CSIS Commentaries DMRU-010

23 March 2020

COVID-19 Exposes Vulnerabilities in Our Cyberspace

Beltsazar A. Krisetya
Head of Knowledge Management, CSIS Indonesia
b.krisetya@csis.or.id

The COVID-19 pandemic in Indonesia has temporarily altered the posture of cyberspace in daily life. As of mid-March 2020, government institutions and private companies have been implementing remote working through video conference, cloud computing, and intranet platforms as part of preventive measures to curb virus spread. Regional governments have also ordered a temporary closure of schools and resorting to online learning methods. President Joko Widodo himself has called for the public to 'work from home, study from home, and worship at home'. In times of pandemic, technology has taken a more central role at a larger portion for people to continue their daily activities and obtain information *via* cyberspace.

But what risks are looming as people (temporarily) stay at home and uses internet more frequently? We can expect at least three vulnerabilities that need to be managed so that the temporal surge of internet users *and* usage can make a meaningful contribution in slowing down the pandemic.

***First*, the rise of 'infodemic'**, an over-abundance of information—some accurate and some not—that makes it hard for people to find trustworthy sources and reliable guidance when they need it[1]. Unlike SARS (in 2002) and H1N1 (2009) outbreak, social media has now taken a key role in proliferating the infodemic. In Indonesia, no less than 232 hoaxes and misinformation surrounding COVID-19 has been identified, which mostly plays on racial sentiments and gives dubious health advices.[2]

Public inoculation against infodemic on infectious disease is then essential. A model by Brainard and Hunter on misinformation surrounding influenza, monkeypox, and norovirus suggested that curbing harmful health misinformation and disinformation by 10 per cent or making at least 20 per cent of the population immune to the harmful advice, mitigated the severity of a disease outbreak.[3]

The central government, however, has just begun to better coordinate in inoculating the public. The turn began when the national COVID-19 task force, led by the National Disaster Management Agency (BNPB), released COVID-19 one-stop online portal: *covid19.go.id*[4]. It highlights case statistics and counter-narrative on hoaxes. To ensure wider outreach, the portal launches its *chatbot* version on WhatsApp and gives free of charge access to its call centre and website from almost every mobile internet provider.

However, it can still do better on its timeliness. The regular updates on the statistics (number of cases, recovered, fatality) is still short of punctual. It still falls behind *kawalcovid19.id*, a crowdsourced initiative that provides almost real-time case update. Timeliness is essential as the disease is currently spreading at an exponential rate, and even a slight delay of information can alter public perception significantly. Also, the so-called "hoax-busters" feature mostly merely mirrors the hoax counter-narrative contents provided by Indonesian Anti-Slander Society (MAFINDO), another voluntary-based crowdsourced initiative. The crowdsourced efforts have initially filled the void left by the government to vaccinate the public against infodemic. As the government has now stepped up in its role, crowdsourced movements currently took a second role in holding government accountable for the data it discloses.

A more sceptical view, however, will say that crowdsourced anti-hoax campaign can also signify public distrusts and dissatisfaction towards the government's effort in providing reliable information so far. The government needs to step up its proactiveness, promptness, and transparency in disseminating information on COVID-19 to match the pace of infodemic from the opposite direction. Otherwise, the public may continue to look for—and be exposed by—information through any means and sources available to them.

***Second*, cyber-pandemic**. As people migrated from physical space to cyberspace, they are exposed to another kind of virus: computer viruses. Following the surging global interest on information on COVID-19, there have been more than 4,000 new coronavirus-themed internet domains registered since January. Compared with other new domains in the same period, coronavirus-themed domains are 50 per cent more likely to be malicious[5]. It

[1] World Health Organization, "Novel Coronavirus(2019-NCoV) Situation Report - 13," 2020, https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf.

[2] Kompas TV, "Kominfo Temukan 232 Berita Hoaks Corona," 2020, https://www.kompas.tv/article/71717/kominfo-temukan-232-berita-hoaks-corona.

[3] Julii Brainard and Paul R. Hunter, "Misinformation Making a Disease Outbreak Worse: Outcomes Compared for Influenza, Monkeypox, and Norovirus," *Simulation*, 2019, https://doi.org/10.1177/0037549719885021.

[4] BNPB, "Gugus Tugas Luncurkan Covid19.Go.Id," 2020, https://bnpb.go.id/berita/gugus-tugas-luncurkan-covid19-go-id.

[5] Check Point Software, "Update: Coronavirus-Themed Domains 50% More Likely to Be Malicious than Other

is apparent that cyber threat actors attempted to exploit public fear against COVID-19 and lack of technical skills of new users.

Most of the attacks come in the form of phishing, a fraudulent attempt to obtain sensitive data such as passwords and credit card details, or employee information. For example, an email has been circulated globally—appears to have been sent by the World Health Organization (WHO)—containing an info-stealing trojan disguised as an e-book "My-Health", which claimed to contain extensive research on novel coronavirus and guidance on protecting children and businesses[6]. Upon opening the file, it loads the notorious info-stealing trojan "FormBook", steals personal data, and sends it back to the cyber attack perpetrators.

In an end-user cyber threat, a large part of prevention depends on the human factor. COVID-19 pandemic has hit older generations the hardest, and cyber-pandemic will be just about the same. Older, working generations are more likely to be part of the 'digital immigrants' who are still familiarising themselves with ICT skills and digitalisation during remote working. This user group will be the likeliest to fall into phishing attempts that may compromise the safety of their data and their employer's.

The health sector will also be vulnerable to cyber-pandemic as they hold valuable and sensitive data in a great amount. In an overwhelmed healthcare system due to COVID-19 outbreak, a ransomware attack that disables hospital network and computers can tip the system over. In the U.S., there has already been a cyber attack amid coronavirus on the Department of Health and Human Services to slow the system down[7]. The second-largest hospital in Czech Republic responsible in running COVID-19 test has also suffered an attack that forced the hospital to temporarily shut down the IT network[8].

The Indonesian health system should not undervalue the cost of cyber insecurity, particularly in a time-sensitive pandemic where computerised hospital information system can both hasten disease control and invite risks of cyberattacks. Lest we forget, the global WannaCry ransomware has rendered patients' online information inaccessible in Jakarta's Dharmais and Harapan Kita hospitals in 2017[9].

***Third*, the digital divide in remote education**. Around 21 million of primary and secondary education pupils in Java and other islands' provinces—more than half of total student nationwide—is expected to resume education in "online classrooms". Ministry of Education (Kemdikbud) promoted its remote learning platform, *Rumah Belajar*. 'Edutech' start-ups have pitched in to provide free access to their education portals and materials. Mobile internet providers have also offered free quota to access online learning portals. It looks like a public-private partnership in edutech have provided ample response to the current pandemic.

And yet, the geographical disparity problem lingers. Internet penetration is higher in urban (74.1 per cent) than rural (61.6 per cent) area. Most internet users are also concentrated in Java (55.7 per cent)[10]. Students from low-

Domains," 2020, https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/.

[6] Malwarebytes Labs, "Cybercriminals Impersonate World Health Organization to Distribute Fake Coronavirus E-Book," 2020, https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/.

[7] Time, "U.S. Health Agency Suffers Cyberattack Amid Coronavirus," 2020, https://time.com/5803816/coronavirus-cyberattack/.

[8] Computer Weekly, "Coronavirus-Linked Hacks Likely as Czech Hospital Comes under Attack," 2020, https://www.computerweekly.com/news/252480022/Coronavirus-linked-hacks-likely-as-Czech-hospital-comes-under-attack.

[9] The Jakarta Post, "Businesses as Risk: Experts Sound Alarm on Cyberthreat," The Jakarta Post, 2019, https://www.thejakartapost.com/news/2019/02/22/businesses-as-risk-experts-sound-alarm-on-cyberthreat.html.

[10] APJII, "Penetrasi & Profil Perilaku Pengguna Internet Indonesia Tahun 2018," *Apjii*, 2019, 51, www.apjii.or.id.

income families and rural areas risks of being left behind in online education because they often do not have necessary devices nor adequate internet bandwidth to access the platform. Senior teachers may also experience generational digital divide in a sudden change from physical to digital classrooms.

Some classes eventually resorted to using messaging platforms like WhatsApp. Problem is, messaging platforms are synchronous, it is a real-time communication where students are expected to engage in the learning process at the same time. This can widen the digital divide for pupils who do not have constant access to the internet and devices. Worse, in some cases, the tutoring element of e-learning is being omitted altogether, as some teachers only give their students homework and assignment throughout the learn-from-home phase[11]. This will bring another problem called "homework gap", where students with limited internet access often find difficulties in finishing homework than those who do[12].

The idea of "closing the digital divide" altogether might be too far-fetched for this situation. Instead, the government should pursue further interventions that can enhance the accessibility and affordability of e-learning platforms. Else, e-learning may deepen the socio-economic class disparity in the cyberspace.

Possible Interventions

In times of pandemic, cyberspace becomes substitute—rather than complement—to physical space. And so, conditioning healthy cyberspace can be a key incentive for people to continue practising social distancing to slower the spread of the disease. These short-term interventions to adjust course can then be considered.

Improve data synchronisation and transparency. The launching of multi-channelled, one-stop information portal by the national task force is a welcomed improvement. The public now has a more centralised, authoritative source of information that may serve as a beacon of light in the fog of infodemic. However, it has yet to disclose anonymised geolocation history of confirmed COVID-19 cases on a national scale. This would have been helpful for the public to trace their movement for possible transmission. Several provincial governments have taken a further step to transparency by disclosing such geolocation data, as well as demography (age, gender), and geographical distribution. Nonetheless, national aggregation of the currently divergent data can help the public to see the entire picture. Coordination between central and regional data centres becomes crucial to achieve this.

Harmonise, but decentralise cyber resilience guidance to public and technical experts. In the current wave of cyber-pandemic, there are at least two risk groups: remote workers and health sector cyberinfrastructure. Thus, the realistic interventions given the time constrain are mass public education and mobilisation of technical experts. These are intertwining interventions and can be achieved through coordinated means by an authoritative national cybersecurity body. For example, the United Kingdom's National Cyber Security Centre (NCSC) recently published six-pages guidelines on preparing organisations for an increase in remote working amid COVID-19[13]. This sets a baseline for new remote workers to be more vigilant in spotting phishing attempts, while also guide technical staffs in organisations to fortify its cyberinfrastructure.

---

[11] Tirto.ID, "Segudang Masalah Belajar Dari Rumah Karena Corona COVID-19," 2020, https://tirto.id/segudang-masalah-belajar-dari-rumah-karena-corona-covid-19-eGqQ.
[12] Pew Research Center, "17% of Teens Sometimes Can't Finish Homework Because of Digital Divide," 2018, https://www.pewresearch.org/fact-tank/2018/10/26/nearly-one-in-five-teens-cant-always-finish-their-homework-because-of-the-digital-divide/.
[13] National Cyber Security Centre, "Home Working: Preparing Your Organisation and Staff," 2020, https://www.ncsc.gov.uk/guidance/home-working.

A similar flow can be modelled. The National Cyber and Crypto Agency (BSSN) can issue a cyber resilience guide to technical experts in public and private sectors, who will disseminate it further to its users. For a start, BSSN's white paper on health sector cybersecurity[14] can be a point of reference in safeguarding sensitive information on COVID-19 cases, particularly on 227 referral hospital nationwide[15].

Focus on specific e-learning platforms with mobile and asynchronous characteristics. The Ministry of Education (Kemdikbud) and regional governments indeed needs to engage with all platform types to broaden options for students and teachers. However, we need to prioritise on improving the more accessible and affordable e-learning platforms. Mobile-based web-apps are more accessible than its desktop counterparts, as Indonesia is a 'mobile-first' country with 44.2 per cent of users use mobile phone *exclusively* to access the internet[16]. 4G coverage is also broader than cable in all provinces. Furthermore, mobile phones and data packages are more affordable and accessible for students in a low-income household compared to laptop and broadband. In engaging partnership with private actors, the government, therefore, needs to ensure that each platform has an equally complete mobile version.

Asynchronous platforms are also preferred than synchronous platforms because it does not require its users to be connected to the internet all the time. Video streaming-based e-learning platform, therefore, must provide options to locally save its content in users' devices. This allows pupils to obtain learning materials and learning the materials at different times. Asynchronous two-way platforms, such as messaging board and forum will increase inclusivity compared to chatting platforms, as students and teachers do not have to be online at the same time. In provinces with low and unstable internet availability, an option to mass-produce learning material via micro-USB sticks can also be considered.

CSIS Indonesia, Pakarti Centre Building, Indonesia 10160
Tel: (62-21) 386 5532| Fax: (62-21) 384 7517
csis.or.id

[14] Badan Siber dan Sandi Negara, "Buku Putih Keamanan Siber Sektor Kesehatan" (Jakarta, 2020).
[15] Kompas, "Indonesia Umumkan 172 Kasus Corona, Pemerintah Siapkan 227 RS Rujukan," Kompas.com, 2020, https://www.kompas.com/tren/read/2020/03/18/09460065/indonesia-umumkan-172-kasus-corona-pemerintah-siapkan-227-rs-rujukan?page=2.
[16] APJII and Teknopreneur, "Infografis Penetrasi & Perilaku Pengguna Internet Indonesia," *Indonesia Internet Service Provide Association* (Jakarta, 2017).