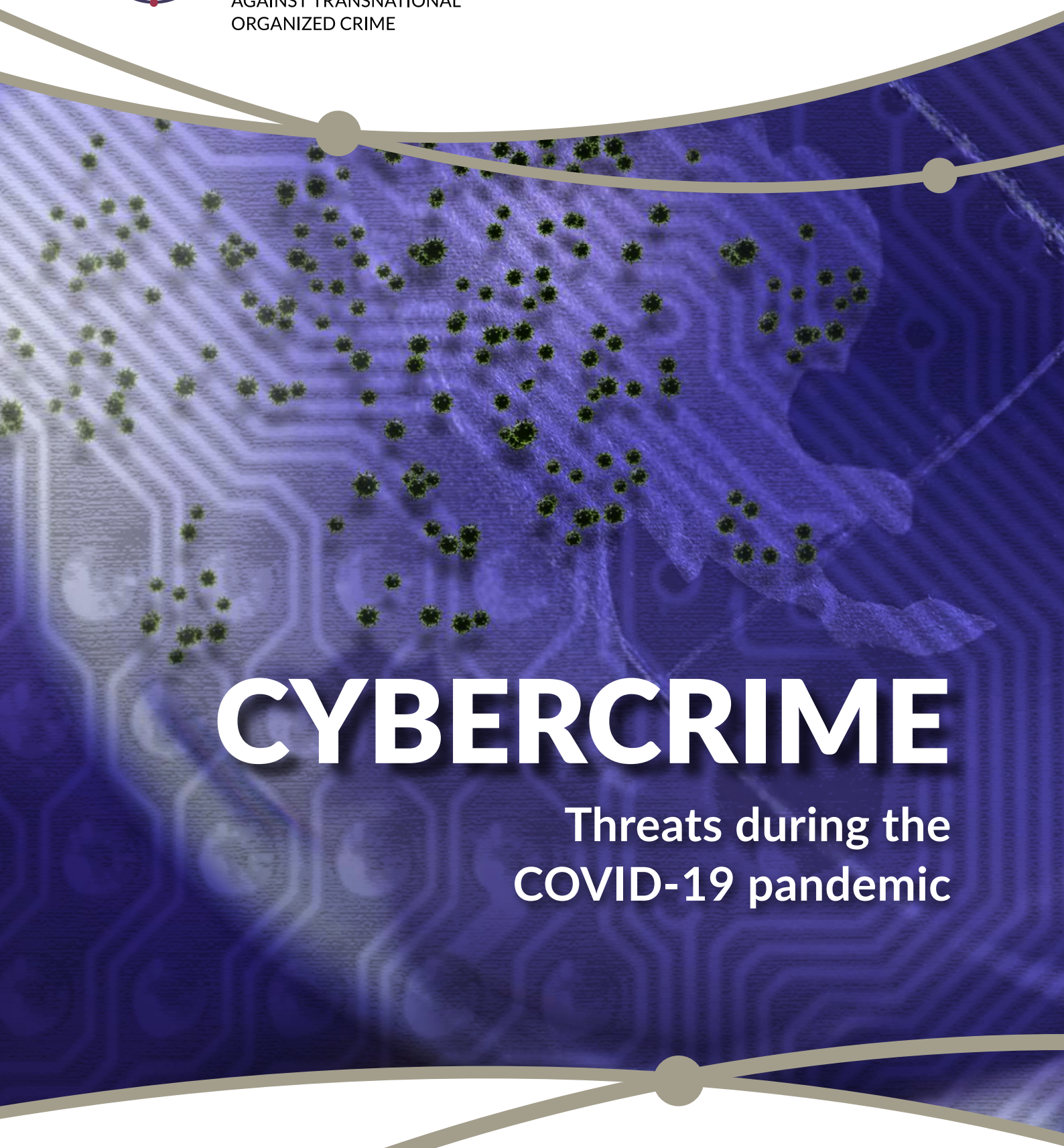
POLICY BRIEF

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME



CYBERCRIME

Threats during the COVID-19 pandemic

#COVIDCRIME WATCH

Prem Mahadevan

APRIL 2020

ACKNOWLEDGMENTS

This paper incorporates inputs of the Global Initiative Network of Experts and several others in the organization. Thanks in particular to Mark Shaw, Tuesday Reitano and Lucia Bird for their invaluable review comments. Thanks also to the Global Initiative publications team. Research for this paper was generously supported by the government of Norway.

Cover photo: © Sirichai Asawalapsakul/Getty Images.

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland

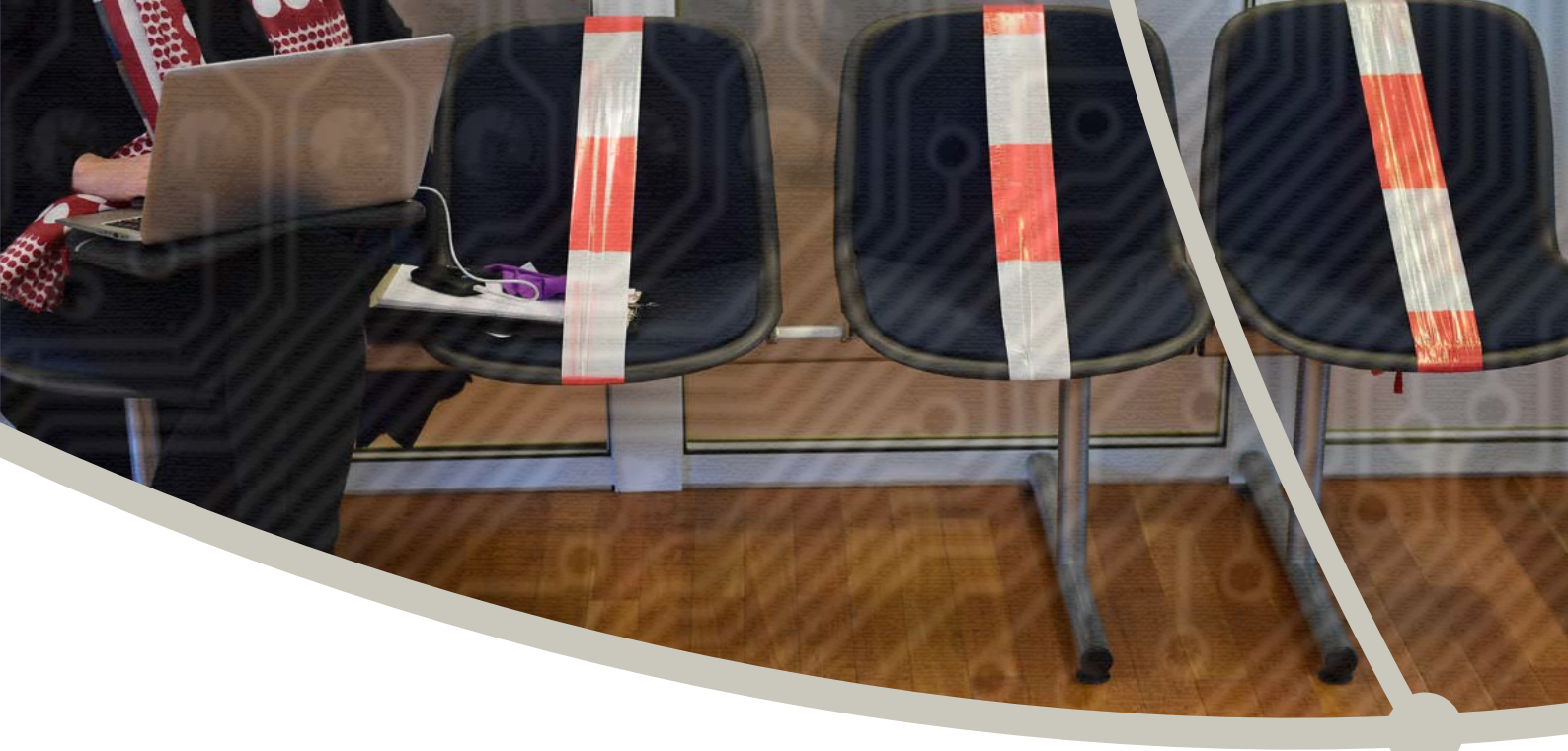
www.globalinitiative.net

CONTENTS

SUMMARY

As COVID-19 spreads quickly, so does the threat of cybercrime. Hackers are taking advantage of the current uncertainty to send out even more phishing messages than usual, with varying degrees of sophistication. The sector which is most crucial to containing the spread of COVID-19 – healthcare – is perhaps also the most vulnerable to ransomware attack.

Security experts are increasingly concerned about cybercrime because it currently benefits from favourable external conditions: a massive and uncoordinated shift to working from home offices in both public and private sectors, nationwide lockdowns which require increasing use of electronic transactions,[1] and a rush for basic necessities, which fractures any semblance of 'civil' society. In the long run, economic recession will likely trigger tectonic changes in how young people sustain themselves. An increased reliance on criminality, both online and offline, is to be expected, particularly in regions where youth unemployment was already high.



A WARNING SHOT IN CENTRAL EUROPE

The Czech city of Brno is an unlikely site for new developments in international cybersecurity. Surrounded by low hills, it is known among military historians for being close to the legendary battlefield of Austerlitz, where in 1805 Napoleon Bonaparte won his most spectacular victory. Yet Brno, which is rarely the subject of discussion outside the Czech Republic, became the site of a cyber attack in March 2020, which could have ripple effects across the world.

At the time of writing, details are still sketchy. Media reports say that on the night of 12–13 March, University Hospital Brno, the country's second largest, was hit by a ransomware attack that disrupted operations significantly. (Ransomware 'is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access'.)[2] Although life-saving patient treatment was not interrupted, the forced shutdown of data systems meant that medical information could not be shared between departments.[3] Urgent surgeries had to be postponed and patients redirected to an alternative hospital. What made this attack ominous was that it occurred less than two weeks after the Czech Republic reported its first case of COVID-19, at a time when the total number of coronavirus infections had already reached 117.[4] Within another two weeks, this figure would balloon to 1 400 nationwide.

University Hospital Brno is a COVID-19 testing and treatment location. The fact that its systems were compromised during a public health crisis made clear that the

Media reports say that on the night of 12–13 March, University Hospital Brno was hit by a ransomware attack that disrupted operations significantly.

hackers were willing to jeopardize patient safety in order to extort a ransom. Hitherto, hospitals and walk-in clinics had been favoured targets of data theft, with demands that they pay to avoid having patients' confidential information leaked over the internet. The human consequences of such attacks could be embarrassing and expensive, but unlikely fatal. Or, as with the British National Health Service (NHS) in May 2017, healthcare could become a collateral victim in indiscriminate ransomware attacks spanning many countries. But it was rarely the primary target, with innocent lives being put at risk.

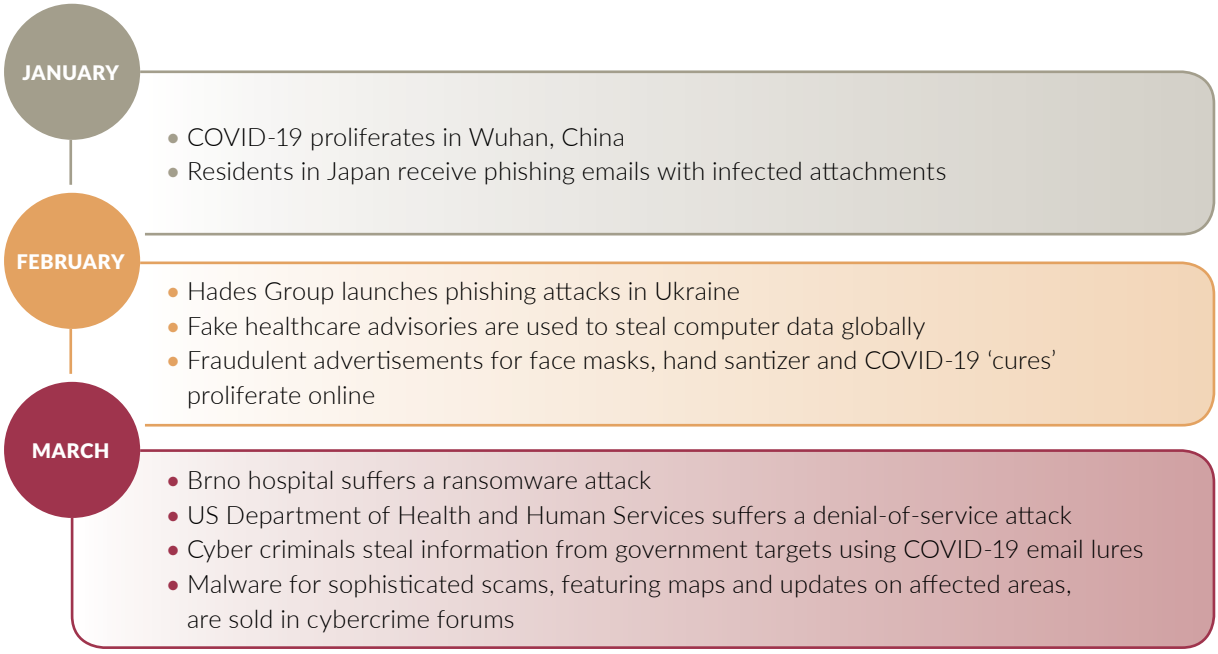


FIGURE 1 Cyber attacks during the pandemic

HEALTHCARE SYSTEMS AS TARGETS

Ransomware attacks

Brno 2020 is an example of criminals' preparedness to push boundaries, since the hack was a targeted one. Its perpetrators would have known the possible consequences of disrupting health services during a pandemic.

Previously, the British NHS had been hit by a free-spreading ransomworm, a type of malware that replicates itself across computers without user involvement. In that instance, cyber attackers exploited a vulnerability in Microsoft programmes. Information about this vulnerability was released on the internet one month before the global wave of attacks occurred in May 2017, including against the NHS. This particular ransomware attack was known as WannaCry and is estimated to have cost up to US$8 billion.[5] The NHS was only one of many targets hit worldwide, and was not specifically targeted. WannaCry indiscriminately hit 200 000 computers in 150 countries and was at the time viewed as possibly the biggest ransomware attack in history.[6]

In the following month, June 2017, a more devastating assault took place. Named NotPetya, it originally targeted businesses in Ukraine and international companies that traded with the country, before spreading across the globe and causing an estimated US$10 billion worth of damage. Like WannaCry, NotPetya did not deliberately target the healthcare sector, but the sector was affected anyway due to the fast-spreading nature of the malware. One Germany-based

One Germany-based multinational pharmaceutical company lost 15 000 computers in 90 seconds.

multinational pharmaceutical company lost 15 000 computers in 90 seconds. All of these machines had used Windows software. Meanwhile, hospital records in the United States could not be updated because NotPetya crippled speech transcription software that was used by doctors to dictate changes to patient files. In rare cases, surgeries had to be cancelled. In Ukraine itself, the encryption of Windows computers in hospitals meant that all upcoming medical appointments had to be cancelled.[7]

Between them, WannaCry and NotPetya escalated the seriousness of cybercrime as an international security concern. They showed that weaponization of encryption software and cryptocurrencies had made ransomware attacks more devastating.

Previously, bank payments to criminals could eventually be traced, and attack information could retrospectively be shared between companies to diminish risk, but the complete encryption of computerized data made it difficult to reject cyber extortionists' demands. Refusal to pay would mean crippling information losses, and paying through cryptocurrency would make it impossible for local law enforcement agencies to track the attackers.[8] In the case of NotPetya, the contrast between the clunky ransom payment mechanism and the malware's sophisticated infection techniques has led analysts to believe that the primary goal of the malware was destruction rather than profit.[9]

The attack on University Hospital Brno could be the start of a trend where healthcare systems are targeted by an increasingly sophisticated range of ransomware at critical moments, including public emergencies, to exert maximum psychological pressure. The level of damage inflicted by a cyber attack is linked to the preparedness of the entity that is hit. Days earlier, on 10 March 2020, the Champaign-Urbana Public Health District in the US state of Illinois was also hit by a ransomware attack. Its website, which was releasing safety information regarding COVID-19, was taken down. The district, which served 210 000 people, had to deliver updates through its Facebook page as it set up a new website. The ransomware used is known as NetWalker (also called MailTo) and has been observed by cybersecurity specialists since August 2019. In this attack, the district was able to continue operating as normal because it had taken the precaution of moving email accounts and patient health records to a cloud-based storage system six months earlier.[10]

Vulnerability due to weak cybersecurity

Although technical details on the Brno attack are still awaited, it is likely that the Czech hospital suffered from the same weakness as the NHS had: years of chronic underinvestment in information technology (IT) security.[11] When the WannaCry attack occurred, the NHS was using an outdated operating system known as Windows XP. Although Microsoft, the system's developer, had warned that users must upgrade to newer operating systems that had been 'patched' (protected) against the vulnerability that WannaCry exploited, this was not done.[12] The NHS's complacency was not unusual. In the following year (2018) there were at least 363 data breaches worldwide affecting the healthcare industry, which together resulted in the compromise of almost 10 million documents.[13] Perhaps

the vulnerability to such breaches stemmed from a naive assumption that because hospitals provide a public service, which even criminals require, they would be immune from malicious disruption. If such an assumption exists, it is not shared by cybercriminals.

Following the Brno hack, cybersecurity experts reached out to online forums, urging 'black hat' (illegal) hackers to exercise restraint against hospitals and pointing out that their own relatives might need treatment for COVID-19. Perhaps in response to this call, or more likely as a decoy to deflect police investigators, some cybercriminal groups have announced that they will not target the healthcare sector. Cybersecurity experts do not treat this assurance as credible.[14] Their scepticism partly stems from the fact that within just three days of promising restraint, a cybercrime group called Maze published the personal details, including healthcare records and passport and insurance information, of more than 2 300 former patients of Hammersmith Medicines Research. The company is engaged in clinical trials and could potentially play a role in testing for a COVID-19 vaccine.[15]

At a time when governments are concerned that the transmission rate of COVID-19 could leave hospitals short of essential equipment such as respirators, a computer system shutdown is one of the most severe threats facing crisis managers. But it is not the only one. Cyber threats vary greatly, and the healthcare sector is especially vulnerable to cybercrime.[16] Healthcare depends on rapid sharing of information, for example during preparation for surgery and in the treatment of accident victims who may have health factors that could trigger complications. The information architecture of medicine is thus built on openness, which is why hospital buildings are also more accessible to the general public than business premises are. This mentality extends to IT security. Studies have found that sizeable percentages of healthcare entities, from hospitals to private clinics, do not invest in basic software, such as email filters, that would normally catch certain types of malicious email. Picture archiving and communication systems are vulnerable to even moderately competent hackers. Such systems contain archived images of hospital patients' bodies and are configured to be swiftly shared with healthcare providers.[17]

PROFITING FROM A GLOBAL CRISIS

Exploiting uncertainty

Both in and outside the healthcare sector, COVID-19-era attacks are the latest in an established trend: cybercriminals take advantage of newsworthy events to spam potential victims with phishing emails. (A phishing email is one where the sender assumes a fake identity to trick the recipient into divulging confidential information, by pretending to offer something that the recipient may need or want.[18]) These scams rely on the innate human desire for clarity during an uncertain and fast-moving situation, and typically present phishing messages as providing an update on recent developments. Brexit, the Olympic Games, and the 2019/2020 Australian bush fires all served as backdrops for coordinated cybercrime offensives.[19] However, none of these events caused the widespread fear triggered by COVID-19. Consequently, none have offered such truly global opportunities for phishing attacks.

Phishing emails can easily be customized to fit local contexts. Countries from Canada to Switzerland have detected malware distributed through official-looking websites that claim to offer advice on avoiding or treating COVID-19.[20] These websites appear believable because they are crafted to convey a sense of immediacy and intimacy. For example, they reference place names which are known mostly to native inhabitants. Since many cyber attacks focus on small- and medium-sized communities in developed countries, a perfect storm of conditions exists for scamming. Ready access to the internet means that more people can potentially be reached by a phishing message, and their willingness to trust in local authorities increases a scam's chance of success.

Perhaps the earliest use of COVID-19 in phishing occurred in Japan in late January 2020. There, hackers used the Emotet banking trojan, a relatively old form of malware first seen in 2014, to infect computers. (A trojan is a type of malware that conceals its true purpose from computer users, who are fooled into downloading it believing it is legitimate software.) Masquerading sometimes as a welfare provider for disabled people and at other times as a local healthcare centre, hackers emailed people in several prefectures; Gifu, Osaka and Tottori were heavily targeted. Email recipients were urged to open a Microsoft Word attachment with information about the latest COVID-19 infections in their area. Those who did saw a prompt on the screen asking them to 'enable content' in order to view the attachments properly. Clicking yes released Emotet onto their computers, which would then harvest user credentials and financial information and allow hackers to use the computer for malware attacks against other targets. The emails were written in Japanese and tailored to look as though the authors were from the same area as the recipients.[21] At the time, public concern about COVID-19 was still limited to East Asia; Japan might have been the first phishing victim because of its proximity to China, where the virus emerged.

Cybercrime favours offensive rather than defensive players. Its practitioners are quick to exploit changes in external conditions.

As the virus spread, so did the scale of cybercrime exploiting it. The sophistication of internet-enabled scams directed at non-government entities, such as private companies and individuals, varied considerably. Several reports have mentioned phishing messages spoofed to look as though they originate from national healthcare authorities, such as the Centers for Disease Control (CDC) in the United States. These messages solicit donations for COVID-19 vaccine development. In other cases, internet advertisements have offered face masks and hand sanitizer, and occasionally even 'cures' for COVID-19. Buyers are required to make full payment in advance, but the product never arrives.

While some scams are basic and crude, others are cleverer. One is an email with a fake link to the CDC's website. Readers who click on the link are redirected to an Outlook login page, where they are asked to enter their account details to proceed further.[22] Those who do so are redirected to the actual CDC webpage, unaware that they could have accessed it directly without having to enter confidential information. A more internationally oriented variant of this scheme features a link to the website of the World Health Organization (WHO). The link in the phishing emails generates a pop-up on the genuine WHO site, which asks for email login details. After entering the requested information out of unthinking habit, the website visitor sees the pop-up disappear and is left free to browse the relevant WHO web pages.[23] The cybercriminals may not immediately use the information harvested in this way to steal money from the victims; instead, they may sell it to other actors in the digital underworld.

Exploiting fear

Cybercrime favours offensive rather than defensive players. Its practitioners are quick to exploit changes in external conditions. Wherever there is an outbreak of disease, cybercriminals play on visceral fears that exist even in modern, civilized society of

A phishing email's design can be enough to convince some people that it is an authentic communication.

dying alone or having to watch loved ones die. Before COVID-19, outbreaks of SARS, Ebola and Zika had provided 'psychological cover' for online scams. By alerting the public to new (and initially unpredictable) health and safety concerns, policymakers and the media inadvertently increase the chances that momentary impulse rather than ingrained caution will guide internet habits. Cybercriminals know how to take advantage of this; their emails are crafted to push readers' emotional buttons. Even people who might be normally cautious about opening unsolicited messages might allow themselves to be convinced that in an extraordinary situation, public health authorities would use big-data technologies to reach out to citizens and alert them about a new danger. A phishing email's design – using logos copied from the WHO website, for example – can be enough to convince some people that it is an authentic communication.

One campaign that began on 19 March 2020 uses a spoofed email address appearing to originate from the WHO director-general. Attached to this message is an executable file (.exe) that contains Hawkeye malware, which uses keylogging to capture passwords for emails and bank accounts and take screenshots and send them to controllers via encrypted email. Another scheme exploits widespread concerns about financial insecurity in the post-COVID world. Lately, there have been reports that Zeus Sphinx malware, a banking trojan first observed in August 2015, has been repurposed to target people who have lost their jobs due to COVID-19. Phishing emails have a Microsoft Word document attached that recipients are urged to fill out to apply for relief funds. When they open the form, they are prompted to enable macros; doing so triggers the malware and enables it to attach itself to files already stored within the device.[24]

New internet domains for COVID-19-specific cybercrime

Deceptive internet domains can also be set up to lend credibility to a message. To many people, emails that originate from *cdc-gov.org* might look like genuine CDC communications; in all likelihood, only a minority know that the agency's actual domain is *cdc.gov*. A pandemic, leading to lockdowns, triggers a mass hunger for both instant information and instant noodles. Being preoccupied with issues such as food hoarding, checking on the well-being of family members, and workplace and school shutdowns all detract sufficiently from one's sense of normalcy that disbelief becomes suspended. People who plan cybercrime attacks are practised manipulators, and know how and when to tap into the public's desire for more clarity about what is happening.

To take advantage of the distress and uncertainty created by COVID-19, many cybercriminals have opened special domains. One study found that out of 4 000 internet domains registered since January 2020 with the terms 'coronavirus' or 'COVID-19', 3 per cent are assessed as malicious and another 5 per cent as suspect.[25] According to the website domainscope.com, the number of domains with the words 'corona', 'virus' and 'covid' surged during the period 7 January 2020 to 4 April 2020 (the date of writing), with the peak being reached around 13 March, even as the Brno attack was underway (see Figure 2).

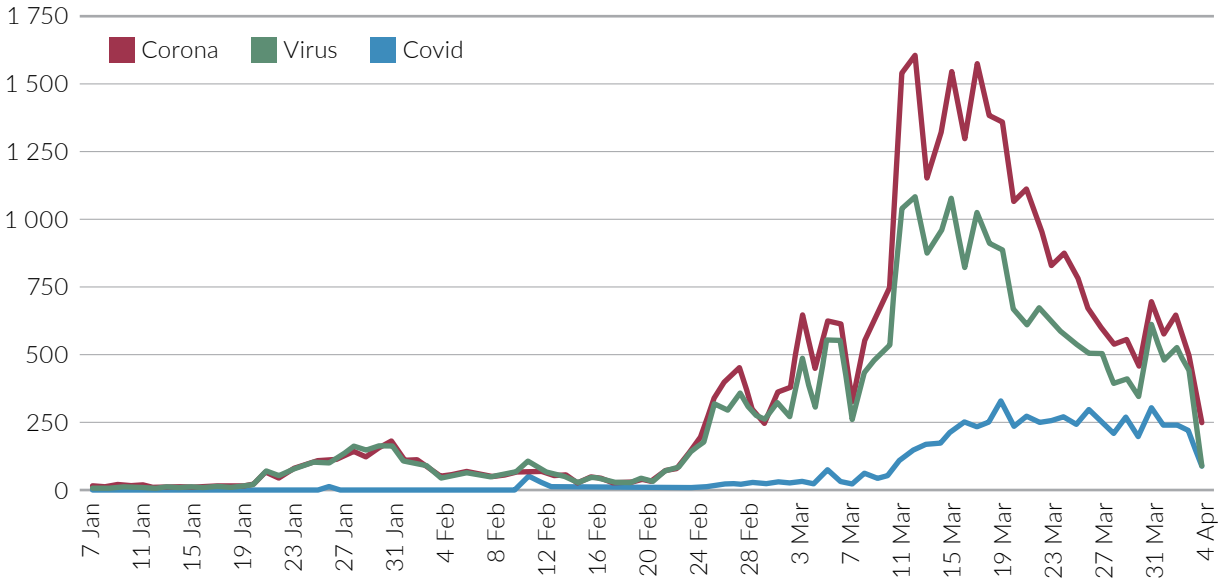


FIGURE 2 Domain names registered between 7 January 2020 and 4 April 2020

SOURCE: Domainscope.com

If public fatigue mounts as a result of 24/7 media reporting on the subject, and disgruntlement sets in with enforced lockdowns in Europe, Asia and North America, interest in COVID-19 could subside. On the other hand, an increase in death rates would be likely to prompt a mushrooming of more domains exploiting public fears. Much therefore depends on how effectively the disease can be contained in the coming weeks and months. In this regard, cybercrimes will follow the trendline of real-world events as medical researchers rush to develop vaccines and governments try to reduce the disease's spread.

A DUAL THREAT: ESPIONAGE AND CRIME FOR PROFIT

Governments confront two broad categories of cyber threats: espionage carried out by state and state-sponsored actors, and actions undertaken by criminal groups (some of which may also be state-sponsored) purely to make money.

Espionage

State-sponsored cybercrime groups are taking advantage of COVID-19 to break into government and corporate IT systems on espionage missions.

False messages about new infections and healthcare guidelines

An advanced persistent threat (APT) is a sophisticated hacking group that might have state backing. In March 2020, an APT originating from China and nicknamed Vicious Panda exploited coronavirus fears to attack Mongolian public-sector organizations. Using a malware known as Poison Ivy, which was embedded in a document titled About the Spread of New Coronavirus Infections, the APT sent spam emails while masquerading as the Mongolian Ministry of Foreign Affairs.[26] Poison Ivy is a remote access trojan (RAT), which allows a distant user to take control of a computer without its owner's knowledge. Using a RAT, hackers can secretly exfiltrate data, edit or delete files and carry out further attacks on other systems, with the infected computer serving as a proxy.

A second China-based APT nicknamed Mustang Panda (also known as TEMP.Hex) is believed to have used malware-infected Microsoft Word documents relating to COVID-19 to target Vietnamese, Taiwanese and Filipino entities via email.[27] For Vietnam, it used a covering message telling readers that the attachment contained a statement from Vietnam's prime minister about COVID-19.[28] Like Vicious Panda, Mustang Panda is speculated to have state backing.[29] In a similar vein, a North Korean APT nicknamed Kimsuky is believed to have inserted a malware called BabyShark into documents that supposedly detailed South Korean disease-control measures. These documents were then emailed to government functionaries in South Korea.[30]

APT36, identified by one cyber-investigations company as 'a Pakistani state-sponsored threat actor mainly targeting the defense, embassies, and the government of India' has been spamming Indian security personnel with fabricated messages about COVID-19.[31] The group uses several aliases, much as a terrorist organization may employ pseudonyms to confuse police investigators. It is also known as Transparent Tribe, ProjectM, Mythic Leopard, and TEMP.Lapis, and has been active since 2016.[32] In attacks on Indian IT systems, it has used a RAT known as Crimson, delivered through an infected document that purports to be a coronavirus health advisory issued by the Indian government. The RAT exploits a vulnerability in Microsoft Windows known as CVE-2017-0199. Such vulnerabilities or programmatic flaws are crucial to successful cyber penetration against a security-conscious target.

Synchronized attacks via phishing emails and social media

The Hades Group has targeted both public-sector entities and individuals in Ukraine using COVID-19 news as a decoy. The group is thought to have ties with APT28, which gained attention after US commentators accused it of hacking into the email accounts of 400 American political figures during 2015–2016. (APT28 is believed to have had a two-thirds success rate in that campaign, having originally targeted 600 individuals.[33])

Hades may have been the first APT to weaponize the intense public demand for information about the coronavirus spread. In mid-February 2020, it hid a trojan in documents containing the latest information on COVID-19. The documents were emailed to government officials in Kiev with covering messages that appeared to originate from the Ukrainian Ministry of Health. Even as these documents were being sent out, a separate wave of spam messages flooded social media users in Ukraine about the spread of COVID-19.[34] This second wave is likely to have had a dual purpose: to throw up a dust cloud that would mask the sophisticated hacking offensive against government networks, and to cause civil unrest. If the latter was an objective, it was attained: in one case, Ukrainians violently protested about the presence of evacuees from China, mistakenly believing that they were carriers of the virus.[35]

Hades may have been the first advanced persistent threat to weaponize the intense public demand for information about the virus.

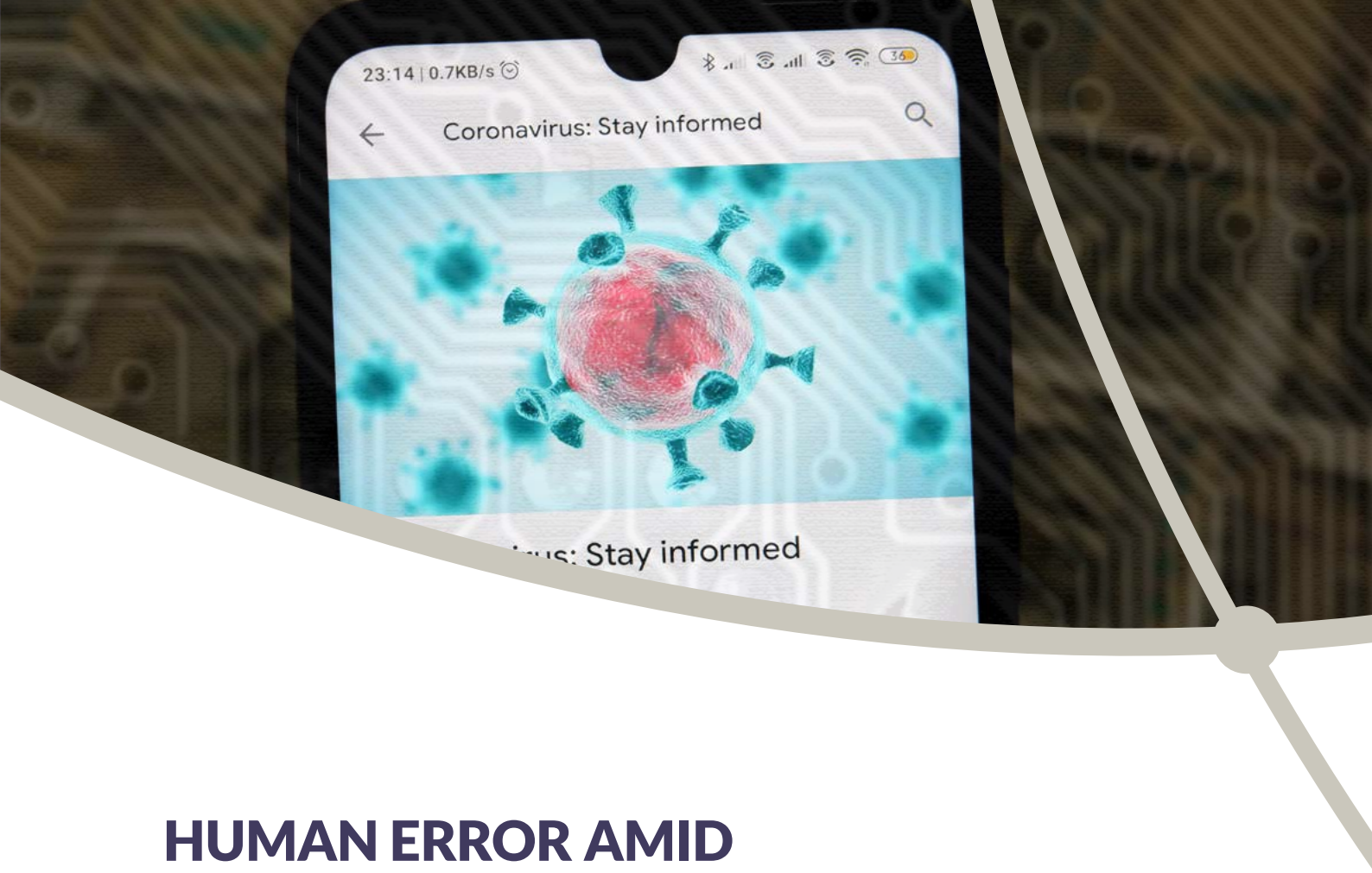
Through synchronized attacks that include rumour-mongering, cybercriminals can interfere with a government's efforts to maintain public order by triggering buying sprees of essential goods.

On 15 March, the US Department of Health and Human Services (HHS) was hit by a distributed denial of service attack, which used multiple computer systems to send simultaneous requests to the HHS website, overwhelming its capacity to handle requests and causing it to crash. The attack coincided with dissemination of a rumour sent by mobile text messages, email and social media that the US government was about to impose a nationwide quarantine. Investigators believe the two events could be linked, since the HHS website is one of the first websites that American citizens visit when they seek reliable information about COVID-19. By disrupting the website, cyber attacks added to public alarm created by the rumour.[36]

Crime for profit

In cybercrime conducted purely for profit, there is no clear boundary between state-sponsored and non-state actors. For example, the 2016 Bangladesh bank heist, which netted US$81 million, is thought to have been carried out by the Lazarus Group, an APT that, according to cybersecurity experts, has the support of an East Asian government.[37]

One of the most prominent cybercrime operations uncovered in recent weeks appears to achieve the sophistication commonly associated with APTs. It consists of spam emails that contain a link to a map of COVID-19's global spread. Clicking on this link activates malware known as AZORult, which is sold on East European cybercrime forums. Different variants of the malware have been available since 2016, with one type used for sextortion (blackmailing someone by threatening to release sexually explicit material about them if they do not yield to the blackmailer's demands) and another secretly establishing administrator privileges through remote-desk protocol (a technology created to enable IT support staff to access a computer remotely to address technical issues).[38] The website with the fake COVID-19 map is configured to closely resemble a genuine Johns Hopkins University website and is a highly convincing enticement for recipients of the phishing email. The malware kit needed for this scam is being sold on cybercrime forums, with prices starting at US$200.[39]



HUMAN ERROR AMID COVID-19-GENERATED VULNERABILITIES

Cybercriminals are serial entrepreneurs who rely on lapses in human judgement. The weaker their targets' security awareness, the easier it is to deceive them. During the current crisis, other urgent concerns may distract many people from the need to maintain cybersecurity. This is particularly because few computer users, even if they are vaguely familiar with words such as 'phishing' and 'trojans', readily associate them with potentially life-threatening situations.

Increasing use of home offices

There has been speculation that with the massive shift to home offices in February to March 2020, a tsunami of cybercrime, targeted at insecure personal wi-fi networks and non-sanitized computers, could lead to severe data breaches or losses.[40] This concern is less about the long-term risk of cyber attack (which is likely to increase regardless of whether people work from home), and more about the short-term risk that employees using less secure non-corporate IT systems could be hacked during the pandemic. There has reportedly been a threefold increase in phishing attempts in recent weeks, as employers have allowed employees to use home offices.[41] The remote conferencing technology used by Zoom, which saw a massive increase in demand during March 2020, proved vulnerable to video hijacking. Hackers were able to gain access to webcams and microphones on individual computers, and interrupt webinars.[42]

In addition to COVID-19-specific considerations, it is worth remembering that robotization was already making certain job categories redundant. One recent survey found that remote working increased in the United States by 173 per cent over the 15 years since 2005.[43] Thus, rather than seeing the current situation as an abrupt paradigm change, it might be more accurate to view it as part of an evolutionary trend in the nature of work practices. COVID-19 may well lead to a rise in the number of people working from home, but it might not be as transformative as some have predicted. While vulnerability to cybercrime is currently increasing, it may stabilize, albeit at a higher level, when conventional office-based work schedules resume.

Increased reliance on remote banking and payment apps

The lockdowns have forced many households to rely more on remote banking and payment.

The lockdowns that have been imposed in some countries have forced many households to rely more on remote banking and payment. As use of these systems becomes more convenient, it could become increasingly routine, even after restrictions on movement and public assembly are lifted. This opens new pathways for phishing scams and other types of cybercrime. Even if people are advised not to reflexively click on unsolicited email attachments or open mobile text messages, the propensity for human error assures that a sizeable percentage of individuals will nonetheless do so.

While lockdowns are still in effect, the increase in remote transactions could put banks' IT systems under strain.[44] This would provide an opening for cybercriminals to commit fraudulent transactions before bank staff can detect them. The fact that many bank staff are also working from home leaves them susceptible to being distracted, which would reduce their capacity to swiftly identify cyber risks. Meanwhile, a customer might not be able to immediately verify whether a supposedly urgent email or telephone call from a bank manager, asking for personal information, is authentic. Cybercriminals who operate phone scams tend to target vulnerable populations – such as the elderly or the isolated – who are most likely to be intimidated by a curt, businesslike voice urging them to divulge personal information or risk having their bank accounts frozen. As lockdown increases the social isolation of many people, the pool of such targets grows.

The effect of unemployment on crime

Even more enduring will be the risk posed by increased unemployment among young people. Job losses from COVID-19 have been projected by the International Labour Organization to eventually reach 25 million worldwide.[45] Particularly affected will be people whose positions were already facing rationalization before the crisis. Such individuals might lack the advanced technical skills needed to engage in cybercrime, but they could be tempted by cybercriminals to provide valuable information about their former employers.

If projections made by the International Monetary Fund prove accurate, and the world enters a recession worse than that of 2008–2009, unemployment will spike.[46] This is likely to drive many, particularly young people with relevant IT skills,

into criminal pursuits, including cybercrime. High unemployment rates among young people in the developing world and limited job opportunities in the legitimate IT sector create push factors for 'deviant globalization'. In such contexts, large numbers of youth can turn to cybercrime.[47] In Nigeria, for example, where unemployment rates exceed 50 per cent among 18- to 35-year-olds, cybercrime is an attractive source of fast money for disaffected youth.[48] During the early 1980s, when unemployment increased following a drop in oil prices and an economic downturn, the first '419 scams' appeared in Nigeria, so-named because the section of the Nigerian criminal code that dealt with fraud was numbered 419. Less than two decades later, the scammers had long stopped using fax machines and switched to phishing emails.[49]

Likewise, in late March 2020, police officials in Honduras noted that crime revenues from extortion declined precipitously as a result of COVID-induced movement controls imposed by the government, as well as the closure of local businesses. Criminal gangs that relied on extortion to pay members' salaries and welfare benefits have seen their revenue stream dry up. Law-enforcement officials have already tracked a displacement into other criminal activities, such as drug trafficking, and believe that the gangs have begun looking to cybercrime as a possible alternative source of funding. The increase in online purchases in Central America due to COVID-19 had caught the gangs' attention, and they were actively looking for ways to monetize this trend.

CONCLUSION AND RECOMMENDATIONS

Protecting both businesses and individuals against cybercrime in the post-COVID economy will be a top-down process in which governments must take the lead. For too long, the state apparatus has viewed cybercrime as a threat only if it engages in espionage (the first threat category discussed in this policy brief). Sophisticated cybercrime that extorts individuals and public and private service providers has fallen between the cracks in law-enforcement responses. The rise of ransomware together with the willingness of cybercriminals to attack healthcare systems at critical moments has meant this indifference is no longer conscionable.

Since investigation and cross-jurisdictional pursuit of cybercriminals is unlikely to become easier with time, especially due to increasing geopolitical tensions, incident-response measures as well as preventive measures will have to be taken. In terms of policy recommendations, these can be understood, respectively, as urgent measures (to be implemented during the crisis-related spike in cybercrime) and important measures (to be implemented after the immediate crisis has passed but while its long-term effects, most likely including a sustained surge in cybercrime, remain).

Urgent measures

1. Streamline public communication by government agencies. During times of uncertainty, people actively seek information and instinctively trust whatever they can find as a result of their own efforts, regardless of its authenticity. At the end of March 2020, the UK government was reportedly dealing with an average of 70 cybercrime incidents a week, many involving inaccurate information about COVID-19. By partnering with social-media firms, the government hopes to reduce the potential for cybercriminals to peddle false information, exploit fear and uncertainty to implement scams and embed malware, and drive public unrest.[50] To reduce the temptation to click on spurious links and email attachments, the UK and other governments can also modify their outreach mechanisms. One option might be to specify that all official information about an unfolding crisis will not be relayed via websites or social media but only via televised statements from authorized government spokespersons, delivered at fixed times daily. This method might reduce some of the risk posed by phishing scams. However, it would be a wholesale change in government outreach and is unlikely to happen quickly. Even so, a start can be made during the present crisis.
2. Promote threat-related information-sharing across and between governments. Information can be shared even if the details of threat-tracking methods remain secret. The most technically competent cybercrime groups tend to target specific geographic areas in accordance with the priorities of their host countries. But their methods, if successful, can be copied by others elsewhere, including groups that are purely mercenary and have no sense of national loyalty. The global cybercrime ecosystem is vast, but truly spectacular exploits are rare, and when they do occur, they grab the attention of other cybercriminals. This can generate a snowball effect within weeks or even days, as criminals rush to exploit a new vulnerability before it can be patched by cybersecurity experts. To reduce the fallout from such episodes, information about cyber threats must be shared between governments, and perhaps also with selected private companies, as a matter of routine.

During times of uncertainty, people seek information and instinctively trust whatever they can find, regardless of its authenticity.

Important measures

3. Introduce cybersecurity sensitization programmes in schools and workplaces. Much as military service is mandatory in certain countries, attendance at these programmes should be mandatory. The biggest vulnerability to both state-sponsored and non-state cybercrime remains human error. Experts agree that over 90 per cent of all cybercrimes involve some degree of active participation from the victim, even if this is just a click on an apparently innocuous and credible phishing email. The World Economic Forum has estimated that the proportion of cyber attacks that use 'social engineering' (i.e. deception) is as high as 98 per cent.[51] Protocols for cross-checking whether a message is genuine, especially if it is sent in a time of crisis or staffing shortage (such as during a holiday season), are essential. It is very well for pundits to advise that one should never open suspicious emails, but many cybercriminals are clever enough

to bait their messages effectively – a busy employee is unlikely to reflexively suspect that a message originating from a colleague in another department is actually a phishing attack, spoofed to look as though it has been sent from within the company.[52]

4. Increase investment in cybersecurity for public systems not linked to defence or intelligence, including healthcare systems. This should be a post-COVID priority. The WannaCry incident raised renewed awareness of the chronic underfunding of cybersecurity infrastructure across public-health systems. The likely continued popularity of health systems as targets for cybercriminals during COVID-19 should spur renewed investment in their cybersecurity infrastructure after the peak of the pandemic has passed and resources can be allocated to non-urgent concerns. Governments should apply the same wisdom more broadly and invest in cybersecurity across pivotal public systems whose targeting could cause widespread harm.

As COVID-19 spreads, ransomware attacks like the one in Brno are likely to increase. The difficulty of pursuing well-organized cybercriminals – not just technically but also jurisdictionally, if they are based in hostile foreign countries – should not be underestimated. Government and private-sector cybersecurity researchers usually make only qualified statements about responsibility for cyber attacks if the evidence trail crosses international borders. Thus, if a criminal actor hacks into a critical healthcare facility, it is unlikely that detection and prevention of the attack would occur quickly, and the attack could result in loss of life. In the world of cybercrime, this would be a watershed moment. INTERPOL has warned that cybercriminals are intensifying efforts to target hospitals during the COVID-19 pandemic, when resources are stretched to the maximum. The UK government believes it is only a matter of time before a cyber attack occurs that would have fatal consequences. All forecasts, therefore, point to an escalating threat to public safety from cybercrime.[53]

NOTES

1 'Lockdown', as used in this report, is a loose, non-technical umbrella term that includes both partial and complete (and both recommended and mandatory) self-quarantines (which are sometimes also referred to as shelter-in-place recommendations or orders).

2 This definition has been quoted from Malwarebytes, a cybersecurity company that is tracking COVID-19-related cyber attacks. See https://www.malwarebytes.com/ransomware/.

3 Sophie Porter, Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak, *Healthcare IT News*, 19 March 2020, https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak; *Prague Morning*, Czech Republic's second-biggest hospital is hit by cyberattack, 13 March 2020, https://www.praguemorning.cz/czech-republics-second-biggest-hospital-is-hit-by-cyberattack/; Rene Millman, Coronavirus test results delayed by cyber-attack on Czech hospital, *SC Magazine*, 16 March 2020, https://www.scmagazineuk.com/coronavirus-test-results-delayed-cyber-attack-czech-hospital/article/1677194.

4 Catalin Cimpanu, Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak, ZDNet, 13 March 2020, https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/.

5 Suzanne Barlyn, Global cyber attack could spur $53 billion in losses – Lloyd's of London, Reuters, 17 July 2017, https://uk.reuters.com/article/uk-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUKKBN1A20AH.

6 Madlen Davies, How hackers held the NHS to ransom, *New Statesman*, 15 May 2017, https://www.newstatesman.com/politics/health/2017/05/how-hackers-held-nhs-ransom.

7 Andy Greenberg, How the worst cyberattack in history hit American hospitals, Slate, 5 November 2019, https://slate.com/technology/2019/11/sandworm-andy-greenberg-excerpt-notpetya-hospitals.html.

8 Alex Hern, WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017, *The Guardian*, 30 December 2017, https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

9 Andy Greenberg, The untold story of NotPetya, the most devastating cyberattack in history, *Wired*, 22 November 2019, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

10 Debra Pressey, C-U Public Health District's website held hostage by ransomware attack, *News-Gazette* (Champaign, IL, USA), 11 March 2020, https://www.news-gazette.com/news/local/health-care/c-u-public-health-district-s-website-held-hostage-by/article_2dadedcd-aadb-5cb1-8740-8bd9e8800e27.html.

11 Brian Pinnock, What coronavirus teaches us about cybersecurity, *Gadget*, 16 March 2020, https://gadget.co.za/what-coronavirus-teaches-us-about-cybersecurity/.

12 Alex Bennett, Cyber superweapons and Windows XP – 5 reasons why the NHS attack was so successful, *Computer Business Review*, 18 May 2017, https://www.cbronline.com/breaches/cyber-superweapons-windows-xp-5-reasons-nhs-attack-successful/.

13 *SC Magazine*, NHS still a sitting duck for cyber-criminals, 5 July 2019, https://www.scmagazineuk.com/nhs-sitting-duck-cyber-criminals/article/1590166.

14 Mathew J Schwartz, Coronavirus cybercrime victims: Please come forward, Bank Info Security, 20 March 2020, https://www.bankinfosecurity.com/coronavirus-cybercrime-victims-please-come-forward-a-13992.

15 Bill Goodwin, Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack, *Computer Weekly*, 22 March 2020, https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus.

16 Courtney DuChene, When COVID-19 and cyber risk collide, lives hang in the balance, *Risk & Insurance*, 16 March 2020, https://riskandinsurance.com/when-covid-19-and-cyber-risk-collide-lives-hang-in-the-balance/.

17 Jessica Davis, Illinois Public Health website hit with

ransomware amid coronavirus, Health IT Security, 16 March 2020, https://healthitsecurity.com/news/illinois-public-health-website-hit-with-ransomware-amid-coronavirus.

18 This definition is adapted from Josh Fruhlinger, What is phishing? How this cyber attack works and how to prevent it, CSO, 13 February 2020, https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.

19 Jürgen Berke, *Cyberkriminelle greifen das Homeoffice an. Echt aussehende Info-Kampagnen zur Corona-Pandemie entpuppen sich als bösartige Phishing-Mails, die den PC zu Hause mit Schadprogrammen verseuchen*, *WirtschaftsWoche*, 20 March 2020, https://www.wiwo.de/technologie/digitale-welt/cybersecurity-hacker-reiten-die-corona-welle/25663550.html; Matt Burgess, Hackers are targeting hospitals crippled by coronavirus, *Wired*, 22 March 2020, https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing; Darren Cartwright, Cyber thieves target charity bushfire grants, *Sydney Morning Herald*, 26 February 2020; *Netzpalaver*, *Hacker bauen weiter auf die Angst vor dem Corona-Virus*, 6 March 2020, https://netzpalaver.de/2020/03/06/hacker-bauen-weiter-auf-die-angst-vor-dem-corona-virus/.

20 Sam Cooper, Canada's cyber agency dismantling fake government coronavirus pandemic response websites, *Global News*, 13 March 2020, https://globalnews.ca/news/6673497/canada-csec-fake-coronavirus-pandemic-response-websites/; *Bluewin*, *Kriminelle nutzen Corona-Krise*, 14 March 2020, https://www.bluewin.ch/de/news/vermischtes/kriminelle-nutzen-corona-krise-368531.html.

21 Okereke Onyekachi, Corona virus – the cyber attack, *Cyberkach*, 5 February 2020, https://cyberkach.com/2020/02/05/coronavirus/; Pascal Geenens, Coronavirus: Its four most prevalent cyber threats, Radware Blog, 12 March 2020, https://blog.radware.com/security/2020/03/coronavirus-its-four-most-prevalent-cyber-threats/?utm_source=Blog&utm_medium=Gaggle_Twitter&utm_campaign=Social.

22 Joe Tidy, Coronavirus: How hackers are preying on fears of Covid-19, BBC, 13 March 2020, https://www.bbc.com/news/technology-51838468.

23 Elaine Christie, Fake news: Phishing and email scams explode in the age of coronavirus, Privacy Hub, 19 March 2020, https://www.cyberghostvpn.com/privacyhub/fake-news-phishing-and-email-scams-explode-in-the-age-of-coronavirus/.

24 Charlie Osborne, Zeus Sphinx malware resurrects to abuse COVID-19 fears, ZDNet, 30 March 2020, https://www.zdnet.com/article/zeus-sphinx-malware-resurrects-to-abuse-covid-19-fears-and-steal-banking-data/.

25 Sara Morrison, Coronavirus email scams are trying to cash in on your fear, Vox, 5 March 2020, https://www.vox.com/recode/2020/3/5/21164745/coronavirus-phishing-email-scams.

26 Zak Doffman, Chinese hackers 'weaponize' coronavirus data for new cyber attack: Here's what they did, *Forbes*, 12 March 2020, https://www.forbes.com/sites/zakdoffman/2020/03/12/chinese-hackers-weaponized-coronavirus-data-to-launch-this-new-cyber-attack/#5c1370533861.

27 Shannon Vavra, Cybercriminals, nation-states increasingly tailoring coronavirus spearphishing campaigns, Cyberscoop, 12 March 2020, https://www.cyberscoop.com/coronavirus-phishing-scams-iran-china/.

28 Laurens Cerulus, Hackers use fake WHO emails to exploit coronavirus fears, *Politico*, 13 March 2020, https://www.politico.eu/article/hackers-use-fake-who-emails-to-exploit-coronavirus-fears-for-gain/.

29 Pierluigi Paganini, State-sponsored hackers are launching coronavirus-themed attacks, Security Affairs, 13 March 2020, https://securityaffairs.co/wordpress/99552/apt/apt-coronavirus-themed-attacks.html.

30 Insikt Group, Capitalizing on coronavirus panic, threat actors target victims worldwide, 12 March 2020, https://www.recordedfuture.com/coronavirus-panic-exploit/.

31 Zak Doffman, Hackers attack Microsoft Windows users: dangerous threat group exploits 'COVID-19 fear', *Forbes*, 16 March 2020, https://www.forbes.com/sites/zakdoffman/2020/03/16/this-dangerous-microsoft-windows-attack-exploits-covid-19-fear-governments-now-on-alert/#5ad415f7742d.

32 Threat Intelligence Team, APT36 jumps on the coronavirus bandwagon, delivers Crimson RAT, Malwarebytes, 15 March 2020, https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/.

33 Michael Isikoff and David Corn, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*. New York: Twelve Books, 2019, 78–79.

34 Catalin Cimpanu, State-sponsored hackers are now using coronavirus lures to infect their targets, ZDNet, 13 March 2020, https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/.

35 Patrick Reevell, Hysteria over coronavirus sparks violent protests in Ukraine, ABC News, 21 February 2020, https://abcnews.go.com/International/hysteria-coronavirus-sparks-violent-protests-ukraine/story?id=69124337.

36 John Santucci, Katherine Faulders, Josh Margolin, Luke Barr and Mike Levine, Suspicious cyberactivity targeting HHS tied to coronavirus response, sources say, ABC News, 16 March 2020, https://abcnews.go.com/Politics/suspicious-cyberactivity-targeting-hhs-tied-coronavirus-response-sources/story?id=69619094.

37 Jim Finkle, Cyber security firm: More evidence North Korea linked to Bangladesh heist, Reuters, 4 April 2017, https://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea/cyber-security-firm-more-evidence-north-korea-linked-to-bangladesh-heist-idUSKBN1752I4.

38 Sherrod Degrippo, Coronavirus-themed attacks target global shipping concerns, Proofpoint,

10 February 2020, https://www.proofpoint.com/us/corporate-blog/post/coronavirus-themed-attacks-target-global-shipping-concerns.

39 Justin Rohrlich, Concern for coronavirus victims evident even among cybercriminals in dark web forums, Quartz, 21 March 2020, https://qz.com/1822744/coronavirus-brings-out-softer-side-of-dark-web-cybercriminals/; Bradley Barth, Russian cybercrime forums seen selling malware-sabotaged COVID-19 map, *SC Magazine*, 13 March 2020, https://www.scmagazine.com/home/security-news/news-archive/coronavirus/russian-cybercrime-forums-seen-selling-malware-sabotaged-covid-19-map/.

40 Mark Sullivan, As people start working remotely, hackers are trying to exploit our anxieties, Fast Company, 18 March 2020, https://www.fastcompany.com/90478521/as-people-start-working-remotely-hackers-are-trying-to-exploit-our-anxieties.

41 Vinod Mahanta and Sachin Dave, Hackers are using Covid-19 disruption to infiltrate corporate networks, *Economic Times* (India), 27 March 2020, https://economictimes.indiatimes.com/tech/internet/hackers-are-using-covid-19-disruption-to-infiltrate-corporate-networks/articleshow/74837213.cms?from=mdr.

42 Kari Paul, 'Zoom is malware': Why experts worry about the video conferencing platform, *The Guardian*, 2 April 2020, https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing.

43 Nitzan Shatil, Protecting remote workers from cyber threats, Security Boulevard, 23 March 2020, https://securityboulevard.com/2020/03/how-to-protect-remote-employees-from-cyber-threats/?utm_campaign=Protecting%20Remote%20Workers%20From%20Cyber%20Threats&utm_content=122758395&utm_medium=social&utm_source=twitter&hss_channel=tw-954069116398329856.

44 Chris Baynes, Coronavirus: Banks urged to prepare for surge in cyberattacks as hackers look to exploit crisis, *Independent*, 6 March 2020, https://www.independent.co.uk/news/business/news/coronavirus-banks-cyber-attacks-hackers-crime-european-central-bank-a9381286.html.

45 Vicky McKeever, Nearly 25 million jobs could be lost globally due to the coronavirus, UN labor organization estimates, CNBC, 19 March 2020, https://www.cnbc.com/2020/03/19/nearly-25-million-jobs-could-be-lost-globally-due-to-the-coronavirus.html.

46 Martin Crutsinger, IMF head says global economy now in recession, ABC News, 28 March 2020, https://abcnews.go.com/US/wireStory/imf-head-global-economy-now-recession-69843184.

47 Prem Mahadevan, A social anthropology of cybercrime: The digitization of India's economic periphery, Global Initiative Against Transnational Organized Crime, forthcoming.

48 *Financial Times*, Nigeria election dominated by 'timebomb' of youth unemployment, 5 February 2019, https://www.ft.com/content/bc74b71a-2628-11e9-8ce6-5db4543da632.

49 Daniel Engber, Who made that Nigerian scam?, *The New York Times*, 3 January 2014, https://www.nytimes.com/2014/01/05/magazine/who-made-that-nigerian-scam.html; see also and John Scannell, The '419 Scam': An unacceptable 'power of the false'?, *Journal of Multidisciplinary International Studies*, 11, 2 (July 2014), https://epress.lib.uts.edu.au/index.php/portal/article/view/3220/4579.

50 Danny Palmer, Coronavirus: Now COVID-19 phishing scammers face 'rapid-response' crackdown, ZDNet, 30 March 2020, https://www.zdnet.com/article/coronavirus-now-covid-19-phishing-scammers-face-rapid-response-crackdown/.

51 Algirde Pipikaite and Nicholas Davis, Why cybersecurity matters more than ever during the coronavirus pandemic, World Economic Forum, 17 March 2020, https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/.

52 Alexander Martin, Coronavirus face masks: Dark web drug dealers rush to meet demand, Sky News, 15 March 2020, https://news.sky.com/story/coronavirus-face-masks-dark-web-drug-dealers-rush-to-meet-demand-11957636.

53 Alexander Martin, Coronavirus: Cyber criminals threaten to hold hospitals to ransom – Interpol, Sky News, 4 April 2020, https://news.sky.com/story/coronavirus-cyber-criminals-threaten-to-hold-hospitals-to-ransom-interpol-11968602.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with 500 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www. globalinitiative.net