No 391 / June 2020

Facts & Findings

KONRAD ADENAUER STIFTUNG

Coronaperspectives

The impact of COVID-19 on cyber crime and state-sponsored cyber activities

Johannes Wiggen

- Through the increased use of digital applications and the use of poorly protected private IT devices when working from home, the COVID-19 pandemic illustrates digital security risks and highlights the need for taking adequate action to protect IT systems in critical infrastructures.
- Cyber crime is currently benefitting from a sense of insecurity in the population and people's need for information
- States are increasingly using cyber espionage in order to gain information on measures for fighting the corona virus, potential vaccines and treatment options.
- Cyber risks can only be reduced to an acceptable level by implementing a set of actions: in terms of cyber crime, for example, programs for education, prevention and digital literacy must be strengthened and the resources of law enforcement agencies to prevent and investigate cyber crime must be enhanced by targeted recruitment of young staff; state-sponsored cyber activities should be addressed by imposing political and economic sanctions or bringing legal charges against countries as well as through cyber diplomacy.

Contents

The pandemic has led to a wider use of digital applications, prompted businesses and government agencies to move entire work processes online in an ad hoc fashion and has increased the dependence of hospitals on the proper functioning of their IT systems. What does that mean for cyber security?

Background

In March 2020, governments worldwide imposed curfews and rules on reducing physical social contact in order to stem the spread of the corona virus. Wherever possible, employers allowed their employees to work from home, where, more and more, private IT devices are being used for official business. This larger IT surface is often less well protected than IT devices used at work. New programs, e.g. for conference calls and video conferences, are being introduced under time pressure, in most cases without adequate security checks. Also, there are more and more reports about cyber attacks on health-care organizations on whose proper functioning governments and societies are more dependent now than ever. What is the impact of the COVID-19 pandemic on cyber security, cyber crime and state-sponsored cyber activities?[1] How can governments reduce cyber threats and address them?

Increased internet use and working from home heighten digital security risks

COVID-19 leads to record-breaking internet use

Digital information channels, social media, streaming and cloud services, e-mails, conference calls and video conferencing tools are being used more than ever.[2] This is reflected by internet usage statistics: in mid-March, Frankfurt-based internet exchange DE-CIX, at which the data flows of various internet service providers converge and which is the world's biggest based on data traffic, reported a peak data traffic of 9,1 Terabit (TBit) per second.[3] This is roughly equivalent to the data volume of 1.800 downloaded HD films. This record level is the biggest jump in data traffic from the previous peak of 8,3 TBit that the company has ever recorded. Originally, it had expected this new peak to occur at the end of the year, based on increasing internet use and seasonal fluctuations. Generally speaking, a more intense use of the internet and an increasing number of new, i.e. inexperienced, users create more opportunities for the activities of criminal and malicious actors.

In addition, the less well-protected IT surface has become larger, driven by millions of people told to work from home on short notice. In big companies, government agencies

Unsafe IT

and organizations, IT systems usually enjoy institutionalized protection. In these cases, ideally, IT security standards including adequate actions are implemented, software vulnerabilities are regularly fixed by installing manufacturer updates and the internal network is protected. Private IT devices are often less safe. Home networks are usually less well-secured. Privately used computers often lack professional antivirus protection programs or firewalls. Also, private devices can run software that has serious security gaps or whose security gaps were not fixed by the installation of a manufacturer update. In some cases, software is used that has simply reached the end of its life cycle, which means it will no longer be eligible for security-relevant updates. The operating system *Windows 7* is a case in point. Microsoft stopped supporting this system in early 2020, but it is still being used by millions – it is still running, for example, on 8.000 computers used by the Hamburg police department.[4] At the same time, by rushing to allow people to work from home, organizations or institutions are setting up more and more interfaces enabling remote access to their internal networks. This makes it harder for the IT experts of these organizations or institutions to identify unauthorized network connections and offers hackers a chance to gain access to internal networks. By the same token, work computers that may contain sensitive data are sometimes used for private purposes when working from home, which can also open the door to hackers. All this drives up the number of security risks.

Cyber crime thrives on curiosity and people's need for information

People – the weakest link

An additional crucial factor is the unprecedented situation: just like other special situations – for example, the introduction of the European *General Data Protection Regulation (GDPR)* in 2018 – the COVID-19 pandemic offers an opportunity to deliberately exploit people's sense of insecurity, curiosity and their need for information for criminal or malicious activities.[5] When someone's personal health is involved, the need for information can be easily aroused – especially, when the issues at stake are protective measures, alleged treatment methods, vaccination or supposed information from government sources. In this way, internet users lose their suspicion and fall prey to scams or malware. This targeted manipulation of people is also known as "social engineering" – "human hacking". Cyber criminals benefit from an exceptional situation and try to exploit it by adapting their activities in order to turn a profit. Sending out huge numbers of so-called "phishing mails" is a popular method.[6] By using forged emails and providing a fake pretext, made to look as credible as possible, internet users are persuaded to enter passwords or other sensitive data or to open an email attachment infected with malware. Criminal phishing campaigns related to the corona virus are supposed to have risen "dramatically" since January 2020, according to the information security company Fireeye.[7]

Fraudulent enrichment

In early April 2020, the Federal Office for Information Security (*BSI*), which is responsible for IT security in Germany, warned of an "increasing number of corona virus-related cyber attacks on businesses and citizens".[8] In the same month, the Ministry of Economic Affairs of the State of Northrhine-Westphalia stopped paying out emergency aid to self-employed recipients and businesses, after the state criminal office had sounded a warning against fake websites, on which criminals had tried to collect data via the required application forms, using these data to file fraudulent emergency aid claims themselves.[9] In mid-March, the Consumer Center Northrhine-Westphalia drew attention to a professional phishing campaign. Using authentic-looking emails, cyber criminals masquerade as banks and deliberately appeal to people's emotions, telling them that at a time of bank branch closures, communication needs to be maintained, in order to lure them into entering sensitive customer data into an authentic-looking website.[10] These digital identity data, such as e-mail addresses, mailing addresses or

dates of birth, are subsequently used for financial enrichment. There are also reports about websites and an Android App that promise users to provide them with realtime information on the spread of the virus, along the lines of the popular map developed by the Johns Hopkins University, but infect them with malware instead.[11]

Health-care as an essential sector in a pandemic

Currently, IT security experts are raising the alarm on an increase of cyber attacks on health-care organizations and institutions.[12] When launching a cyber attack on hospitals, criminals are primarily interested in obtaining demographic and financial information, in order to make money with digital identity data.[13] In this process, hospital IT systems can be deliberately or inadvertently compromised. On March 13, Czechia's second biggest hospital, the university clinic of Brno, became the target of an unspecified cyber attack from a source unknown until today.[14] The hospital, which also has responsibility for carrying out Corona tests, had to shut down parts of its IT system and postpone planned operations. The clinic was able, however, to guarantee basic operations. There was no negative impact on its work to fight the new virus.

Health-care sector under double pressure

In addition, hospitals and other health-care sector facilities can become the target of so-called "ransomware". Criminals use such malware to encrypt the stored data of their victims in order to blackmail them afterwards. The vague promise: the data will be decrypted in return for a ransom payment. In London, for example, a laboratory that was ready to test a potential vaccine against the corona virus, became the victim of a ransomware attack carried out by an established group of cyber criminals.[15] While the company was able to protect its IT systems successfully, the attackers managed to skim patient records which they published on the internet. Moreover, in late March, the Computer-Emergency-Response-Team (CERT-FR) of the French government warned its local authorities against a ransomware campaign.[16]

From espionage to sabotage: COVID-19 and state-sponsored hackers

Apart from criminals, state actors, trying to operate covertly in cyber space in order to evade political responsibility, are exploiting the exceptional situation by using targeted phishing emails – so-called "spear phishing" – for espionage purposes. Groups of hackers that are believed to be sponsored by Russia, China and North Corea are using personalized emails containing references to the pandemic in order to infect their targets with malware or pick off passwords.[17] In the COVID-19 pandemic, which illustrates again that national security should not only deal with traditional military threats, the collection of online information by intelligence services, the so-called *Signals Intelligence* (*SIGINT*), is shifting its focus to new targets. Classical *SIGINT* targets are political and military institutions that could, for example, provide information on the political decision-making processes or military capabilities of a country.[18] Apart from counterintelligence, i.e. protection against the activities of other intelligence services, industrial espionage is another important field of operation of intelligence services on the internet.

"Knowledge is Power"

At this time, governments are keenly interested in obtaining information on the spread of the corona virus, different national policies for containing the virus and potential drugs as well as vaccines. This information can provide key strategic benefits for fighting the pandemic. Consequently, especially institutions and organizations of the health-care sector, pharmaceutics and biotechnology, government agencies in these sectors as well as logistics infrastructures are moving into the crosshairs of intelligence services.[19] So it does not come as a surprise that, in March 2020, staff members of the World Health Organization (WHO), for example, were

the target of spear-phishing emails, that are believed to have originated in Iran.[20] In mid-May, the US American Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) together warned against groups of hackers linked to China and "non-traditional collectors".[21] Their job is to collect digital intelligence on US institutions that do research on the corona virus. The objective is to identify and gain intellectual property as well as public health data related to vaccinations, treatments and corona tests. Allegedly, they were partially successful in penetrating these institutions' networks. Two groups that are also believed to be connected to China are suspected to have sent emails with attached documents containing genuine health information to targets in Vietnam, Mongolia and the Philippines in order to infect them with spyware. A Russian group operating against Ukrainian targets is believed to be using similar methods.[22]

New communication channels are vulnerable to espionage and industrial espionage

A paradise for spies

As physical meetings cannot be held at the present time, businesses, governments and public authorities often resort to conference call and video conferencing programs at short notice, depending on availability and user friendliness. It is possible, however, that these programs are unsafe or that the manufacturer is dubious or has been infiltrated by intelligence services. In the past, these communication channels were an attractive target for intelligence services, as illustrated by the Swiss Crypto AG case.[23] Governments and public authorities usually have secure communication channels. In a scenario like the current COVID-19 pandemic, in which many members of government and government officials are working at physically separate locations, there are often not enough secure communication lines.

This is illustrated by the fact that the British government, for example, used the video conferencing tool Zoom, developed by the eponymous US company, for a digital "cabinet meeting". The company that has 700 employees in China working in research and development saw the number of its users skyrocket from 10 million per day in December 2019 to more than 200 million per day in March 2020.[24] Zoom promoted its product by claiming that the service has end-to-end encryption, which means that only the individuals involved in the communication can read the shared information. Due to inadequate data protection standards and poor encryption of transmitted conversations, the company came under public criticism in early April, 2020.[25] Zoom immediately reacted to these grievances by implementing actions to boost transparency and data protection and provide first software updates and by presenting a comprehensive plan on how data protection and program security could be improved in the future, including by the planned implementation of real end-to-end encryption.[26]

As a result, intelligence services can use the COVID-19 pandemic to skim sensitive communication that is increasingly happening online right now. According to a report, the German Ministry of Foreign Affairs (AA) prohibited the use of Zoom by its staff on mobile devices after an internal security check.[27] Since many partners of the Ministry use the program, a total ban was not possible, the report stated. There was, however, no uniform rule on using the service within the federal government, apparently.

Cyber sabotage

Even indirect impacts of cyber attacks can cause considerable damage.

Apart from espionage, states can also use cyber operations for the purpose of sabotage in times of peace, i.e. corrupting software and operating processes in order to weaken an economic or political system.[28] In this way, the state doing the sabotage expects to profit from influencing a given situation.[29] In an existing crisis like a pandemic, such cyber attacks, e.g. on the IT systems of critical infrastructures, can be an additional aggravation in an already tense situation. In 2017, the example of *NotPetya* showed that cyber attacks can have far-reaching consequences even without causing direct physical damage, by having a negative impact on the functionality of computers: the Russian malware irreversibly encrypted essential data for running Windows computers, thereby rendering these computers useless.[30] The Ukraine was the main target of this operation, whose total damage was estimated at ten billion US dollars by the US administration. In mid-April, the Czech National Cyber and Information Security Agency (NUKIB) warned its allies of an imminent wave of cyber attacks on hospitals and critical infrastructures of the country, planned by a "serious" and technically sophisticated attacker.[31] The objective, again, was to disable Windows computers. The next day, the IT systems of two Czech hospitals became the targets of unspecified cyber attacks from an unknown source.[32] Both, however, were successfully thwarted.

How do we deal with cyber crime, cyber espionage and cyber sabotage?

Differentiation between crime and state-sponsored activities is helpful.

The COVID-19 pandemic highlights existing cyber threats and security gaps. Just like in the "real" world, there is no 100 per cent security in the cyber domain. Dangers can only be reduced to an acceptable level by implementing a set of actions. When dealing with cyber threats, it is helpful to distinguish between the activities of criminal actors, who are mostly driven by a motive of personal enrichment, and state-sponsored actors who try to gain strategic advantages in times of peace by launching cyber operations.

Education, prevention, digital literacy & financial support

Generally speaking, we should expect the significance of cyber crime to keep increasing due to the advance of digitalization. Corona virus-related scams and developments resulting from them will remain at a high level as long as the virus dominates the headlines. Cyber criminals will adapt their activities, depending on how the pandemic develops. It is only through the joint efforts of the population, businesses and organizations that this threat can be reduced to an acceptable level. Since social engineering focuses on the human element, education and prevention work, as done by the BSI, the Federal Criminal Police Office (BKA) or the police departments of the federal states, need to be strengthened.[33] Large-scale awareness-raising campaigns that highlight the dangers posed by phishing mails could be an adequate measure, just as an expansion of digital literacy programs in schools, universities and in adult education. Small and medium-size companies (SMEs) that often do not have sufficient resources need to be financially supported based on clear criteria so that they can better protect their IT systems and train their staff.

As far as law enforcement agencies are concerned, their capacities and expertise for preventing and investigating cyber crime should be expanded. Just as in the ministries and federal agencies, in which one in four of the 2.800 IT-security jobs are vacant, there is often a lack of adequately trained staff.[34] This challenge needs to be addressed by a targeted program for training IT experts. A good example is the introduction of in-service training for skilled staff who are developed to become cyber crime investigators at the Federal Criminal Police Office BKA or the establishment, in the state of Hesse, of an academic program called "cyber crime investigation" in order to provide specialized training for police officers.[35]

Identification of new facilities requiring protection & evaluation of existing safeguards

In order to protect critical infrastructures (CI), such as power plants, essential government and administration structures or hospitals, the European Union (EU) adopted the *Network and Information Security* directive in 2016.[36] Based on this directive, member states required the operators of "essential services" to introduce and comply with organizational and technical security standards, among other things, to boost the security of IT systems.[37] The current COVID-19 pandemic illustrates which organizations and institutions are really critical in a crisis. As hospitals are relatively soft targets and often have to cut costs in order to stay within budgets, which is reflected by outdated and unsafe IT systems, it is probably a good idea to make more funding available to them for better protecting their IT systems. COVID-19 could also serve as a trigger to identify new organizations that require protection or to evaluate existing safeguards.

Maintaining secure communication channels for governments and public authorities is essential.

With regard to state-sponsored cyber activities, it is to be expected that *SIGINT* activities carried out by intelligence services will increasingly focus on health issues and will become more widespread.[38] As a general principle, whenever communication programs or programs for data sharing are used, the question of whether and to what extent the information concerned requires protection needs to be reviewed. Using Zoom for talking to friends, for example, is not a problem, but using it in its current version for sharing highly sensitive business secrets or for holding cabinet meetings is a risk. Therefore, the pandemic highlights the need for maintaining secure and reliable communication channels for confidential information and for extending it to most employees – especially those working for governments and public authorities. Similar to the *5G* issue, which has triggered a vivid debate about the pros and cons of involving Chinese companies in building up the new mobile communication standard, there should be a fundamental and comprehensive political discussion on weighing potential security risks in using information and communication technologies in sensitive areas. Because, in terms of security risks, it should not be forgotten that a state actor, who can influence established software and hardware, can change his intentions at any time in a crisis.

Preventing the risk of escalation

There should be a discussion about the potential risks of the gathering of information getting out of control and about the role that increasingly aggressive intelligence services play in the future behaviour of states in the cyber domain, in order to prevent an escalation of state-sponsored interaction in this domain.[39] Governments should not respond to acts of cyber espionage or cyber sabotage by penetrating the opponent's networks or neutral IT systems. Depending on the context, so-called measures of active cyber defence are rarely effective in continuing scenarios: often, they can no longer stop the objectives of an ongoing attack being achieved – e.g. theft of data that can easily be copied – and pose the risk of collateral damage as well as of inadvertent escalation.[40] Rather, the few existing IT experts should primarily be deployed to handle defensive tasks such as the protection of IT systems.

Sanctions, legal charges and further juridification

At the political-strategic level, governments should respond to cyber incidents launched by another state by imposing political and economic sanctions or bringing legal charges to isolate and stigmatize the aggressor, in order to achieve a change of behaviour in the long term.[41] A conceptual framework such as the *Cyber-Diplomacy-Toolbox*, adopted by the EU for these purposes in 2017, can provide guidance for a country's response and can send a message to other countries as to what constitutes non-acceptable behaviour.[42] In the long run, the COVID-19 pandemic which has clearly shown that a functioning health-care sector is equally relevant for all countries, could be the opportunity for reviving the process of juridification and setting of standards with regard to the use of information and communication technology (ICT) by states at the level of the United Nations, which was stalled in 2017.[43] To this end, German and European cyber diplomacy should develop an understanding with like-minded countries about

non-accepted state behaviour when using ICT. On this basis, a dialogue should be held with non-like-minded countries about red lines and the handling of state-sponsored cyber attacks.

1 In essence, cyber security is based on the confidentiality, integrity and availability of data (it used to be called IT security). As ICT permeates almost all areas of society, the term "cyber security" has acquired a social, legal, political, military, economic and cultural dimension on top of its technical one. Cyber security can also denote a condition, i.e. the absence or reduction of threats to an acceptable level. Here, the reference object is the cyber domain, i.e. the internet as the technical medium, IT devices connected and not connected to it as well as the social dimension that results from the use of these technologies (see: Sven Herpig: Anti-War and the Cyber Triangle. Strategic Implications of Cyber Operations and Cyber Security for the State, Hull: University of Hull 2016, S. 37). Simply put, cyber security policy or cyber defence policy – if operations come under the remit of the military – deal with defensive and offensive actions to protect the cyber domain.

2 See Ella Koeze/Nathaniel Popper: The Virus Changed the Way We Internet, in: The New York Times 07.04.20, retrieved from: https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html?action=click&module=Editors%20Picks&pgtype=Homepage; Statista: Media consumption increase due to the coronavirus worldwide 2020, by country, retrieved from: https://www.statista.com/statistics/1106766/media-consumption-growth-coronavirus-worldwide-by-country/.

3 DE CIX: Highest jump ever: DE-CIX Frankfurt reaches 9.1 Tbps, 11.03.20, retrieved from: https://www.de-cix.net/de/news-events/news/de-cix-frankfurt-reaches-9-1-tbps.

4 See Ed Bott: It's 2020: How many PCs are still running Windows 7, in: zdnet.com 07.01.20, retrieved from: https://www.zdnet.com/article/how-many-pcs-are-still-running-windows-7-today/; Gabi Probst: Den digitalen Anschluss verpasst, in tagesschau.de 16.04.2020, retrieved from: https://www.tagesschau.de/investigativ/kontraste/kriminaltechnik-bundesrepublik-101.html.

5 Danny Palmer: Phishing alert: GDPR-themed scam wants you to hand over passwords, credit card details, in: zdnet.com 03.05.18, retrieved from: https://www.zdnet.com/article/phishing-alert-gdpr-themed-scam-wants-you-to-hand-over-passwords-credit-card-details/.

6 Bundeskriminalamt: Cybercrime. Bundeslagebild 2018, Stand Oktober 2019, S. 17, retrieved from: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.pdf?__blob=publicationFile&v=3; Symatec: Internet Security Threat Report, Volume 24, February 2019, S. 21 ff.; retrieved from: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

7 Patrick Howell O'Neill: Chinese hackers and others are exploiting coronavirus fears for cyber espionage, in: MIT Technology Review 12.03.20, retrieved from: https://www.technologyreview.com/2020/03/12/916670/chinese-hackers-and-others-are-exploiting-coronavirus-fears-for-cyberespionage/.

8 Bundesamt für Sicherheit in der Informationstechnik: Cyber-Kriminelle nutzen Corona-Krise vermehrt aus 02.04.20, retrieved from: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Cyber-Kriminell_02042020.html.

9 FAZ.net: NRW stoppt Auszahlung von Soforthilfen, 09.04.20, retrieved from: https://www.faz.net/aktuell/wirtschaft/nrw-stoppt-auszahlung-von-soforthilfen-wegen-betrugsverdacht-16718743.html.

10 Verbraucherzentrale Nordrhein-Westfalen: Achtung, Phishing! Wie Betrüger die Corona-Krise in E-Mails nutzen 18.03.20, retrieved from: https://www.verbraucherzentrale.nrw/aktuelle-meldungen/digitale-welt/achtung-phishing-wie-betrueger-die-coronakrise-in-emails-nutzen-45714.

11 Dan Goodin: The Internet is drowning in COVID-19-related malware and phishing scams, in arstechnica.com 16.03.20, retrieved from: https://arstechnica.com/information-technology/2020/03/the-internet-is-drowning-in-covid-19-related-malware-and-phishing-scams/; World Economic Forum: Hackers are using coronavirus maps to spread malware 14.03.20, retrieved from: https://www.weforum.org/agenda/2020/03/hackers-are-using-coronavirus-maps-to-spread-malware?fbclid=IwAR1OSDE-Yf__vchx1qcUONrJZeYz23LhMpUZEaxOSuxTfo-3MaC0efjBW1Sg.

12 See Matt Burgess: Hackers are targeting hospitals crippled by coronavirus, in: wired.co.uk 22.03.20, retrieved from: https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing.

13 Caroline Brooks/Xuefeng Jiang: Here's the Kind Of Data Hackers Get About You From Hospitals, in: Michigan State University 23.09.19, retrieved from: https://msutoday.msu.edu/news/2019/heres-the-kind-of-data-hackers-get-about-you-from-hospitals/.

14 Sean Lyngaas: Czech Republic's second-biggest hospital is hit by cyberattack, in: cyberscoop.com 13.03.20, retrieved from: https://www.cyberscoop.com/czech-hospital-cyberattack-coronavirus/.

15 Davey Winder: COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online, in forbes.com 23.03.20, retrieved from: https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#ad64a7618e55.

16 Computer Emergency Response Team France: Rapport Menaces et Incidents du CERT-FR. Attacks involving the Mespinoza/Pysa ransomware 01.04.20, retrieved from: https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-003/.

17 Catalin Cimpanu: State-sponsored hackers are now using corovirus lures to infect their targets, in zdnet.com 13.03.20, retrieved from: https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/; Shannon Vavra: Cybercriminals, nation-states increasingly tailoring coronavirus spearphishing campaings, in cyberscoop.com 12.03.20, retrieved from: https://www.cyberscoop.com/coronavirus-phishing-scams-iran-china/.

18 Ben Buchanan: The Cybersecurity Dilemma. Hacking, Trust, and Fear Between Nations, Oxford: Oxford University Press 2017, S. 89-96.

19 Sandra Joyce: Limited Shifts in the Cyber Threat Landscape Driven by COVID-19, in: Fireeye.com 08.04.20, retrieved from: https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html.

20 Joseph Menn/Christopher Bing/Raphael Satter/Jack Stubbs: Exclusive: Hackers linked to iran target WHO staff emails during coronavirus – sources, in reuters.com 02.03.20, retrieved from: https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC.

21 Federal Bureau of Investigation/Cybersecurity and Infrastructure Security Agency: People's Republic of China (PRC) Targeting of COVID-19 Research Organizations 13.05.20, retrieved from: https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.pdf.

22 Patrick Howell O'Neill: Chinese hackers and others are exploiting coronavirus fears for cyber espionage.

23 Elmar Theveßen/Peter F. Müller/Ulrich Stoll: #Cryptoleaks: Wie BND und CIA alle täuschten, in: zdf.de 11.02.20, retrieved from: https://www.zdf.de/nachrichten/politik/cryptoleaks-bnd-cia-operation-rubikon-100.html.

24 Kalila Sangster: Zoom users surge from 10m to 200m as world works from home, in: yahoo Finance UK 02.04.20, retrieved from: https://uk.finance.yahoo.com/news/zoom-users-surge-from-10-m-to-200-m-as-world-works-from-home-110022110.html.

25 Bill Marczak/John Scott-Railton: Move Fast and Roll Your Own Crypto. A Quick Look at the Confidentiality of Zoom Meetings, in: citizenlab.ca 03.04.20, retrieved from: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/; Micah Lee/Yael Grauer: Zoom Meetings Aren't End-To-End Encrypted, Despite Misleading Marketing, in: theintercept.com 31.03.20, retrieved from: https://theintercept.com/2020/03/31/zoom-meeting-encryption/.

26 (Eric S. Yuan: A Message to Our Users 01.04.20, online: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/). In mid-April 2020, Zoom announced the use of a higher encryption standard that came with the version "5.0". Also, Zoom introduced an option for its business customers that enables them to select the location of servers that are used for a conversation so that encryption and decryption keys of conversations without a Chinese participant are no longer supposed to be transmitted by Chinese servers, as had happened before in some cases. (Colleen Rodriguez: Zoom Hits Milestone on 90-Day Security Plan, Releases Zoom 5.0 22.04.20, online: https://blog.zoom.us/wordpress/2020/04/22/zoom-hits-milestone-on-90-day-security-plan-releases-zoom-5-0/). The keys, however, are still generated by Zoom servers, which, theoretically, gives the company access to content and which could force it to surrender the keys if required to do so by a lawful information request from security agencies. Due to its business footprint in China and in view of the legal situation in the country, the company could be required to cooperate with the authorities. Zoom is still working on genuine end-to-end encryption, which it plans to offer in a paid version in the future. The company is involving civil society, cryptographics experts and its customers in this process (Eric S. Yuan: Zoom Acquires Keybase and Announces Goal of Developing the Most Broadly Used Enterprise End-to-End Encryption Offering 07.05.20, retrieved from: https://blog.zoom.us/wordpress/2020/05/07/zoom-acquires-keybase-and-announces-goal-of-developing-the-most-broadly-used-enterprise-end-to-end-encryption-offering/).

27 Reuters.com: German foreign ministry restricts use of Zoom over security concerns 08.04.20, retrieved from: https://www.reuters.com/article/us-health-coronavirus-germany-zoom/german-foreign-ministry-restricts-use-of-zoom-over-security-concerns-report-idUSKBN21Q1SC.

28 Thomas Rid: Cyber War Will Not Take Place, in: Journal of Strategic Studies 1 (2012), S. 5-32.

29 Ben Buchanan: The Hacker And The State, Harvard: Harvard University Press 2020, S. 8.

30 Andy Greenberg: The Untold Story of NotPetya, The Most Devasting Cyberattack in History, in: Wired 22.08.18, retrieved from: https://www.wired.com/story/notpetya-cyberattack-ukraine- russia-code-crashed-the-world/.

31 Jason Hovet/Christopher Bing/Jack Stubbs: Czechs warn of imminent, large-scale cyberattacks on hospitals, in: http://reuters.com 17.04.20, retrieved from: https://uk.reuters.com/article/uk-czech-cyber/czechs-warn-of-imminent-large-scale-cyberattacks-on-hospitals-idUKKBN21Z00N.

32 Reuters.com: Czech hospitals report cyberattacks day after national watchdog's warning 17.04.20, retrieved from: https://www.reuters.com/article/us-czech-cyber-ostrava/czech-hospitals-report-cyberattacks-day-after-national-watchdogs-warning-idUSKBN21Z1OH?__twitter_impression=true.

33 See Bundesamt für Sicherheit in der Informationstechnik: Social Engineering – der Mensch als Schwachstelle o. A., retrieved from: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering_node.html; Bundeskriminalamt: Forschungs- und Beratungsstelle Cybercrime o. A., retrieved from: https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsUndBeratungsstellen/Cybercrime/Cybercrime.html.

34 Dominik Rzepka: Jede vierte Stelle für IT-Sicherheit unbesetzt, in zdf.de 12.02.20, retrieved from: https://amp.zdf.de/nachrichten/politik/cyberabwehr-bundesregierung-it-sicherheit-stellen-unbesetzt-100.html?__twitter_impression=true.

35 Bundesministeriums des Innern, für Bau und Heimat: Verstärkung im Kampf gegen die Cyberkriminalität 02.10.19, retrieved from: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/10/aenderung-krimLV-cyber-krim.html; FAZ.net: Polizei bildet Spezialisten aus 19.04.20, retrieved from: https://www.faz.net/aktuell/rhein-main/cyberkriminalitaet-polizei-bildet-spezialisten-aus-16731824.html.

36 2016/1148/EU: Directive of the European parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, in: Official Journal of the European Union L194, 19.07.16, S. 1-30, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=NL.

37 In Germany, the BSI is responsible for the implementation and observance of the so-called NIS directive (see Bundesamt für Sicherheit in der Informationstechnik: Gesetz zur Umsetzung der NIS-Richtlinie o. A., retrieved from: https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html).

38 Glenn S. Gerstell/Michael Morell: Four ways U.S. intelligence efforts should change in the wake of the coronavirus pandemic, in: washingtonpost.com 07.04.20, retrieved from: https://www.washingtonpost.com/opinions/2020/04/07/four-ways-us-intelligence-efforts-should-change-wake-coronavirus-pandemic/.

39 See Alexandra Paulus/Sven Herpig: Covid-19: Why states now need to consider self-restraint in the cyber domain, in: aboutintel.eu o. A., retrieved from: https://aboutintel.eu/covid-cyber-china/.

40 See Sven Herpig: Zurückhacken ist keine Lösung, in: Zeit.de 21.04.17, retrieved from: https://www.zeit.de/digital/internet/2017-04/cyberangriffe-bundesregierung-hackback-gegenangriff/komplettansicht.

41 An example of "naming and shaming" is the arrest warrant issued by the Federal Prosecutor's Office against an agent of the Russian military intelligence service GRU, which is suspected of having been involved in the hacking of the German Parliament's network in 2015 and which had already been indicted by a US court for its involvement in the so-called DC hack as early as 2018. Germany is only the second country, after the US, that has filed charges against the member of a state-organized cyber unit (Florian Flade/Georg Mascolo: Bärenjagd, in: SZ.de 05.05.20, retrieved from: https://www.sueddeutsche.de/politik/hack-bundestag-angriff-russland-1.4891668).

42 Rat der Europäischen Union: Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, 13007/17, Brussels, 9 October 2017, retrieved from: http://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf.

43 See Kubo Mačák/Laurent Gisel/Tilman Rodenhäuser: Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?, in: justsecurity.org 27.03.20, retrieved from: https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/.

Last retrieval of the above Internet links: 29/05/2020.

Imprint

The Author

Johannes Wiggen is desk officer for cyber security in the department International Politics and Security at the Konrad-Adenauer-Stiftung e.V.

Konrad-Adenauer-Stiftung e. V.

Johannes Wiggen
Desk Officer for Cyber Security
Analysis and Consulting
T: +49 30 / 26 996-3934
johannes.wiggen@kas.de

Postal address: Konrad-Adenauer-Stiftung e. V., 10907 Berlin

Publisher: Konrad-Adenauer-Stiftung e. V., 2020, Berlin
Design and typesetting: yellow too, Pasiek Horntrich GbR / Janine Höhle,
Konrad-Adenauer-Stiftung e. V.

ISBN 978-3-95721-682-3