Cybersecurity and COVID-19

Wenqing Zhao, YLS ‘20

In recent years, cybersecurity has increasingly gained attention from different actors and countries across the globe. Advanced cyber technologies, while epitomizing developments of the modern era, also generate unprecedented threats and risks for communities now relying on cyber tools as crucial means to communicate. The central feature of cyberspace as a borderless sphere with enormous reach provides both a significant monetary and political incentive for cyber crimes and misconduct and a seemingly insurmountable difficulty for cyber-defenses. How does COVID-19 affect cyber threats and defenses? This background paper aims to briefly discuss why COVID-19 could have a long-lasting influence on cybersecurity norms and how stakeholders should move forward.

Challenges

COVID-19 pandemic is a hotbed for cyber-security risks. It is not an exaggeration to characterize it as “the first event of its kind since the birth of the Internet,” a perfect setting for cyber criminals. In reality, long before COVID-19 was declared a pandemic, it had already spurred “an unprecedented number of online scams targeting people and business.” This COVID-prompted cybersecurity crisis is not going away anytime soon; its scale of attack and damage may not have been felt, properly detected, or sufficiently understood yet.

Various aspects of the pandemic could contribute to a potentially larger explosion of cyber crimes. First, the pandemic has forced many communities to exercise physical distancing, bringing numerous communications, operations, sales, and services to cyberspace. This creates an enormous incentive for hackers to breach the security of communications and transactions, as valuable information that is traditionally safeguarded in the form of physical copies (confidential materials like contracts) or secured transactions (banking accounts) can now be more easily accessed illegally online in a massive batch. That information is often processed using less safe encryption tools, as the technologically unsophisticated work-from-home masses are often lax on cyber protections, neglecting to use VPN software or attempting to “bypass controls for the sake of getting things done.” In some cases, the increase in online traffic itself can create technical maintenance pressures, undermining service providers’ capacities to provide cyber protections and exacerbating potential privacy breaches. In other cases, web or app services of online communications might not initially be designed to incorporate sufficient privacy-centric mechanisms. One now familiar concern is Zoom’s security and privacy problems, but it is merely one example of the new vulnerabilities.

Second, the pandemic generates significant social uncertainty and psychological anxiety, rendering the affected communities more vulnerable to cyber exploitations in the form of fraud and distortion. Cyber scams target the public’s heightened emotions in a crisis, a psychological phenomenon known as amygdala hijacking, and turn people’s fear, anxiety, and curiosity into opportunities to rip them off. Recent cases include cyber-criminals’ attempt to plant viruses on health workers’ communication systems with “phishing emails themed around coronavirus and pretending to offer information.” The public at large has also seen waves of scams,
ransom-ware, and other cyber-viruses disguised as application portals for COVID-19 tests, vaccines, and stimulus checks, preying on people’s desire for more certainty and security in a time when millions are experiencing financial and medical hardships. The rampant COVID-related cyber crimes have forced institutions like the Department of Justice, Internal Revenue Service, and even World Health Organization to issue statements on their websites, warning the public of risks of “hackers and cyber scammers.”

Last, the pandemic has no doubt stimulated political and racial messages, often times in forms of misinformation, propaganda, conspiracy theory, and information spams, all of which when coupled with tools of cyber disinformation intelligence can be deployed as powerful weapons against individuals, political parties, races, and even nation states. This risk is best illustrated by a quote from Tedros Adhanom Ghebreyesus, the Director-General of the WHO, that “we are not just fighting an epidemic; we are fighting an infodemic,” which are “an excessive amount of information about a problem, [making] it difficult to identify a solution.” Currently, the information space about COVID-19 is clogged by misinformation and rumors. Although any malicious disinformation operation from state-actors has yet to be identified, cyber-attacks with the aim of spreading misinformation have already been unleashed towards the Department of Health and Human Services related to its coronavirus response. Officials from HHS are concerned that the suspicious cyber activities could be linked to Russia in its attempt to “sow even more chaos in the American public.” In any case, the existing chaotic information space is already flooded with layman rumors, making professional cyber disinformation operations from both state actors and non-state actors even harder to detect and to prevent.

Implications

COVID-19 presents a fascinating opportunity to study two distinct but profound cyber-security questions: (1) in the short run, how could cybersecurity defense adequately respond to a disruptive emergency when a gap exists between current technologies/policies and the challenges presented? (2) in the long run, how would cybersecurity defense adapt to the possible prospect of a largely connect-from-home society? The answer to the first question could be integrated as part of cyber emergency protocols useful for other types of future crises that require immediate cyber defenses. The second question focuses on the long-lasting effects of the COVID-19 pandemic, although this possibility of a connect-from-home society where a large portion of human activities migrate to cyberspace has long been contemplated. COVID-19 accelerates and substantiates that possibility, making it an imminent issue of high relevance.

In the present case of COVID-19, the following observations emerge: (1) Existing technologies and policies clearly had not anticipated the scale of the cyber impact of a pandemic such as that caused by COVID-19. As a result, society has to cope with problems and risks as they surface along the way, but this defensive stance makes society vulnerable to invisible threats that have not yet been detected. (2) Certain aspects of disruptive emergencies are harder to deal with than others, for instance the limitation of fundamental technological capacities to host communications of the entire community online. In light of these
observations, society should aim in the future to adopt both preventive measures in the form of better critical infrastructure developments and promotions of digital literacy, and remedial measures that mitigate damage due to cyber breaches. As we ponder the question of COVID-19’s long-term effects, some of the emergency preventive measures will eventually converge with what a future connect-from-home society would generally require. In this process, policy-makers have a larger than usual role to play, in terms of not just emergency management, but also continuing behavior-guidance, utilizing tools like domestic criminal laws and international laws to hammer wrongful conducts, and also regulatory devices like subsidy and tax to incentivize public learning and cyber-security capacity building. Following discussions are some suggestions of how to move forward, with additional recommended readings attached at the end providing other interesting perspectives.

One thing to do in such an emergency is to equip the citizens with tools of cyber self-defense, by among other things promoting cybersecurity and digital literacy. The community has to be amply warned of cyber risks in their daily online operations, from security breaches to online scams, from privacy leaks to misinformation, and they need to know how to react. As the society gradually moves more of its functions online, cyber self-defense becomes indispensable.

Corporate America has reacted to COVID-19 by promoting cybersecurity literacy. Various consulting services, including McKinsey, have updated their corporate clients on work-from-home cybersecurity risks, outlining strategies to combat cyberthreats by enhancing security programs and reiterating safe remote-working protocols to their employees. The average mom and pop stores are not so lucky, however, as disclaimer-like public warnings from institutions like the WHO, by themselves, have proven unhelpful without more broadcasted systematic education of cyber-security literacy. The U.S. Department of Justice went a little bit further by identifying some examples of cyber fraud schemes in its public news release and by urging the public to report COVID-19 scams, promising to prioritize the “investigation and prosecution” of such crimes. Those measures are nevertheless largely remedial in nature, and therefore could not prevent the public from falling into victims in the first place. The FBI likewise issued a public alert regarding COVID-19 related fraud schemes. However, the reach of such alerts is limited. Furthermore, aside from warnings about cyber-fraud, not much public education has been devoted to addressing misinformation and privacy breach.

Policymakers should be thinking about creative ways to promote cybersecurity literacy in times of emergency and general media literacy in normal times. One way to do so is to collaborate with traditional media and social media to broadcast warnings, to educate the public on how to identify cyber risks, to teach them ways of defense, and to enhance the public’s general awareness of the importance of cybersecurity. Paid advertisements and special alert subscriptions are some of the ways to send out the message. A civics education program on digital literacy could also be incorporated into curricula that “span K-12 through adulthood,” as proposed by the Cyberspace Solarium Commission.
In addition to equipping citizens with tools of cyber self-defense, policymakers should use regulatory and legal tools to safeguard the information space, to strength capacities of critical infrastructure, and to incentivize privacy-centric communication and transaction software, working closely in collaboration with research institutions, the industry, and other nation states. Policymakers should also develop and maintain plans for different emergency circumstances, regardless of how remote they might seem at the moment, incorporating cybersecurity into their response plans.

DOJ and FBI have prioritized prosecuting COVID-19-related fraud in the hope of deterring cyber-criminals, but such measures have been limited to largely domestic frauds. Disinformation and other forms of international cyber threats are hard to contain. Therefore, active approaches like cybersecurity-monitoring should be adopted to combat cyber threats. The WHO, for instance, has set up a team of “mythbusters” working with search and media companies to spot the spread of rumors and to counter misinformation through aggressive filtration. Domestically, more governmental resources could similarly be devoted to identifying and fighting public cyber threats by working with search and media companies to take down scientifically unsound information harmful for public health, and also by sanctioning websites that facilitate misinformation of cyber crime.

Regulators should also incentivize the industry to develop more privacy and security features for their products. Even though the emergency of COVID-19 highlighted the importance of privacy and security, leading the market to gravitate towards privacy-centric products, that may not last. In absence of emergencies, companies by themselves might not be sufficiently incentivized to enhance their security features as those features are not always viewed as top priorities in more normal times. The U.S. government should encourage industry through subsidies, licensing, and regulatory requirements to continue strengthening consumer products’ privacy and security during ordinary times in anticipation of the inevitable extraordinary times.

**Further readings:**


