SECURITY & DEFENCE QUARTERLY
https://securityandefence.pl/

Mechanisms for providing cybersecurity during the COVID-19 pandemic: Perspectives for Ukraine

Oleksandr Karpenko[1], Aleksander Kuczabski[2], Vitalii Havryliak[3]

[1] https://orcid.org/0000-0002-9301-7973

[1,3]Department of Information Policy and Digital Technologies, National Academy of Public Administration under the President of Ukraine, 20, Antona Tsedika str., 03057, Kyiv, Ukraine

[2] https://orcid.org/0000-0003-1271-0782

[2]Department of Regional Development, University of Gdańsk, Jana Bażyńskiego 4, 80-309, Gdańsk, Poland

[3] https://orcid.org/0000-0002-2058-1987

Abstract

The article analyses key cybersecurity trends against the background of the COVID-19 pandemic, trends that could lead to an increase in cyber threats. It also looks at cyber threats related to remote work in this period. Foreign experience in counteracting the spread of disinformation online, about COVID-19, has been studied. A global trend for strengthening law enforcement control over cyberspace content, network traffic, and digital devices of users has been identified. It has been established that some states are finding it difficult to counteract the spread of coronavirus-related threats and are sometimes resorting to violating the traditional balance of rights and freedoms of citizens in cyberspace, in fact, legalising cyber-surveillance of citizens. The paper investigates the limits of state intervention in the lives of citizens in the face of a real threat to national security. In matters of cybersecurity in the medical sphere, a shift of emphasis from the problem of protection of personal data of patients to the protection of key functions of the medical sphere is revealed. Mechanisms for implementing cybersecurity to counter the spread of fake news (misinformation) on the internet, about COVID-19, are substantiated. Practical tools and cybersecurity measures used during the COVID-19 pandemic are recommended for Ukrainian authorities. The importance of creating appropriate conditions for ensuring the balance between the implementation of restrictive policies in the field of cybersecurity and ensuring freedom of speech and openness of the internet is proven.

Keywords:

cybersecurity, fake news, pandemic, COVID-19, Ukraine

Article info
Received: 22 May 2020
Revised: 30 December 2020
Accepted: 8 Februrary 2021
Available online: 12 March 2021
DOI: http://doi.org/10.35467/sdq/133158

Introduction

The COVID-19 pandemic is one of the most significant challenges facing human civilisation today. The key features of the pandemic are its global nature, its ability to radically transform the established way of life and activities of people, and its ability to cause a domino effect that extends far beyond health care, economics, or politics. The pandemic forced the mobilisation of significant resources to avoid threats and overcome its likely consequences; each state was forced to respond quickly and effectively to the challenge. The most effective and widespread method was the quarantine scenario although were some differences in the approaches, actions, features, and consequences of the fight against coronavirus infection.

The most vulnerable dilemma was to reconcile the tasks of human health with the protection of fundamental rights and freedoms. Each state, to one degree or another, acted to temporarily infringe on the rights and freedoms of its citizens to stop the spread of the disease and take control of the epidemiological situation. With the unprecedented strengthening of state control over people's lives and activities, the role of security elements has grown. Cybersecurity has therefore taken up the role of a guarantor of the management system and not only of its stability. In fact, cybersecurity measures are designed to guarantee the rights and freedoms of citizens, even in limited forms.

Fortunately, the pandemic began in an environment where the dynamic development of technology allowed the means for counteracting the negative effects of the spread of the disease to be found quickly. In the search for a medical and pharmacological solution to the problem, e-government systems, which have been implemented in most countries of the world, have proved to be quite useful.

At the same time, crisis phenomena traditionally lead to the intensification of various hacker groups. One of the most discussed issues in the international arena today is the COVID-19 pandemic, in the context of which there has been an increase in illegal activity in cyberspace at the global level. Attackers have been using the coronavirus situation to commit phishing, fraud, disinformation, and other criminal activities on the internet. The purpose of the article is to analyse the COVID-19 pandemic in terms of cybercrime, to identify cyber threats related to the COVID-19 pandemic and remote work during restrictions, and to identify problematic aspects of providing cybersecurity in Ukraine during the COVID-19 pandemic.

In the research process, a critical analysis of the scientific literature in the field of cybersecurity was carried out. A study of the functions of the public administration system for the formation and provision of cybersecurity was made and official documents that regulate various security issues were analysed. In addition, an analysis of the practical implementation of the internet system for preventing the spread of coronavirus infection in Ukraine was conducted.

Global cybersecurity challenges related to the pandemic

Society was unprepared for quarantine measures related to the spread of COVID-19. The pandemic has had global socio-economic consequences, and its effects, according to experts, will be felt for decades to come (Tedros, 2020). The spread of the SARS-CoV-2 virus, among other things, has exacerbated the issue of cybersecurity, which directly affects society and business, because during crisis situations in cyberspace, various hacker groups traditionally become active.

Long before the pandemic, much in terms of the development of technologies of information exchange between people and authorities for mapping the spread of infectious diseases had been achieved in the world (Lwin *et al.*, 2014). But the effectiveness of systems such as communication between government and the people in general depends on the factor of trust (Goggin, 2020).

An unprecedented threat to public health has prompted authorities in various countries to resort to various COVID-19 tracking programmes to help contain the pandemic. However, according to Klar and Lanzerath (2020), the introduction of that kind of technology creates serious efficiency problems, technological problems and risks to confidentiality and fairness.

Haste in the introduction of new control technologies has, in practice, opened up the possibility of promoting commercial interest in various dimensions. Klein (2020) reveals the dangers of using anonymous behavioural data for commercial purposes. In general, the threat of social stratification under the influence of the deliberate use of the pandemic for enrichment has been defined as coronavirus capitalism (for more, see: Fuchs, 2020).

As the virus spreads around the world, people are naturally searching the internet for the latest information on COVID-19 and how it can affect them, what they can do to protect themselves and their families. Cybercriminals began to try to exploit this interest. Growing anxiety and the global fear of a pandemic have increased the likelihood of successful cyberattacks, as evidenced by the increasing number and range of cyberattacks in which cybercriminals exploit the COVID-19 pandemic using «social engineering» schemes, including cyber-fraud and phishing. The vast majority of cyberattacks begin with phishing by email, which directs a potential victim to download a file or access a URL that serves as malware.

On April 8th, 2020, the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) published a joint advisory on how cyber criminals and advanced persistent threat (APT) groups are exploiting the global pandemic (The United Kingdom's National Cyber Security Centre, 2020). An analysis of the situation in the UK shows that cybercriminals leveraged key events and governmental announcements to carefully craft and design cyber-crime campaigns (Lallie *et al.*, 2020).

Many countries have taken anti-epidemic measures to combat the coronavirus. As a result of the COVID-19 pandemic, hundreds of millions of citizens in many countries around the world were forced to go into mass quarantine. As restrictions on movement forced citizens spend more time at home, the time spent by people on the internet, in general, has increased, and the low level of digital competence (literacy) of most Internet users has intensified the illegal activities of hackers, cybercriminals and cyberterrorists. Demand for the use of various online communication platforms, especially video conferencing tools, has also increased.

The transition to remote work has highlighted, among other things, the issue of online work security. For example, thousands of Zoom video calls were left exposed (Harwell, 2020). The technical capabilities of video conferencing, text chatting, and collaboration tools were not ready for such increased demand from millions of people around the world.

Working from home has further increased the level of problems and challenges of cybersecurity that employers and employees have never faced before. The US National Security Agency (NSA) published a security assessment of the most popular video conferencing, text chatting, and collaboration tools in April 2020, including a list of security criteria to con-

sider when choosing tools/services for teleworking. (ZDNet, 2020). The NSA document is not only meant for US government and military entities but the private sector as well.

Cybersecurity is extremely important when working remotely. It requires extra effort and vigilance because of the inherent safety measures that are perceived and applied as appropriate when working directly in secure networks of government agencies, and businesses may not be fully aware during teleworking. Some organisations in Ukraine are tempted to temporarily reduce access to information by providing it to employees in a remote format. At the same time, such workers often do not have the appropriate digital skills and use home IT devices for remote work, which are less secure than the equipment they use in their workplace. This leads to a potential increase in the number of cyber incidents (including cyber espionage and compromising sensitive information or the organisation itself).

Cybercriminals have also targeted critical infrastructure, such as medical services (Stein and Jacobs, 2020; Fouquet, 2020; Computing, 2020). As a result, medical units fighting the coronavirus are periodically forced to fight viruses that infect their information systems. Such viruses can potentially damage not only the ability of medical information systems to protect patients' personal data, but also make it impossible to perform key functions of the medical field for a long time. Booking medical appointments, having distant medical consultations, and acquiring prescriptions electronically are just three health services that are already common, and can be vital at a time when lockdown plays a central role in the response to COVID-19 (Watts, 2020).

To prevent the spread of COVID-19, some countries have developed mobile apps and other digital tools to track potential contacts of their citizens with COVID-19 patients. Many countries have had recourse to apps, as flexible agents with the capacity to encode, materialise, represent and integrate such requirements, including some contradictory ones, and imagine and forge majoritarian support for social action (Goggin, 2020).

For example, a «COVIDSafe» app has been developed by the Australian Government Department of Health to help keep the community safe from coronavirus (COVID-19). «Aarogya Setu» is a mobile application developed by the Government of India to connect essential health services with the people of India in the fight against COVID-19. The «Aarogya Setu» app is aimed at augmenting the initiatives of the Government of India, particularly the Department of Health, in proactively reaching out to and informing the users of the app regarding risks, best practices, and relevant advisories pertaining to the containment of COVID-19. «Hamagen» is the Israeli Ministry of Health's COVID-19 prevention app. Germany's coronavirus tracking app «Corona Warning App» aims to track infection chains and curb the spread of the disease. Such mobile applications also help governments monitor public compliance with quarantine and self-isolation.

Researchers pay attention to the ethical aspect of the problem (Cosgrove *et al.*, 2020). It is a question of the probable restriction of the autonomy of users of such mobile applications. However, we should not forget about technical problems that may be the result of errors by developers or conscious or unconscious interference in their work from the outside. We have to agree with Klar and Lanzerath (2020) that any technology is only as good as the environment that supports it. Examples of the discrepancy between the expected state and reality can also be different. One of the technical problems is that some COVID-19 tracking apps do not work on smartphones that are older than two years (McLachlan *et al.*, 2020). According to Leprince-Ringuet (2020), false-positives could result in needless self-isolation or might cause users to ignore warnings if they are perceived as unreliable.

Ukrainian experience in implementing control over the epidemiological situation and security issues in a pandemic

To curb the spread of COVID-19 in Ukraine, a mobile app «Act at Home» was launched. Its basis is the experience of countries that use digital tools to ensure the safety of citizens during a pandemic. Prior to the pandemic, Ukraine already had significant e-government experience. In particular, the population was largely ready to use virtual forms of interaction with government agencies. However, some problematic issues remained:

- the traditionally low level of law-abiding citizens, which created problems with frequent evasion of the «Act at Home» application;
- the significant legal ignorance of the population about the requirements of the system and the possible consequences of evading its application;
- insufficient administrative and managerial discipline, which caused some chaos in terms of its practical application;
- deficient organisational culture, which arose in the effective cooperation of various services in the project: border authorities, health care facilities, police, social services, etc.;
- corruption and lobbying of individual medical laboratories that made money from clients who wanted to avoid long-term quarantine.

The «Act at Home» app's functions are as follows:

- Confirmation of the location of self-isolation with location determination;
- Photo confirmation of stay at the place of self-isolation;
- Emergency call to the Ministry of Health of Ukraine hotline;
- Planned functions for monitoring symptom development.

The «Act at Home» app is designed to maintain contact with the person and control the observance of obligatory self-isolation during the quarantine. The «Act at Home» app provides benefits during self-isolation, but installation is voluntary. It can only be installed by citizens with Ukrainian phone numbers (+380).

The «Act at Home» app allows you to confirm the location of self-isolation with the definition of geolocation, provide photo confirmation of the location of self-isolation, make an emergency call to the hotline of the Ministry of Health of Ukraine and monitor the development of symptoms. The app should be installed by people who came from countries in the «red zone» and must undergo a 14-day quarantine. An alternative to self-isolation is to take a PCR test in one of the Ukrainian certified laboratories.

According to the Ukrainian legislation, every citizen of Ukraine who has returned from the «red zone», does not want to undergo self-isolation for 14 days and wants to pass the PCR test to cancel self-isolation, must act according to the described algorithm:

- Install the «Act at Home» app, indicating your phone number and place of self-isolation;

• After crossing the border, reaching the place of self-isolation within 24 hours;

• During this time, the application will automatically remind you to mark whether a person has arrived at the selected location;

• Within 24 hours, it is possible to take a PCR test in a certified laboratory/clinic.

During the PCR test, the person must tell the laboratory/clinic representatives the phone number linked to the «Act at Home» app and fill in the consent for data processing. The agreement should establish that the border of Ukraine has been crossed and if this occurred in the last 14 days and the exact date of arrival in Ukraine. After passing the PCR test, the person should go to the place of self-isolation and indicate that they have arrived in the «Act at Home» app. The PCR test result should be ready within 24-48 hours. Employees of the certified laboratory/clinic independently transmit information about a negative PCR test result to the electronic system of the Public Health Centre of the Ministry of Health of Ukraine, indicating the person's phone number linked to the «Act at Home» app.

Abiding by self-isolation rules with the use of the «Act at Home» app is monitored with the help of regular messages at optional intervals throughout the day and verification of the person's face photo with the reference photo taken at the time the mobile app was installed, as well as the geolocation of the mobile phone at the time of photographing. If you receive a message, you need to take a photo of your face against the background of the environment within 15 minutes, so you should always keep your smartphone close by. Messages won't be sent at night.

If a person chooses self-isolation with the «Act at Home» app, this person must confirm this decision when passing passport control – first by providing a personal phone number and the address of the self-isolation place, and then showing the appropriate app screen to the State Border Service employee.

To get started with the «Act at Home» app, the person needs to enter the mobile phone number of the Ukrainian mobile operator, which will be active for the next 14 days. The number should receive a short SMS message with the code that must be entered for registration and, after permission to send messages is granted, the person should fill in information about the place of isolation (residence). After filling in the data about the place of self-isolation, the application will show a window "Are you already at the address of self-isolation or observation?". Upon arrival at the place of isolation, it is necessary to confirm arrival at the address of self-isolation and send a reference photo, which is also the recorded geolocation. In the future, artificial intelligence will compare the following photos, which should coincide with the reference photo. From the moment of authorisation, the person is considered to have chosen to exercise control with the help of the «Act at Home» app and can undergo self-isolation at the place of residence. After the user takes his reference photo, the main screen will open in the application with a counter of days until the end of quarantine. The countdown starts from 14 days. On the last day of self-isolation, the counter will show «0 days of self-isolation or observation left». When the self-isolation period expires, the message «Your self-isolation or observation period has expired» will appear instead of the counter, and the «Log out» button will become active, with which the user can log out of the application and delete if desired.

The experience of using the «Act at Home» platform in Ukraine has revealed several problems related to security issues, in particular concerning the impact of the poverty factor, which has reduced the effectiveness of the mechanism copied from the practice

of rich countries. Nagy (2019) claimed that Ukraine is at a very early stage of the evolution into a multiscreen nation. He noticed that although the number of Internet users in Ukraine is growing rapidly and steadily, it is still significantly lower (66%) than it was in Hungary five years ago.

The grounds for processing personal data by the «Act at home» app are defined in the Law of Ukraine No. 555-IX dated Apr. 13, 2020 «On Amendments to the Law of Ukraine «On Protection of Infectious Diseases» to Prevent the Spread of Coronavirus Disease (COVID-19)», according to which for the period of quarantine or restrictive measures related to the spread of coronavirus disease (COVID-19), and within 30 days of the date of its cancellation, «the processing of personal data is allowed without the consent of the person, including data relating to health, place of hospitalisation or self-isolation, surname, name, patronymic, date of birth, place of residence, and work (study), in order to counteract the spread of coronavirus disease (COVID-19), in the manner specified in the decision to establish quarantine, provided that such data is used solely for the purpose of anti-epidemic measures» (The Law of Ukraine, 2020).

At the same time, experts (Deutsche Welle, 2020a) are concerned about the technologies used in such coronavirus tracking apps, which enable governments to collect personal information. It also can lead to mass state surveillance, as well as the violation of the traditional balance of rights and freedoms of citizens in the digital space.

Coronavirus tracking apps may pose such personal security risks as:

- Deanonymisation of people who are in self-isolation or under observation;
- Unreasonable control over specific people through tracking their geolocation and movement;
- Using of personal data outside the official purpose for which it is legitimately collected;
- Processing information about individuals outside the time limits established by national legislation;
- Unauthorised interference with the operation of mobile devices in which mobile apps are installed.

Misinformation about COVID-19 as a global threat and a new challenge to the authorities

One of the current challenges today is the outbreak of disinformation about COVID-19. Although COVID-19 is not the first pandemic in history, it is the first to be covered so massively and with lightning speed. And the «fault» for this, oddly enough, lies with the internet and the technical privileges of this century.

Since the beginning of the coronavirus pandemic, the World Health Organisation has emphasised that not only COVID-19 but also false information about it poses a threat. False or misleading information about the coronavirus is primarily a threat to public health. The 2019-nCoV outbreak and response has been accompanied by a massive «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 (World Health Organisation, 2020).

Research has also shown that COVID-19 disinformation is disseminated significantly more widely than information about the virus from authoritative sources like the World Health Organisation (WHO) and the United States Centers for Disease Control and Prevention. By calling into question official sources and data and convincing people to try bogus treatments, the spread of dis- and misinformation has led people to ingest fatal home cures, ignore social distancing and lockdown rules, and not to wear protective masks, thereby undermining the effectiveness of containment strategies. The harmful effects of disinformation, however, go beyond public health concerns. For example, in the United Kingdom, the false claim that radio waves emitted by 5G towers make people more vulnerable to COVID-19 has resulted in over 30 acts of arson and vandalism against telecom equipment and facilities, as well as around 80 incidents of harassment of telecom technicians (Organisation for Economic Co-operation and Development, 2020).

A key channel for COVID-19 disinformation is internet platforms. The procedure for removing harmful and malicious content on internet platforms, including disinformation about COVID-19, is quite complicated. The spread of misinformation about COVID-19 forced many internet platforms to take bold action, including strengthening their support for independent fact-finding organisations and automated content moderation technologies to intensify their efforts to detect, remove, and counter false, deceptive, and potentially harmful content about COVID-19. In particular, Facebook has added a new feature to prevent the spread of fake news about COVID-19: a warning will appear before the user chooses whether to share the post. Facebook has added a new notification screen, which displays information about the article (for example, the date of first distribution and the source).

The goal, Facebook says, is to "help people understand the recency and source of the content before they share it" and to direct "people to our COVID-19 Information Centre to ensure people have access to credible information about COVID-19 from global health authorities." It builds on the platform's existing notifications, which it launched in June to help cut down on the spread of older links that routinely resurface in ways that can misrepresent current events (The Verge, 2020).

An additional problem in combating the spread of misinformation about COVID-19 on the internet is to ensure the preservation of users' rights to privacy and freedom of expression.

Key actions that governments and platforms can take to counter COVID-19 disinformation on platforms are:

• Supporting a multiplicity of independent fact-checking organisations;

• Ensuring human moderators are in place to complement technological solutions;

• Voluntarily issuing transparency reports about COVID-19 disinformation;

• Improving users' media, digital and health literacy skills.

A new trend among cybercriminals is the exploitation of the topic of a coronavirus vaccine. Experts of Check Point Software Technologies Ltd. were witnessing a doubling in the number of new vaccine-related coronavirus domains between June and July 2020 (Check Point, 2020).

In July 2020, the US Department of Justice formally charged two Chinese hackers with a global campaign to invade computer systems aimed at stealing intellectual property and

confidential business information, including a COVID-19 study (The United States Department of Justice, 2020). The indictment alleges two hackers worked with the Guangdong State Security Department (GSSD) of the Ministry of State Security (MSS), while also targeting victims worldwide for personal profit. The defendants also probed for vulnerabilities in computer networks of companies developing COVID-19 vaccines and treatments, testing the technology.

The UK, US and Canada accused Russian agents of carrying out cyberattacks to steal information on potential COVID-19 vaccines in July 2020 (Deutsche Welle, 2020b). The UK's National Cyber Security Centre (NCSC) said the hackers "almost certainly" operated as "part of Russian intelligence services" (BBC, 2020).

The potential theft of information about the development of a vaccine against COVID-19, testing technology and treatment may jeopardise the provision of safe, effective and efficient treatment options for the SARS-CoV-2 virus. The intelligence services called on research organisations in these areas to ensure a high level of cybersecurity to prevent the possibility of illegal access or theft of COVID-19-related materials.

In our opinion, the main factors that contributed to the increase of destructive (illegal) cyberactivity against the background of the COVID-19 pandemic were:

- Growing anxiety and global fear (panic) before the COVID-19 pandemic;
- The increased time that people were spending online in general, due to being at home more because of restrictions on movement;
- A sharp increase in the number of people around the world who, due to mass quarantine, switched to remote work;
- Growth in the number of phishing attacks in which cybercriminals exploit the COVID-19 pandemic by applying "social engineering";
- Increasing the number of fake sites through which attackers try to benefit from the pandemic.

The most dangerous categories of cyber threats and cyberattacks using the COVID-19 theme are:

- Spreading disinformation about COVID-19 on the Internet;
- Malware and phishing campaigns using COVID-19 baits;
- Cyberattacks on organisations conducting research and work related to treatment for COVID-19.

Conclusion

The Covid-19 pandemic, without objection, underscores our widespread dependence on the correct functioning of digital systems and tests the effectiveness and sustainability of government and corporate cybersecurity programmes. Hasty and unplanned decisions related to digital transformations are substantially fuelling the spate of cybersecurity issues. The COVID-19 pandemic has affected our entire work culture and has led to the emergence of a «new normal». The shifts were global, rapid, and widespread,

including remote work as the new norm, the use of collaboration tools «zooming» up, increased pace of digital transformation and the move to cloud (Sagey, 2020). How this ultimately turns out, and with what benefits for health, and what legacies it might leave for democratic freedoms and daily life, we must wait and see (Goggin, 2020).

At the same time, this new model of work increases security risks.

To ensure the preservation and protection of sensitive information, employees who perform tasks remotely are recommended to follow the following basic security measures:

- Configure home Wi-Fi according to the required level of protection (set a secure password, enable encryption, etc.);
- Use secure connections through standard VPN solutions (especially in public places);
- Make sure that personal devices have antivirus protection and are updated to the latest version of the operating system and security patches;
- Close all applications that are not actively used;
- To get acquainted with the methodology of attackers in the context of coronavirus issues;
- Follow the recommendations of the employer's organisation on cybersecurity.

In this case, it is recommended to avoid such actions:

- Leaving personal devices unlocked;
- Using unreliable connections to the internet or Wi-Fi;
- Auto-forwarding or forwarding sensitive information from official email accounts to personal email accounts;
- Opening suspicious emails or letters containing «emotional» headers with links;
- Using personal email accounts and personal cloud/file accounts for business purposes.

It is important for Ukraine's integration into the world community for it to continue implementing the strategy. The experience of advanced countries in the field of cybersecurity is key for Ukraine to avoid the negative consequences of the pandemic. However, it is important to take into account the poverty factor when implementing advanced information technologies for the general population. It is also advisable to work on improving the system to eliminate problematic issues that have arisen in terms of its practical application. Authorities are encouraged to fix vulnerabilities in their systems, perform periodic data backups, actively scan all web applications for unauthorised access, improve cybersecurity with protections such as multi-factor authentication, and identify suspicious account activity and stop their access to systems.

Funding
This research received no external funding.

Author Contributions
Conceptualization OK and AK; methodology OK, AK and VH; software VH; validation OK, AK and VH; formal analysis OK and VH; investigation OK, AK and VH; resources OK, AK and VH; writing—original draft preparation AK; writing—review and editing AK; supervision OK, AK; project administration OK and AK. All authors have read and agreed to the published version of the manuscript

Data Availability Statement
Not applicable.

Disclosure statement
No potential conflict of interest was reported by the authors.

References

BBC (2020) *Coronavirus: Russian spies target Covid-19 vaccine research*. Available at: https://www.bbc.com/news/technology-53429506 (Accessed: 9 September 2020).

Check Point (2020) *Threat actors join in the race towards a coronavirus vaccine*. Available at: https://blog.checkpoint.com/2020/08/11/threat-actors-join-in-the-race-towards-a-coronavirus-vaccine (Accessed: 7 September 2020).

Computing (2020) *Spanish hospitals targeted with coronavirus-themed phishing lures in Netwalker ransomware attacks.* Available at: https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware (Accessed: 4 September 2020).

Cosgrove, L., Karter, J. M., Morrill, Z., and McGinley, M. (2020) 'Psychology and surveillance capitalism: The risk of pushing mental health apps during the COVID-19 pandemic', *Journal of Humanistic Psychology*, 60(5), pp. 611–625. doi: 10.1177/0022167820937498.

Deutsche Welle (2020a) *In U-turn, Germany backs Google and Apple on virus app.* Available at: https://www.dw.com/en/in-u-turn-germany-backs-google-and-apple-on-virus-app/a-53252223 (Accessed: 6 September 2020).

Deutsche Welle (2020b) *Cyberattacks on COVID-19 vaccine research centers*. Available at: https://www.dw.com/en/cyberattacks-on-covid-19-vaccine-research-centers/av-54209631 (Accessed: 9 September 2020).

Fouquet, H. (2020) 'Paris Hospitals Target of Failed Cyber-Attack, Authority Says'. Bloomberg, 23 March. Available at: https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says (Accessed: 4 September 2020).

Fuchs, C. (2020) 'Everyday life and everyday communication in coronavirus capitalism. Triple C: Communication, Capitalism & Critique', *Open Access Journal for a Global Sustainable Information Society*, 18(1), pp. 375–399. doi:10.31269/triplec.v18i1.1167.

Goggin, G. (2020) 'COVID-19 apps in Singapore and Australia: Reimagining healthy nations with digital technology', *Media International Australia*, 177(1), pp. 61–75. doi: 10.1177/1329878X20949770.

Harwell, D. (2020) 'Thousands of Zoom video calls left exposed on open Web'. The Washington Post, 3 April. 2020 Available at: https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web (Accessed: 2 September 2020).

Klein, N. (2020) 'Coronavirus capitalism—and how to beat it', The Intercept, 17 March. https://theintercept.com/2020/03/16/coronavirus-capitalism/ (Accessed: (2 September 2020).

Klar, R., and Lanzerath, D. (2020) 'The ethics of COVID-19 tracking apps–challenges and voluntariness', *Research Ethics*, 16(3-4), pp. 1–9. doi: 10.1177/1747016120943622.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., and Bellekens, X. (2020) 'Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic'. arXiv preprint arXiv:2006.11929. Available at: https://arxiv.org/abs/2006.11929 (Accessed: 1 September 2020).

Leprince-Ringuet, D. (2020) 'Contact-tracing apps: why the NHS said no to Apple and Google's plan', *ZDNet*. Available at: https://www.zdnet.com/article/contact-tracing-apps-why-thenhs-said-no-to-apple-and-googles-plan/ (Accessed: 1 September 2020).

Lwin, M. O., Vijaykumar, S., Fernando, O. N. N. *et al.* (2014) 'A 21st century approach to tackling dengue: crowdsourced surveillance, predictive mapping and tailored communication', *Acta Tropica* 130, pp. 100–107. doi: 10.1016/j.actatropica.2013.09.021.

McLachlan, S., Lucas, P., Kudakwashe, D., *et al.* (2020) 'Bluetooth smartphone apps: are they the most private and effective solution for COVID-19 contact tracing?' arXiv. Epub ahead of print 15 May. Available at: https://arxiv.org/abs/2005.06621 (Accessed: 1 September 2020).

Nagy, S. (2019) 'Digital Economy and Society. A Cross Country Comparison of Hungary and Ukraine', *Visnyk Natsionalnogo Tekhichnogo Universytetu Kharkivskyj Politekhnichnyj Instytut Ekonomichni Nauky*, 46(1267). Available at: https://arxiv.org/ftp/arxiv/papers/1901/1901.00283.pdf (Accessed: 9 September 2020).

Organisation for Economic Co-operation and Development (OECD) (2020) *Combatting COVID-19 disinformation on online platforms*. Available at: http://www.oecd.org/coronavirus/policy-responses/combatting-covid-19-disinformation-on-online-platforms-d854ec48 (Accessed: 7 September 2020).

Sagey, M. (2020) *Securing the 'new normal' – protecting the post Covid-19 world*. Available at: https://blog.checkpoint.com/2020/06/09/securing-the-new-normal-protecting-the-post-covid-19-world (Accessed: 9 September 2020).

Stein, S. and Jacobs, J. (2020) 'Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak'. Bloomberg, 16 March. Available at: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response (Accessed: 4 September 2020).

Tedros, A. G. (2020) *Coronavirus pandemic still accelerating: WHO chief.* Available at: https://economictimes.indiatimes.com/news/international/world-news/coronavirus-pandemic-still-accelerating-who-chief/articleshow/76509332.cms?from=mdr (Accessed: 1 September 2020).

The Law of Ukraine (2020) *Pro vnesennja zmin do Zakonu Ukrajiny «Pro zakhyst naselennja vid infekcijnykh khvorob» shhodo zapobighannja poshyrennju koronavirusnoji khvoroby (COVID-19)* [On Amendments to the Law of Ukraine «On Protection of the Population from Infectious Diseases» to Prevent the Spread of Coronavirus Disease (COVID-19)]. Available at: https://zakon.rada.gov.ua/laws/show/555-20?lang=uk#Text (Accessed: 6 September 2020).

The United Kingdom's National Cyber Security Centre (2020) *Advisory: COVID-19 exploited by malicious cyber actors.* Available at: https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory (Accessed: 1 September 2020).

The United States Department of Justice (2020) *Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research*. Available at: https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion (Accessed: 9 September 2020).

The Verge (2020) *Facebook will now show a warning before you share articles about COVID-19.* Available at: https://www.theverge.com/2020/8/12/21365305/facebook-covid-19-warning-notification-post-misinformation (Accessed: 6 September 2020).

Watts, G. (2020) *COVID-19 and the digital divide in the UK*. Available at: https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30169-2/fulltext (Accessed: 4 September 2020).

World Health Organization (WHO) (2020) *Novel Coronavirus (2019-nCoV) Situation Report – 13.* Available at: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf?sfvrsn=195f4010_6 (Accessed: 7 September 2020).

ZDNet (2020) *NSA security guide: How to choose safe conferencing and collaboration tools.* Available at: https://www.zdnet.com/article/heres-the-nsas-guide-for-choosing-a-safe-text-chat-and-video-conferencing-service (Accessed: 3 September 2020).