Global Health & Medicine. 2021; 3(4):246-248.
LETTER
DOI: 10.35772/ghm.2020.01105

Advocacy of cyber public health

Naofumi Hashimoto[1,2,*]

[1] Division of Partnership Development, Department of Global Networking and Partnership, Bureau of International Health Cooperation, National Center for Global Health and Medicine, Tokyo, Japan;
[2] Health Care Unit, Economic Research Institute for ASEAN and East Asia (ERIA), Senayan Jakarta Pusat, Indonesia.

Abstract: Thanks to technological advances in computers and communication, the Internet of Things (IoT) has been increasingly used in healthcare to foster digital health in several countries. In conjunction with this trend, cybersecurity has become a matter of paramount importance in terms of protecting healthcare services and health-related information from cyberattacks. With the spread of the COVID-19 pandemic, individuals are encountering false information on the Internet and social media. As a result, an infodemic, which involves people taking inappropriate actions that threaten their health, has occurred worldwide. Cyber public health is a concept that comprehensively encompasses the above issues from the viewpoint of health. This concept helps to prevent various attempts that adversely affect people's health and it utilizes the advantages of cyber technology to promote public health. Cyber public health is also an important concept from the viewpoint of national security.

***Keywords*:** Internet of Things, digital health, cybersecurity, cyberattacks, infodemic, national security

Thanks to technological advances in computers and communication, the Internet has become an indispensable element of social infrastructure, allowing people to exchange images, videos, audio clips, and documents through emails and social media and to purchase products online. With the advent of the Internet of Things (IoT), the concept of digital health is gradually expanding not only in high-income countries but also in low- and middle-income nations (*1*).

The World Health Organization (WHO) has explained digital health as follows: "Digital health, or the use of digital technologies for health, has become a salient field of practice for employing routine and innovative forms of information and communications technology (ICT) to address health needs". The term "digital health" is rooted in eHealth, which refers to "the use of ICT in support of health and health-related fields". Mobile health (mHealth) is a subset of eHealth and is defined as "the use of mobile wireless technologies for health". More recently, the concept of digital health has been introduced as "a broad umbrella term encompassing eHealth (which includes mHealth), as well as emerging areas, such as the use of advanced computing sciences in 'Big Data', genomics, and artificial intelligence" (*2*).

In conjunction with the expansion of digital health, the number of cyberattacks on health facilities is increasing in many countries (*1*). For instance, a hospital system in Germany had to shut down due to a cyberattack, and an emergency room patient died as a result (*3*). Moreover, Japanese research institutes developing vaccines have also reported cyberattacks (*4*). Therefore, the importance of cybersecurity in the field of digital health is increasing. In a white paper on ensuring digital health, the Global Digital Health Partnership describes cybersecurity in digital health as "the means by which health care, better services, and enhanced patient outcomes are delivered and ensured through a resilient and secure digital ecosystem that encompasses culture, people, process, and technology" (*5*).

In addition, the technologies used to conduct cyberattacks can dramatically evolve due to the rapid increase in communication speeds provided by 5G (currently in progress) and threats to conventional cryptography through the development of quantum computing technology (*6*). To enhance its response to cyberattacks, the Japanese Government will establish a cyber defense organization through collaboration among industry, government, and academia in 2022 to analyze cyberattacks and to devise countermeasures (*7*).

Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) broke out in Wuhan, China in December 2019 and subsequently spread around the world. It has become a crucial public health issue and has negatively impacted the world economy. Governments and institutions have implemented public health measures to control infection rates and prevent the spread of the disease. Several countries – including

Western countries, Japan, China, and Russia – have begun to develop vaccines, medicines, and diagnostic test kits for SARS-CoV-2.

Under such circumstances, a situation known as an infodemic may occur. In response to this issue, the WHO announced a joint statement with the UN, UNICEF, the UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, and the IFRC on September 23, 2020, about COVID-19 entitled "Managing the COVID-19 infodemic: Promoting healthy behaviors and mitigating the harm from misinformation and disinformation" (*8*).

The joint statement describes infodemics as follows: "An infodemic is an overabundance of information, both online and offline. It includes deliberate attempts to disseminate wrong information to undermine the public health response and advance alternative agendas of groups or individuals. Mis- and disinformation can be harmful to people's physical and mental health; increase stigmatization; threaten precious health gains; and lead to poor observance of public health measures, thus reducing their effectiveness and endangering countries' ability to stop the pandemic" (*8*).

A large number of deaths due to drinking methyl alcohol in Iran and Kazakhstan have also been reported as infodemic-related harms due to COVID-19 (*9*).
Moreover, a threatening new technology – deepfakes – can promote infodemics. Deepfake technology has begun to be used as artificial intelligence has evolved. According to the British Government, deepfakes can be defined as visual and audio content that has been manipulated using advanced software to change how a person, object, or environment is presented (*10*). At the same time, the US–China conflict has heated up, social divisions have expanded inside countries and beyond, and the spread of COVID-19 has spurred economic disparities; consequently, the number of people in dire straits has increased rapidly. As a result, social factors that encourage cyberattacks and infodemics have become more prominent.

Within this context, cyber public health is a concept that comprehensively encompasses the above issues from the viewpoint of health. This approach will help prevent various problems that adversely affect people's health in the cyber realm and utilize the advantages of cyber technology to promote health. Cyberattacks enable hackers to rapidly attack a large number of targets at the same time, at a low cost. Such attacks can negatively affect people receiving medical care at health facilities, cause misunderstandings regarding access to medical services, and hamper the research, development, and production of medical products. Hence, the concept of cyber public health is also important from the viewpoint of national security.

Funding: None.

Conflict of Interest: The author has no conflicts of interest to disclose.

References

1. Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. BMC Med Inform Decis Mak. 2019; 19:10.
2. World Health Organization. WHO guideline: Recommendations on digital interventions for health system strengthening. *https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1* (accessed October 19, 2020)
3. MIT Technology Review. A patient has died after ransomware hackers hit a German hospital. September 18, 2020. *https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware- hackers-hit-a-german-hospital* (accessed October 19, 2020)
4. The Japan Times. Cyberattacks on Japan coronavirus vaccine projects point to China. Oct 19, 2020. *https://www.japantimes.co.jp/news/2020/10/19/national/cyberattacks-coronavirus-vaccine-china-japan* (accessed October 20, 2020)
5. The Global Digital Health Partnership (GDHP). Securing Digital Health, White Papers, Global Digital Health Partnership (GDHP). *https://gdhp.nhp.gov.in/assets/pdf/WhitePapers2019/GDHP_Cyber_0102_Final2.1.pdf* (accessed January 25, 2021)
6. Takagi T. Cryptographic compromise risk. In: Cryptography and Quantum Computers (Takagi T.). Ohmsha, Tokyo, Japan. 2019; pp.28-52.
7. NIKKEI Asia. Japan calls on industry and academia to fortify cyber defenses. October 20, 2020. *https://asia.nikkei.com/Business/Technology/Japan-calls-on-industry-and-academia-to-fortify-cyber-defenses* (accessed October 20, 2020)
8. World Health Organization. Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation. Joint statement by WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, and IFRC. September 23, 2020. *https://www.who.int/news-room/detail/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation* (accessed October 19, 2020).
9. ABC News. Hundreds die in Iran over false belief drinking methanol cures coronavirus. April 28, 2020. *https://www.abc.net.au/news/2020-04-28/hundreds-dead-in-iran-after-drinking-methanol-to-cure-virus/12192582* (accessed October 21, 2020).
10. Government of United Kingdom. Centre for Data Ethics and Innovation. Independent report Snapshot Paper - Deepfakes and Audiovisual Disinformation. Published 12 September, 2019. *https://www.gov.uk/government/publications/cdei-publishes-its-first-series-of-three-snapshot-papers-ethical-issues-in-ai/snapshot-paper-deepfakes-and-audiovisual-disinformation* (accessed October 21, 2020)

Received November 24, 2020; Revised January 25, 2021; Accepted January 27, 2021.

Released online in J-STAGE as advance publication February 7, 2021.

Address correspondence to:
Division of Partnership Development, Department of Global Networking and Partnership, Bureau of International Health Cooperation, National Center for Global Health and Medicine, 1-21-1 Toyama, Shinjyuku-ku, Tokyo 162-8655, Japan.
E-mail: n-hashimoto@it.ncgm.go.jp