SECURITY NEXUS
A free, open access, international, peer-reviewed, online publication for the Daniel K. Inouye Asia-Pacific Center for Security Studies faculty and alumni.
apcss.org/nexus

Security Nexus Perspectives

COMBATING HEALTH-RELATED CYBER SECURITY THREATS WITH HEALTH SYSTEMS APPROACHES

By Drs. Sebastian Kevany and Deon Canyon *

Cyber Attacks on Health Systems

A clear overlap between cyber security and public health realms was made evident during the cyber attacks on Ireland's health system in May 2021. Through an encryption process, hackers were able to disable the functionality of the Irish health system, putting lives at risk through the postponement of operations and other essential services.

The challenge faced by the Irish government, and the public health system, was to weigh the trade-offs between paying ransom to the hacking group versus risking the release of protected public health information. At the time of writing, a legal injunction against the use of the information combined with public anti-ransom statements, has been an effective

* Drs. Kevany and Canyon are professors at the Daniel K. Inouye Asia-Pacific Center for Security Studies (DKI APCSS) in Honolulu, USA. The views expressed in this article are the author's alone, and do not necessarily reflect the official position of the DKI APCSS or the United States Government.

tool against the hacking group, and the feared loss of private data or contamination of medical records has been avoided.

Nonetheless, there are important global lessons in the Irish experience: firstly, that health systems have to be protected by enhanced cyber security in the same way that banks and other key societal mechanisms do; second, the risks associated with the increased reliance on digital versus paper records; and, third, questions around the degree to which privacy in health information should be idealized, or even routinely maintained, in modern society, remain unanswered.

The Contemporary Cyber Environment

Contemporary cyber insecurity and unregulated internet have been described as the modern Wild West – a domain in which conventional rules and laws, even when they can be applied, are almost impossible to enforce. The extremes of cyber freedom can be seen all around us – from verbal assaults and racism, to enabling extremist positions on political and social issues, to the ease with which pharmaceuticals, pornography, and other extreme or violent content can be accessed with relative ease by all members of society, regardless of age or educational level.

In turn, this collection of threats to both society and public health presents a range of national and international security challenges. At the present time, however, it seems highly unlikely that the transnational freedom of expression, trade, and virtual movement that the internet represents will be successfully controlled by any one government or surveillance effort. In the absence of a national or supranational controlling body, the status quo, therefore, looks set to continue. Even countries that enforce stricter national

internet policies are inevitably exposed at the international level, and circumnavigated by the inherently global and non-conformist nature of cyberspace.

The era of extreme cyber freedom, however, may be drawing to a close in the free world - as it has already drawn to a close in some nations where governments have determined social media to be 'unhealthy' for their populations. The exposure of links between cyber liberty and the growth of extremist and terrorist organizations dates back over a decade to the Arab Spring era, but has only more recently been felt in developed countries is the context of electioneering, Brexit, and most recently the January 6 attacks on the Capitol building.

Many, if not all, of the above issues can, in some way, be classified as global public health threats as well as security threats - for virtually every crisis is accompanied by impacts on health. There may, therefore, be opportunities for a concerted public health response to cyber extremism as part of a broader national and international response to the issue.

The Unique Cyber-Health Nexus

Health systems are particularly vulnerable to hacking, not least because of the sensitivity, and therefore potential ransom value, of the information they contain. In 2020, a research organization, Becker Health, revealed that of the hospitals surveyed in the US, 82% had experienced a cybersecurity incident in the past year, and yet healthcare cyber incidents account for only 1.5% of data breaches. However, of note, the average cost per breached data record was $408, which is two to five times the costs in other industries.

Further, Verizon's 2021 Data Breach Investigations Report shows that 2.2% (655) of all reported incidents and 9.0% (472) of all reported data breaches occurred in the healthcare industry. Also of note, the origin of threat actors behind these attacks has shifted from 2019, when actors were predominantly internal, to 61% external. The motivation behind these attacks has been 91% financial, 5% 'fun', 4% espionage and 1% 'grudge'. Cyberattack sophistication is also increasing, with hackers now able to modify medical records and even imaging scans in addition to stealing them.

There are three main causes of losses of confidential information in the cyber environment: malicious and criminal attacks account for 48% of all data breaches, followed by human error at 27% and system errors at 25%. Cyber incidents in healthcare organizations also have a more pronounced impact on customers who bring class-action lawsuits and are more likely to take their business elsewhere.

In response, there can be significant hardware and software costs to healthcare institutions as they may be required to update to new supported software or replace their entire networks. Some attacks, such as the 2017 WannaCry ransomware sponsored by North Korea, targeted medical devices and health services. Motivations behind state-sponsored attacks likely include market manipulation by targeting large healthcare organizations and the theft of intellectual property.

Far more specific motivations may be the aim behind future cyberattacks. Cyber assassinations are now well in the range of the possible as hackers could cease airflow to a patient or a ward; prevent patients from being moved to urgent surgery by freezing elevators; modifying patient scans to initiate emergency surgery; and altering the function of medical devices that keep patients alive.

During the pandemic environment in 2020, cyberattacks against healthcare-related organizations doubled, 28% of them were tied to ransomware. Phishing attacks were high risk, with tactics including: "exploitation of individuals looking for details on disease tracking, testing, and treatment; the impersonation of medical bodies requesting information, including the World Health Organization (WHO) and U.S. Centers for Disease Control and Prevention (CDC); and offering financial assistance or government stimulus packages in exchange for private information."

Public Health and Cyber Health Parallels

In both public had cyber realms, much of the nomenclature is the same: viruses, scans, bugs, and many other terms in the cyber security realm have been appropriated from the medical. In much the same way, cyber threats have much in common with infectious disease threats, often following the same arcs of acceleration and tapering off – in much the same way as epidemics. Further, the global nature of both cyber and public health considerations is now clear. There may, therefore, be much to learn from public health's responses to epidemic infectious diseases and viruses (rather than its approach to non-communicable disease) that may help with the conceptualization of a response to current cyber threats.

A Solution from Within Public Health?

Public health campaigns have a long history of success in responding to public health issues. Whether it is prevention messaging regarding HIV/AIDS, health education regarding STDs, malaria or tuberculosis, or the declarations of primary health care accords

such as Alma Ata, the world's population health has been inestimably improved by the efforts of organizations such as the World Health Organization; the World Bank; UNAIDS; the Global Fund to Fight AIDS, Tuberculosis, and Malaria; and bilateral initiatives such as the United States' Presidents Emergency Plan for AIDS Relief (PEPFAR).

Integrating cyber awareness messages into public health campaigns, and vice versa, may thus be a meaningful way of promoting education as to the perils and disinformation that is readily available in cyber space. For example, policy recommendations might include:

- Health campaigns for HIV and other infectious diseases could be expanded to include warnings about the risk of disinformation on the internet regarding treatment and prevention efforts. Such indirect approaches may result in both health and cyber awareness gains in many countries, with the public being encouraged, in health as in other realms, not to trust everything they read online.

- There may also be scope for a more direct level of involvement by the World Health Organization and other UN organizations to combat more general levels of misinformation in cyberspace. This might include a generalized set of policies and messaging campaigns that warn against internet 'facts' and 'fake news' in the realms of extremism, terrorism, and other realms through their distal or proximal relations to public mental or physical health.

- The primacy of internet privacy should be reviewed when balanced against the functioning of health systems, ransom requests, and hacking threats. The reality that we trade personal privacy for the many instant benefits of internet use may mean that personal data privacy can no longer be held sacrosanct. Likewise, a reduced

emphasis on data privacy will have significant potential benefits in preventing and containing future epidemics.

- Many of the apps, organizations and companies that allow for untraceable hacking activities are based in the US and Europe. Some of these, such as the Tor Onion Project, allow hackers to operate with complete freedom and anonymity during their ransom efforts. Though these apps are framed as ways of allowing fee and anonymous communication by dissident journalists and other noble cases via the internet, they also facilitate many dark web activities such as ransom, hacking, and human and arms trading. There may, therefore, be a need to review policies that allow for such criminal activities.

- Leadership perceptions of cybersecurity being an IT problem in healthcare must change as this has rapidly become a patient-care threat that requires an enterprise risk management approach to ensure the presence of adequate security controls.

The control of rampant cyber liberty will take time to achieve, in much the same way as speed limits for automobiles came long after their introduction. However, with a multi-sector national, supranational, and international response, employing the resources of all relevant organizations, progress can still be made in bringing both a thrilling and dark era of extreme cyber liberty to a close. As a civilization, we have learned - in recent years in particular - that threats to personal health are taken extremely seriously when presented to us by senior national and international health officials. There is no reason why the same set of principles should not be applied to the continuing and expanding cyber security threat and its nexus with global health.

The views expressed in this article are the author's alone, and do not necessarily reflect the official position of the DKI APCSS or the United States Government.
July 2021