
CyberPeace Lab	(4)
Donor Series	(5)
Event	(5)
From the CEO's Desk	(4)
Future of Cyberpeace	(2)
Guest Blog	(1)
News	(29)
Podcast	(1)

Position Paper	(4)
Press Release	(13)
Statement	(24)
Submissions	(7)
Testimonial	(3)
Toolkit	(4)

TAG CLOUD

[Accountability](#)

[Adrien Ogée](#)

[Advancement](#)

[Africa](#)

[Analysis](#)

[Asia Pacific](#)

[Call](#)

[Compendium on Protecting the Healthcare Sector](#)

[Conflict](#)

[COVID-19](#)

[Critical Civilian Infrastructure](#)

[Cyber 4 Healthcare](#)

[Cyberattack](#)

[Cyberattacks](#)

[Cyber Operations](#)

[Cyberpeace](#)

[CyberPeace Builders](#)

[CyberPeace Cafe](#)

[CyberPeace Institute](#)

[CyberPeace Lab](#)

[Cybersecurity](#)

[Event](#)

[general public](#)

[Global](#)

[Healthcare](#)

[Healthcare sector](#)

[Humanitarian](#)

[Human Security](#)

[Infodemic](#)

[International Norms](#)

[Marietje Schaake](#)

[Microsoft](#)

[NGOs](#)

[OEWG](#)

[Ransomware](#)

[Statement](#)

[Strategic Analysis Report](#)

[Stéphane Duguin](#)

[Together 4 Cyberpeace](#)

[Toolkit](#)

[Ukraine](#)

[UN](#)

[United Nations](#)

[WEF](#)

[Workshop](#)

RECENT POSTS

[Measuring harm from cyberattacks](#)

December 11, 2023

[Welcome to a new Executive Board Member of the CyberPeace Institute](#)

December 7, 2023

[Donor Series: Patricia Toothman](#)

November 22, 2023

Donation

Support the CyberPeace Institute

Individual lives can be changed dramatically by the acts of cyber criminals. We need your support to assist victims of cyberattacks in the NGO, humanitarian and healthcare sectors.

[Donate now](#)

Newsletter

Subscribe to our newsletter

Receive monthly news on what’s happening at the Institute: our impact, publications, events and important milestones.

First name*

Last name*

in capital letters please

Email*

Subscribe



Find Out More

[Careers](#)

[FAQ](#)

[Glossary](#)

[Privacy Policy](#)

Stay Connected

[Contact](#)

[Newsletter](#)

[Follow us](#)



© CyberPeaceInstitute 2023

The CyberPeace Institute’s staff and experts generate their own work and ideas consistent with the Institute’s mission. The Institute maintains strict intellectual independence for all its projects, events, and publications. The Institute maintains independent control of the content and conclusions of any products resulting from sponsored projects.