NO LOCKDOWN IN CYBERSPACE. STATE-SPONSORED CYBERATTACKS DURING THE FIRST YEAR OF THE COVID-19 PANDEMIC

Claudiu Mihai CODREANU, PhD Student
National University of Political Studies and Public Administration
Bucharest/Romania

Abstract
The uptick in malicious activity in cyberspace observed during the initial stage of the coronavirus pandemic highlighted once again the need for addressing cyberattacks. Health-related facilities were some of the main targets of cyber operations, several cyberattacks hitting even COVID-19 hospitals. Cyber operations grew in both intensity and numbers, both regarding cyberattacks and cybercrime. However, alleged state-sponsored cyberattacks are the main focus of this research. Malicious cyber operations set dangerous precedents during the pandemic, and it strengthens the need to adequately address these threats, but also broaden the research, especially in the field of International Relations. The discussion is centred on the most significant cyber incidents during the first year of the COVID-19 pandemic, beginning with the surge of cyberattacks and cybercrime during the first months of increased dependence on digital technologies for companies and state institutions. Therefore, this paper will start with a literature review regarding cyber operations and IR. Research on cyberspace in IR is not scarce, but it is still lagging behind new and dynamic evolutions. Further, I shall focus on the major state-sponsored cyber operations that occurred during this period, while also paying attention to the problem of attribution. All of these developments regarding cyber operations should stand as significant threats and warnings for governments, private companies, and citizens, and they must be addressed properly in order to prevent future

considerable disruptions. Given the above, I shall summarise several general lessons and recommendations that emerged from studying the major state-sponsored cyberattacks during the COVID-19 pandemic.

Keywords
COVID-19 pandemic; cyber operations; cybersecurity; state-sponsored cyberattacks.

1. INTRODUCTION

The SARS-CoV-2 virus which is causing the COVID-19 disease was first identified in China around December 2019, spreading then to the rest of the world. The World Health Organisation (WHO) eventually declared COVID-19 a pandemic in March 2020. The first two months of the pandemic saw thousands of daily deaths in Europe and North America, especially in countries such as Italy, Spain, the UK, France and the US. During March, most of the world's governments imposed national or regional lockdowns to limit the spread of the virus, which meant that a large portion of employees started working from home and a large part of students began studying from home, mostly by using digital and online means. As of April 22, 2021, more than 143 million cases have been officially reported globally, while more than 3 million deaths have been confirmed to be caused by COVID-19 (WHO 2021).

The COVID-19 pandemic caused significant disruption all over the world and pushed health systems to their limits, especially in the first few months when uncertainty was prevalent. As if the virus did not have a sufficient large impact, the healthcare sector started to become a target of cyber operations and even cyberattacks, both direct and collateral. Malicious actors started deploying series of ransomware attacks and phishing campaigns trying to exploit the pandemic (ENISA 2020). In addition to this, state actors started cyber espionage campaigns in an attempt to learn more about countries' management of the pandemic and of the research regarding the virus or about the development of vaccines (Walker 2020; Stubbs 2020; Strohm, Gallagher 2020; Sabbagh, Roth 2020).

Moreover, besides cyber operations targeting health-related facilities that occurred in Czechia, Germany, the UK and the US among others (Reuters 2020; ENISA 2020; Cimpanu 2020a; Burgess 2020a; Stein, Jacobs 2020; Sabbagh, Roth 2020), cyberattacks targeted electrical grid operators and water treatment facilities, as in the case of the cyberattacks on water supply infrastructure in Israel and the United States and attacks on the US electrical grid (Staff 2020; Marquardt, Levenson 2021; Martin, Freitas Jr. 2020). Furthermore, cybercrime increased significantly both in numbers and intensity and targeted private companies, state institutions and individuals, and state-sponsored cyberattacks and cyber espionage campaigns escalated in the context of the public health crisis provoked by the pandemic. Cyber operations such as the SolarWinds and Microsoft Exchange hacks, even though they had the aim of espionage, represented a serious escalation because of their impact, complexity and magnitude (Willet 2021; Sanger, Barnes, Perlroth 2021a; Greenberg 2021). In this context, the EU, and later the US, imposed sanctions on Russia for several cyber operations, while other cyberattacks were publicly attributed to China (Consilium 2020a; Consilium 2020b; Greenberg 2021).

The main aim of this research is studying the impact that cyber operations had during the first year of the COVID-19 pandemic, mainly the period between March 2020 (when the COVID-19 was declared as a pandemic by the WHO) and March 2021, focusing on major state-sponsored cyber operations targeting other state actors. During this study, I followed major cyber operations that have affected states, organisations, companies and the population at large, dividing them in cyberattacks, cyber espionage campaigns and cybercrimes. Furthermore, states' and organisations' reactions and responses to these cyber operations have also been taken into consideration, noting the seriousness of the developments occurring in this period. Thus, this paper begins with the introduction of several theories and concepts regarding cyber operations, cybercrime and malware, taking into consideration states' role in cyberspace and the issue of public attribution. Afterwards, I study the main cyber operations that occurred during the coronavirus pandemic, highlighting state-sponsored cyberattacks and cyber espionage campaigns against other state actors, but also taking into account the surge of cybercrime and the particular

cases of cyber operations against COVID-19-related health and research facilities. In the end, I analyse the impact and importance of these cyber operations and try to identify several lessons learned and put forward a number of recommendations, as cyber incidents must continue to be addressed properly because they might have serious effects if left unchecked. In order to assess the impact of the cyber operations included in this study, I highlight whether the cyber campaigns were publicly attributed by the affected states to other state actors, subject of international sanctions, considered as serious incidents by affected governments or by related research, and whether they affected key infrastructures (e.g., cyberattacks against COVID-19 related health facilities and research, water supply networks or electrical grid operators). Moreover, I take into account the fact that these cyber operations created disruptions during an already ongoing global disruption, namely the COVID-19 pandemic, and hence some cyber operations occurred because of the pandemic and others might have occurred by exploiting the issues created by the pandemic. In addition to this, the research differentiates between cyberattacks, cyber espionage campaigns and cybercrime.

The SolarWinds cyber operation, the Microsoft Exchange hack, the Israel-Iran cyberattack exchange, cyberattacks on health facilities during March-April 2020 or the cyber espionage campaigns regarding COVID-19 research were all state-sponsored cyber operations (Willet 2021; Sanger, Barnes, Perlroth 2021a; Baram, Lim 2020; Reuters 2020; Cimpanu 2020a; Sabbagh, Roth 2020; Strohm, Gallagher 2020). However, cybercrime also increased during this period (Wiggen 2020; Matthews 2020; Jolly 2020), most of it having being done by non-state actors (cybercriminal groups). The focus was put on state-sponsored cyber operations, but the research also includes references to the increase in cybercrime, in order to encompass the whole picture of cyber incidents occurring during this period. Thus, the research focuses on major state-sponsored cyber operations that occurred during the first year of the pandemic, including the Russian SolarWinds cyber operation targeting the US, the Chinese Microsoft Exchange hack targeting the US, the Israel-Iran cyberattack exchange, state-sponsored cyberattacks against COVID-19 related health facilities in Europe and the US, and state-sponsored cyber espionage campaigns regarding COVID-19 research.

2. CYBER OPERATIONS. FROM CYBERCRIME TO STATE-SPONSORED CYBERATTACKS

2.1. Cyberspace and cyberattacks

Over the last two decades, and even more in the last few years, governments, citizens and companies alike have increased their dependence on information technology. This, alongside with the expanding interconnectedness of critical infrastructures, has led to new and significant vulnerabilities, risks and threats. Cyber incidents, provoked by various actors or even by accident, have the ability to cause significant disturbances in the provision of key public services. (Boeke 2017, 449-450)

Cyber operations allow actors to target a country, individual or organization covertly, as attribution is sometimes difficult to be done. Cyberattacks have become more and more frequent and their potential of triggering serious disruption is growing. The 2020 World Economic Forum Global Risk Report named cyberattacks in the top 10 risks in terms of likelihood and impact. (Baram, Lim 2020)

All of the developments discussed in this paper are related to cyberspace, which can be briefly be defined as a "physical, social-technological environment" encompassing "the network system of microprocessors, mainframes and basic computers that interact in digital space" (Valeriano and Maness 2015, 24). Closely related, a malicious activity regarding cyberspace, or a cyberattack, can be defined as an attack targeting a network, computer system, digital device or an individual or organisation which aims "to disrupt, steal or corrupt assets" which can be digital assets, digital services or physical assets that have a cyber component (Hodges and Creese 2015, 34). Another definition of cyberattacks has been provided by the *Tallinn Manual 2.0*, in which a cyberattack is determined as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Schmitt 2017, 415). Furthermore, Brandon Valeriano and Ryan Maness argue that cyber conflict should be used to describe the usage of digital or computational technologies in cyberspace "for malevolent and/or destructive purposes in

order to impact, change, or modify diplomatic and military interactions between entities" (2015, 32). Since the 2000s, the focus changed from cyberwar and apocalyptic cyber scenarios to the concept of cyber conflicts, which are seen as a regular element of political conflicts, and hence targeted cyberattacks became the highlight of research (Dunn Cavelty and Egloff 2019, 44).

Even though the private companies and individuals have become more important actors in cyberspace, the state still maintains an essential role in cyberspace, especially in matters of cybersecurity. States act as the owners of networks, cybersecurity providers for state institutions and critical infrastructure, legislators in cyberspace and partners for private companies that operate critical infrastructure. Furthermore, intelligence services play a crucial role both in cyber offense and defence, as they look for and exploit vulnerabilities in software and operating systems in order to obtain access, plant malware or create backdoors. The entry points can be accessed at any time as long as they remain hidden, and they can be used for espionage, surveillance, but also for disruptive actions. This kind of operations are done by intelligence services of all major states, and one particular issue ensues – no matter the initial aim of creating the access point, the backdoors can be detected and exploited by other intelligence services or non-state hackers, and they can be used even against the state that designed them in the first place. (Dunn Cavelty and Egloff 2019, 47-50)

2.2. Different types of cyber 'weapons'

There are several means (or weapons) used in cyber conflict, such as distributed denial of service attacks (DDoS), website defacement, or intrusions and infiltrations by using malware. For this research, the focus will be put on the latter. Intrusions and infiltrations are targeted methods which can have long-term damage on affected systems and organisations/individuals. They include the use of malware, Trojans and/or backdoors, software which are patched/attached or injected in a program in order to permit penetration into networks, systems or software, with the main objective of stealing sensitive

information. The backdoors can be used at any time after the first intrusions and they can be exploited by other actors as well, if left unchecked. Infiltrations are designed to evade detection by victims, and most of the hacks done by state actors are employed covertly. (Valeriano and Maness 2015, 34-36)

More specifically, malware, a broad term which can also encompass spyware or computer viruses, is a software that can be spread from one computer (or network) to another, corrupting or stealing data, or even causing system failure. Malware can also be used to disrupt or even deny computer and network operations. While malware is a type of malicious software, hacking is an action, representing the unauthorised access or usage of a computer or network. (Buil-Gil et al. 2020, 5)

Moreover, ransomware, increasingly common during the COVID-19 pandemic, is a type of malware that locks victims' computers and encrypts their data. It also offers a way out – the victims can pay out a ransom to recover their data and regain access to their computers, but there is no guarantee that this will happen after making the payment. Ransomware attacks are becoming one of the most common types of malware used in cyber operations. (Kharraz et al. 2015, 3-4)

Closely related to ransomware, cybercrime refers to criminal acts "committed online by using electronic communications networks and information systems" (European Commission 2020a). Cybercrime includes phishing (using emails that carry malware infected links or attachments), scams, attacks on information systems, ransomware or online fraud (Pranggono and Arabo 2020, 2-3; NCA 2020, 46; European Commission 2020a). Cybercrime can refer to regular crimes which are conducted online (such as using the Internet to sell illegal products), but it is more commonly related to crimes that depend on digital technologies and the Internet (NCA 2020, 46).

2.3. The role of public attribution of cyber operations

Florian Egloff and Max Smeets define public attribution of cyberattacks as "the act to publicly disclose information about the malicious cyber activity to a

machine, specific perpetrator, and/or ultimately responsible adversary" (2021, 3). Attribution needs to be credible by the international community, but it does not have to be flawless, as damaging the reputation of the attacker might lead to deterrence and restrain (Nye Jr. 2011, 34). Publicly attributing a cyber operation could coerce and compel an actor, altering the cost-benefit calculus because of potential delegitimization, and it can also open on to other forms of punitive measures, such as sanctions (Egloff and Smeets 2021, 6). Public attribution can also lead to using a larger amount of resources and capabilities to launch cyber operations (Egloff and Smeets 2021, 7). Furthermore, by making cyber operations, potential threats and vulnerabilities public, network and system owners might apply patches and updates quicker in order to secure their devices and data, and this can lead to enhancing prevention and defence from further attacks (Egloff and Smeets 2021, 7). Another upside of publicly attributing a cyber operation is that it can contribute to the world community by forming international standards of cyber conflict and setting the norm, securing a common understanding of what an actor can and cannot do in cyberspace (Egloff and Smeets 2021, 5; Rowe 2015, 67).

3. CYBER OPERATIONS DURING THE COVID-19 PANDEMIC

3.1. Cybercrime on the rise

The COVID-19 pandemic was also associated with unprecedented and significant changes in crime opportunities, as individuals started spending more time on the Internet and less time outside, leading to a decrease in street crime but to an increase in Internet crimes. Moreover, people started using their personal computers for teleworking, participating in videoconferences, accessing COVID-19 related information and more online shopping. (Buil-Gil et al. 2020, 2-4)

During the coronavirus pandemic, cybercrimes have not only substantially increased, but also grew in diversity and methods used, adjusting to the changes generated by the pandemic, malicious actors in cyberspace exploiting the higher dependency on digital means of individuals, companies, governments and

organizations (Naidoo 2020, 306-317). Online phishing was the most common form of cybercrime during this period, having a rapid and significant increase during the first months of the pandemic (Pranggono and Arabo 2020, 2). For instance, the UN disarmament chief stated in May that cybercrime was rising considerably during the pandemic, mentioning that there has been an 600% increase in malicious emails during the first months on the coronavirus pandemic (Lederer 2020). Interpol (2020) also saw a significant increase in malicious cyber activity since March 2020, stating that governments, critical infrastructure and large companies became the main targets of cybercrime (online scams and phishing), disruptive malware (such as Ransomware and DDoS) and spyware.

In May 2020, the Guardian reported, based on the data from a cybersecurity company (Darktrace) that the proportion of cyberattacks targeting employees working from home increased in May to 60% of malicious email traffic, as compared to the period before UK introduced the lockdown, when the proportion was only 12% (Jolly 2020). Furthermore, according to Microsoft, cyber operations related to COVID-19 started once the WHO declared a global health emergency, in early February 2020. The overall volume was low at first, but during the first week of March cyber operations (mostly cybercrime) reached a volume of almost one million per day. But, after this spike, the volume started to fall at the end of March 2020, with levels remaining relatively lower for the following months, with the exception of a slightly higher volume in May 2020. (Matthews 2020)

3.2. The most significant COVID-19 related cyberattacks

Cyberattacks targeting organisations and institutions such as healthcare providers, banks, and individuals intensified during the COVID-19 pandemic, alongside the rise in remote work, which created new and potentially vulnerable access points (Martin, Freitas Jr 2020). The pandemic created several conditions which had been exploited as vulnerabilities by malicious actors: the high demand for PPE products; border closures and decreased mobility; increased

reliance on teleworking (especially counting that it was done in urgency and mostly with little planning or previous experience); and increased uncertainty, doubt and fear in the general population (ENISA 2020).

During the first 5 months of the coronavirus pandemic, the Center for Strategic & International Studies (CSIS) has identified 43 significant cyber incidents, out of which 5 targeted directly hospitals or research centres that studied the disease or on the development of a vaccine – the US, the UK, Australia and even the WHO were victims of various cyber operations (CSIS 2021).

The first significant cyberattacks occurred in the Czech Republic targeting the Brno University Hospital on March 13. The attacks occurred right at the beginning of the pandemic, during an already busy, uncertain and chaotic period. The cyberattacks were severe enough that the hospitals had to postpone urgent surgical interventions and planned operations and also redirect new patients to the St. Anne University Hospital, which was nearby. Moreover, Brno University Hospital had to shut down all of its IT network during the cyberattack. As the hospital was one of Czechia's biggest COVID-19 testing facilities at the time, the incident was considered a severe one. (Burgess 2020a; Cimpanu 2020a; Wiggen 2020, 4)

Moreover, in March 2020, the US Health and Human Services Department was also the target of a cyberattack on its computer networks, identified as a DDoS, and even though it did not manage to cause serious damage to the agency's systems and it did not seem that the attackers stole any data, it was also doubled by a disinformation campaign spreading fake news about an introduction of a nationwide lockdown in the United States (Stein and Jacobs 2020). In the same month, a series of DDoS attacks targeted a group of hospitals in Paris and the US Department of Health, affecting access to email services and online servers (Pranggono and Arabo 2020, 3).

Later, on April 17, two hospitals in the Czech Republic reported that their computer systems were targeted by attempted cyberattacks, only one day after its cybersecurity agency warned that a campaign of cyberattacks was expected to hit Czech critical infrastructure. The hospitals managed to avert any serious disruption and the attacks were thwarted. (Wiggen 2020, 6; Reuters 2020)

After the cyberattacks against Czech hospitals, US Secretary of State Mike Pompeo issued a statement, calling upon "the actor in question to refrain from carrying out disruptive malicious cyber activity against the Czech Republic's healthcare system" (Corera 2020a). The most significant cyberattack on hospitals occurred in 2017, during the global ransomware campaign WannaCry. The ransomware caused severe disruption in UK's National Health System and it cost the NHS over 100 million pounds (Burgess 2020a). Other similar examples are in the US, where a public health department in Illinois was targeted by a ransomware campaign, and in France, where ransomware began targeting local authorities (Burgess 2020a). In another case, a London laboratory which carried out research on a COVID-19 vaccine was targeted by a ransomware attack and even though the research facility managed to protect its IT systems, the attackers published stolen patient records on the Internet (Wiggen 2020, 4).

In addition to this, worrying reports about cyber operations targeting power infrastructure started to appear during the first stage of the pandemic. Cyberattacks on power sector employees surged in Spring and Summer, after some of its employees started working from home, with hackers using phishing emails to gain access to workers' computers. Cyber operations were launched with the goal of shutting down company systems with ransomware or in an attempt of infiltrating networks. (Martin and Freitas Jr 2020)

In March 2020, Europe's association of grid operators suffered a cyberattack that affected its internal office systems. Later, in May, United Kingdom's grid data systems was hacked, but it did not affect electricity supplies. Moreover, United States' largest grid operator announced during July that the amount of attacks started to grow during the pandemic. (Martin and Freitas Jr 2020)

In this context, on April 30, the High Representative of the European Union, Josep Borrell issued a statement on behalf of the EU in which it acknowledges that cyber operations have targeted essential operators (including in the healthcare sector) in its member states and international partners, condemning the malicious cyber activities. The EU noted that it detected significant phishing and malware distribution campaigns, DDoS attacks and scanning activities since the beginning of the COVID-19 pandemic, with some of this operations affecting critical infrastructures essential to managing the crisis. (Consilium 2020a)

Thus, in June 2020, European Commission President Ursula von der Leyen suggested that China may have been behind cyberattacks targeting hospitals and behind online disinformation campaigns in Europe (European Commission 2020b). After an EU-China Summit videoconference, von der Leyen declared that "we have seen cyberattacks on hospitals" and "a rise of online disinformation", adding that "we pointed out clearly that this cannot be tolerated" (ibid.).

As cyber operations affected hospitals, COVID-19 vaccine research centres and critical infrastructure represented serious incidents, the EU provided a clear response, acknowledging the escalation of malicious state-sponsored cyber activity. The European Union imposed in July 2020 the first ever sanctions against cyberattacks. The EU imposed restrictive measures against three entities and six individuals responsible or involved in several cyberattacks which were carried out in recent years, including the attack against the Organisation for the Prohibition of Chemical Weapons, the global ransomware campaign WannaCry (which heavily affected the UK), NotPetya (2017 cyberattacks against Ukraine) and Operation Cloud Hooper (a Chinese cyber espionage campaign against Western states). (Consilium 2020b)

3.3. Attempts of tampering with water filtration systems in Israel and the US

The cyberattacks between Israel and Iran deserve a separate section, as they were not directly related to the COVID-19 pandemic, but the crisis situation might have been used in order to launch such attacks, or the attack might have been launched to divert domestic or international public opinion from looking at the epidemic situation in Iran.

In late April, Israel's Water Authority and the National Cyber Directorate reported a series of cyber incidents on six water and sewage treatment facilities around the country. Israel determined that the incidents were in fact, a series of cyberattacks, but they did not manage to cause serious disruption in the systems. The cyberattack could have raised chlorine levels of water that is supplied to homes to dangerous levels and cause serious disturbances, but it

was thwarted by Israeli authorities. Moreover, as the attacks occurred during a heatwave, a shutdown of water supply would have caused significant problems. Israeli and international media assessed that Iran was behind the attacks, but the Iranian regime denied any involvement. (Staff 2020; Baram and Lim 2020; Glosserman 2020)

Later, in May, a cyberattack was launched against the computer systems of Iran's Shahid Rajaee Port near the Strait of Hormuz, the country's most important hub for maritime trade, which manages almost half of the Iran's foreign trade. Iranian authorities claimed that the attack only disrupted private companies' systems, but unnamed officials appeared in international media claiming that Israel launched the cyber operations as retaliatory attacks. More than this, it was reported that the cyberattack caused serious road and waterway congestion for several days. For instance, Israel's Defense Forces Chief of Staff spoke about retaliating against Israel's adversaries, but he did not acknowledge Israel's role in the attack against Iran. One month later, Israel reported that its water management facilities were targeted once again by cyberattacks, but authorities claimed that the new attacks did not cause any serious damage. (Baram and Lim 2020; Cimpanu 2020b; Glosserman 2020)

However, the cyberattacks on Israel's water supply were not the only ones occurring during the pandemic. In February 2021 a Florida city's water supply was targeted by a malicious cyber operation, during which an unspecified hacker gained access to its remote access software and raised the levels of sodium hydroxide by a factor of 100 compared to normal levels, but the intrusion was noticed quickly and the level was reduced back (Marquardt and Levenson 2021; CSIS 2021).

3.4. COVID-19 related cyber espionage campaigns

Especially during the first stage of the pandemic, marked by uncertainty and a lack of information regarding the virus, world governments were interested in obtaining substantial information on potential treatment for COVID-19, vaccine research or even national policies and the spread of the virus (Wiggen 2020, 4).

In mid-April 2020, FBI Deputy Assistant Director Tonya Ugoretz stated that there had been reports of cyber espionage campaigns targeting institutions working on research related to COVID-19 (Corera 2020a). In May 2020, the British National Cyber Security Centre reported that 'adversary' state actors were attempting to hack research facilities and British universities to steal information and research related to coronavirus vaccine development, or even research regarding the COVID-19 pandemic (Grierson and Devlin 2020).

Likewise, in April 2020 Google published findings related to its tracking of cyber operations during the COVID-19 pandemic. According to Google, cyber operations, especially phishing campaigns, have not only risen due to cybercrime, but also due to state actors. Hackers backed by governments exploited the pandemic and carried out digital reconnaissance and cyber espionage campaigns. Google detected over 12 state-sponsored hacking groups that were using the coronavirus pandemic in an attempt to distribute malware through phishing emails disguised as information regarding the virus. During April, the company warned that it had identified more than 18 million coronavirus related spam and phishing messages per day, from a total of more than 100 million daily phishing emails. (Newman 2020a)

On April 23, 2020, the World Health Organization reported a fivefold increase in cyberattacks worldwide. The organization recorded a significant increase both in the number of cyberattacks directed at its staff and phishing emails targeting other institutions and individuals. In addition to this, staff members of the WHO were targeted by phishing emails allegedly originating in Iran also in March 2020. (WHO 2020; CSIS 2021; Wiggen 2020, 4)

UK's National Cyber Security Centre stated in July 2020 that research groups and drug companies were targeted by a hacking group known as APT29, considered to be part of one of Moscow's intelligence services. Nevertheless, British authorities stressed that the cyber operations did not cause serious disruptions to vaccine research. In the Summer of 2020, the UK was among the countries leading global efforts to produce a coronavirus vaccine, with the work of researchers from Oxford University and Imperial College London. (Sabbagh, Roth 2020)

Moreover, during the first months of the pandemic it seems that most of the cyber espionage came from China, Chinese state-hackers targeting research institutions, companies and governments around the globe. For example, in March, a hacking group known as APT41 (Advanced Persistent Threat) disrupted the systems of a social care services provider in the UK, but China's goal was to gather information that could be beneficial for its government (Burgess 2020b). James Brokenshire, UK's security minister, declared that London is "more than 95%" sure that the US, UK and Canadian organisations involved in developing a vaccine against COVID-19 were targeted by Russian state-sponsored cyber operations (Walker 2020; Sabbagh and Roth 2020).

In July 2020, the US Justice Department released an indictment against two Chinese hackers accused of working for China to steal and try to steal terabytes of data, including information regarding COVID-19 research. The Beijing-backed hackers targeted companies based in the US, Germany, the UK, South Korea, Japan, Australia, Belgium, the Netherlands, Spain and Sweden. One of these operations of cyber espionage occurring in April 2020, against a UK medical research company. Furthermore, the Justice Department stated that the hackers were assisted by the Chinese Ministry of State Security, adding that weapon systems and defence contractors were hacked along with coronavirus related medical research. (Strohm and Gallagher 2020; Burgess 2020b)

During the same month, a coordinated statement from the UK, US and Canada attributed cyber operations targeting COVID-19 vaccine research to APT29 (aka 'Cozy Bear'), a Russian government-based hacker group (considered part of Russian intelligence services). The cyber operations had the goal of breaking into computers used by academic and pharmaceutical institutions and companies around the world working on a coronavirus vaccine in an attempt to steal research. The group's attacks used both phishing and custom malware as tools for breaking into the systems. (Strohm and Gallagher 2020; James and Scherer 2020)

Nevertheless, cyber espionage was still prevalent for the remainder of the year, as vaccines against the COVID-19 started to be produced and transported to several countries. In December 2020, IBM announced that cyber espionage campaigns targeted the international supply chain of vaccines, using phishing

emails sent to the WHO, World Bank, European Commission and UNICEF – the organisations that provide the delivery "cold chain" used for keeping vaccines at required temperatures during transportation (Corera 2020b). In the same period, the European Medicines Agency announced that it had been the victim of a cyber espionage campaign, during which hackers "unlawfully accessed" documents related to the Pfizer-BioNTech COVID-19 vaccine (Stubbs 2020).

3.5. The case of the Russian 'SolarWinds' cyber operation and the Chinese hack on Microsoft Exchange

The SolarWinds cyber operation (or hack) became known in December 2020, when the US cybersecurity company FireEye announced that it had discovered a hacking campaign deployed by a state actor, of which FireEye was also a victim. The company uncovered that the hackers used as a vector for intrusion SolarWinds, an American IT infrastructure and network-management company that maintains the Orion software which manages and monitors networks. Afterwards, it became known that Orion had been infected since October 2019, which allowed hackers to hijack a routine software update from SolarWinds in March 2020, silently installing malware on clients' systems and networks. Thus, clients that installed Orion's software update planted a Russian backdoor on their systems and networks (Willet 2021, 7-8; Newman 2020b).

The U.S. government announced in February 2021 that the hackers managed to gain access to emails and data of several American federal agencies, such as the Departments of Treasury and Justice, the Department of Homeland Security or NASA, and also of dozens of companies, with Microsoft, Intel, FireEye or Cisco among others (Willet 2021, 8; Greenberg 2021).

The aim of the cyber operation was espionage, or gathering intelligence, but such operations can also be used both for espionage and destructive cyberattacks, using the same vulnerability or access point, and there is also the possibility that other hackers (state or non-state) can exploit it for disruptive attacks (Willet 2021, 11). Therefore, the first step to mitigating the cyber

campaign is to successfully disinfect the systems and eliminate the backdoor, as there is a significant risk that other hackers could access it (Newman 2020b).

In April 2021, the United States imposed sanctions on Russia in relation to the SolarWinds hack and other cyber operations and aggressions, such as disinformation operations, interference in the 2020 US elections, the persecution of Aleksey Navalny and, most relevant, the 2017 NotPetya cyberattack and the cyberattack on the 2018 Winter Olympics (Greenberg 2021). Moreover, the US publicly attributed the Solar Winds cyber operation to the Foreign Intelligence Service of the Russian Federation (SVR), the intelligence agency hiding its code in Orion's software updates, managing to infect around 18.000 networks (Greenberg 2021).

During its assessment, mitigation and remediation of the SolarWinds hack, the U.S. was targeted once again by a large cyber espionage campaign, which was also very similar to the Russian one. In early March 2021, another cyber operation was made public, this time by Microsoft, whose software was affected. Microsoft attributed the cyber espionage campaign to China, state-sponsored hackers managing to exploit security flows in Microsoft's Exchange email servers and infect tens of thousands of individuals, institutions and companies (Willet 2021, 9). The cyber operation compromised over 60.000 victims globally and other estimates run up to over 300.000 victims, but the company was quick to release a patch that covered the vulnerability (Sanger, Barnes and Perlroth 2021a; Robertson, Mehrotra and Gallagher 2021). Moreover, there is a high possibility that China might have taken advantage of the disruption caused by the Russian cyber operation to deploy the cyber operation when attention was put elsewhere (Robertson, Mehrotra and Gallagher 2021).

Similar to the SolarWinds hack, the Chinese cyber operation leaves victims vulnerable to other cyber operations, as their computers could get used as botnets to attack other systems or get infected with malware, and Microsoft already warned that cybercriminals started using the backdoors created by the Chinese state-hackers to infect systems with ransomware. (Sanger, Barnes and Perlroth 2021b; Robertson, Mehrotra and Gallagher 2021).

The state-sponsored Chinese hacking group, identified as such by Microsoft, targeted tens of thousands of organisations, from government agencies,

legislative bodies, local authorities and defence contractors, to think tanks, small businesses and COVID-19 research centres (CSIS 2021; Sanger, Barnes and Perlroth 2021a).

4. EXPLOITING THE PANDEMIC. A SIGNIFICANT ESCALATION OF CYBER OPERATIONS

4.1. Business as usual in cyberspace or a serious escalation of cyber incidents?

The importance and impact of cyber operations during the first stage of the pandemic was amplified because of the already ongoing public health crisis which seriously affected most of the world's states. Nevertheless, the cyber incidents during the coronavirus pandemic stand as a great example of why cybersecurity has become more and more an issue over the years, and why it is so important for states, institutions and companies (and even individuals) to have in place proper cybersecurity practices. Alongside the cyberattacks on Czech hospitals in March and April 2020, another important event was the exchange of cyberattacks between Iran and Israel in May-July 2020. Even though the attacks were not directly related to developments regarding the pandemic, the two states might have taken the pandemic as an opportunity to boost their attacks, and this is also a dangerous development. More than considering the potential disruptive impact of a full-blown Israel-Iran cyber conflict, the issue of tampering with water supply systems shows how important it is to protect critical infrastructure from malicious cyber activity.

Going further, even though there have been observed some major cyberattacks, the large proportion of cyber operations was comprised by cyber espionage campaigns related to coronavirus research and developments, and cybercrime, caused primarily because of the large and rapid increase in teleworking. Moreover, the increase was mainly attributed to the fact that malicious cyber actors exploited the higher and unprecedented dependency on digital means. But not only the number matters, as the intensity and impact are more important. The SolarWinds and Microsoft hacks, cyberattacks on hospitals,

vaccine-related research centres and on critical infrastructure represent major escalations in cyber conflict.

Adding to this, the research done regarding this period shows that cybercrime and online fraud have increased during the COVID-19 pandemic, with cybercrime peaking during the first months of the pandemic, when strict lockdowns were in place (Newman 2020a; Naidoo 2020; Matthews 2020). In March 2020, Microsoft recorded the largest uptick in COVID-19 cyber operations, which numbered more than 5 million per day (Matthews 2020). Later on, in April 2020, the WHO saw a 'fivefold increase' in cyber operations directed at its staff and at the 'public at large' and Google stated that it identified over 240 million COVID-19 related spam and phishing messages per day, more than double compared to what it usually recorded, adding that most of the phishing campaigns were actually part of state-sponsored cyber espionage campaigns targeting state actors, including the US (WHO 2020; Newman 2020a). Buil-Gil et al. observed that, even though there was a general increase in cybercrime affecting both individuals and organisations, cybercrimes have mainly targeted individuals (2020, 9-10). For instance, in the UK cybercrime targeting individuals doubled in March-April 2020, compared to the previous months, while cybercrime targeting organisations increased by 50% (Buil-Gil et al. 2020, 3). However, it is likely that a significant proportion of cybercrime recorded during this period could have been part of state-sponsored cyber espionage campaigns, online phishing being one of the main ways of spreading malware-infected files to systems and networks of organisations, including state-institutions (Wiggen 2020, 4).

Moreover, the cyberattacks on hospitals and other health care facilities, the cyber espionage campaigns targeting COVID-19 related research, the surge in teleworking and COVID-19 related cybercrimes, all of these developments show that cyber operations are very significant threats and become even more dangerous during other crises. Moreover, one very important aspect is that the cyberattacks were identified as state-sponsored, with the EU, UK and US attributing cyber operations to China and Russia. Furthermore, the EU imposed the first ever sanctions related to cyberattacks (but regarding cyber operations taking place before 2020) and the US indicted several Chinese state-hackers for

cyber espionage activities and imposed sanctions on Russia for cyber operations, also attributing the SolarWinds hack to the SVR intelligence service.

More generally, these events can be regarded as malicious cyber activity, which can be divided in cyber operations (cyberattacks and cyber espionage, which use or are facilitated by the use of malware, ransomware, Trojans or backdoors) and cybercrime (phishing, fraud, scams, ransomware). All things considered, there are two types of cyber operations that occurred during the first year of the COVID-19 pandemic. The first type describes cyber operations deployed during the pandemic that exploited the fact that attention was put on the public health crisis, and so attacks that might have occurred in the near future regardless of the pandemic, but they were launched during 2020 and 2021 because the health crisis created a perfect environment for them and they might have been less substantial if not the pandemic. This is the case of cyber espionage that is not entirely related to COVID-19, such as the SolarWinds and Microsoft hacks, cyberattacks on electrical grid operators, attempts of tampering with water filtration facilities in Israel and the U.S. or cybercrime targeting individuals and companies for financial gain. Public attributing the cyber operations to China and Russia by the European Union, United States, Canada or the United Kingdom, and the announcement of sanctions show the magnitude of the escalation. Ultimately, they can all be considered major state-sponsored cyber operations used against other state actors, as the cyber operations included in this research targeted key infrastructures, especially taking into account the pandemic. Moreover, state actors exploited the situation and disruption created by the pandemic to launch major cyberattacks, because the governments' attention was mainly put on managing the public health crisis.

The second type concerns cyber operations deployed because of the COVID-19 pandemic, and so it refers to COVID-19-related operations. This is the case of cyberattacks on hospitals, health-related facilities and institutions (DDoS, ransomware and others), cyber espionage related to the research on the disease, national policies and vaccines, and cybercrime directly related to COVID-19. Moreover, the dividing line between cybercrime and state-sponsored cyber operations is blurred, as they often use the same tools and/or tactics, and hence

a part of the increase in cybercrime during 2020 might have been the result of state-sponsored hacking.
Furthermore, the impact, relevance and importance of the cyber operations mentioned in this research are shown by the effects that these attacks had – the operations were of great complexity and magnitude (as in the case of SolarWinds), and this was shown especially because they were publicly attributed to China and Russia by the US, UK and EU. In addition to this, the cyberattacks against water infrastructure in Israel and the US created a dangerous precedent, as this kind of targets were usually avoided by high-profile hackers (state or non-state).

4.2. Lessons learned and a way forward

Finally, there are some lessons learned that emerged from these cyber incidents. All of these developments must generate a call to action for states to enhance their cybersecurity capabilities. The cyberattacks in the Czech Republic or the cyber operations against dozens of research facilities were not thwarted only because the attackers did not have sufficient capabilities or because they did not intent to do so, but because these states and organizations had in place sufficiently good cybersecurity practices and managed to prevent a major impact. But this was not also the case of cyber espionage campaigns such as SolarWinds's Orion or Microsoft's Exchange exploits and infiltrations targeting the US.
States and organizations must take all of these cyber developments as calls to action and start enhancing their cybersecurity capabilities, because cyber operations like these are only the beginning. Furthermore, a cyberattack on healthcare providers or on the power grid will have a serious impact on the state and on the general population and it will cause great disruptions, but it will also create large vulnerabilities and provide space for even more cyber operations. Moreover, publicly attributing cyber operations, condemning and even imposing sanctions must become the new norm in order to prevent serious escalations. Sophisticated, widespread and disrupting cyberattacks have a high

possibility of occurring in the near future, and organisations and governments should prepare for such events.

In order to enhance the level of cybersecurity, society, business and government must work together and coordinate their efforts (Dunn Cavelty and Egloff 2019, 50). Other steps that organisations (and individuals) need to take are general recommendations such as: updating all software and firmware, most especially internet security software, implementing multi-factor authentication as much as possible across the network and training all employees on cybersecurity issues (Pranggono and Arabo 2020, 4-5). The government must enhance public awareness activities, provide and fund education related to cyber issues and uphold public-private collaboration and also international cooperation (Davis and Pipikaite 2020; Willet 2021, 16). Governments should also employ efficient communication with the general public in order to raise awareness regarding cyber issues (Dunn Cavelty and Egloff 2019, 49).

All things considered, this whole development of cyber incidents during the pandemic has brought forward important lessons learned. One important aspect of a good cybersecurity practice is taking early, rapid, decisive actions (Davis and Pipikaite 2020). Moreover, all actors should enhance their cybersecurity capabilities and keep in mind the need to always be prepared for complex and targeted cyber operations. Cyber incidents that occurred during the pandemic have shown that the role of private cybersecurity companies and large IT companies is pivotal, as was the case of FireEye disclosing the SolarWinds hack and Microsoft disclosing the Exchange hack and attributing it to Chinese state hackers, and hence the need for public-private collaboration and information exchange becomes crucial. Furthermore, cyber operations seem to be more likely to be deployed during other crises and major events, so all actors need to take even more prevention and caution during such times. Hospitals, health-related facilities, research centres and critical infrastructure such as water facilities are not intangible and they have become major targets and vulnerabilities must be quickly addressed in order to avoid serious disruptions.

Finally, recommendations can be divided in general and specific recommendations. General recommendations are those that can be implemented by everyone (individuals, private companies, governments etc.). They comprise

the necessity of applying regular updates on software, hardware, operating systems and firmware as often as possible; implementing multifactor authentication wherever possible on systems and networks; maintaining an efficient and constantly updated internet security software; and self-education (as much as possible) on cyber issues and basic cybersecurity practices (for individuals, it can be enough to just read online some steps and advice, and for private companies it can be enough to have some general training sessions or workshops for employees). Furthermore, specific recommendations refer to actions that mainly relate to state actors and governments. They include enhancing, consolidating and maintaining a well-working, close and efficient public-private cooperation and international cooperation; having clear, complex and efficient procedures in place for cybersecurity and cyberattack mitigation, and provide and organise simulations, exercise and training sessions, at least for critical public sector employees; provide education, training and information on safe cyber practices for the general population, state institutions and private companies and funding for programs and academic research related to cybersecurity issues; securing critical infrastructure; paying more attention to hospitals, as they have started to become one of the major targets of cybercrime and state-sponsored cyber operations; and putting more emphasis on the public attribution of cyber operations, indictment of state-sponsored hackers and imposing international sanctions on states and agencies that deploy major cyber operations. After publicly attributing a cyberattack, a state can also indict the hackers (like the U.S. does in some cases), impose sanctions, and all of these actions are even more efficient if they are done together with other states, such as the joint U.S., U.K. and Canada statements (Willet 2021, 13), and so international cooperation becomes important in this aspect too.

5. CONCLUSIONS

Cyberattacks on COVID-19 hospitals and health departments, cyberattacks targeting water treatment facilities and electrical grid operators, cyber espionage campaigns against COVID-19 research facilities, cybercrime and large-scale

cyber espionage campaigns unrelated to the pandemic are very serious events and must be adequately addressed by governments, but the fact that they occurred during the public health crisis caused by the pandemic is a worrying development. Thus, state actors responded properly, mitigating the effects and publicly attributing some of the major cyber operations. Overall, it can be said that the situation could have been far worse, and all of these cyber operations show that any individual and any organisation can become a target and can have its activities significantly disrupted.

The cyber operations that occurred during the pandemic set some serious precedents and raised the stake of cybersecurity even higher, as cyberattacks on already overwhelmed COVID-19 hospitals could have provoked the first ever direct deaths resulting from a cyberattack. In the future, this might become a reality, as critical infrastructure will continue to be one of the main targets. Furthermore, cyber espionage campaigns such as the SolarWinds hack might become the norm in cyberspace, and cybercrime might blend even more with malicious state-sponsored cyber operations.

The upcoming widespread digitalization of public services and work without implementing proper cybersecurity practices can lead to one daunting assumption – in terms of cyberattacks and cybercrime, the worst is yet to come. Even with a significant level of cybersecurity and prevention, a major cyberattack can still occur in the future, and the extent of damages will depend on how good have governments prepared for it. The pandemic will be over in a couple of years, but the escalation of cyber operations is here to stay.

REFERENCES

- Baram, Gil, and Kevjn Lim. 2020. "Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks". *Foreign Policy*. June 5. Accessed April 20, 2021. https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.
- Boeke, Sergei. 2017. "National cyber crisis management: Different European approaches". *Governance*. 31, no. 3: 449-464.

- Buil-Gil, David, Fernando Miró-Llinares, Asier Moneva, Steven Kemp, and Nacho Díaz-Castaño. 2021. "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK". *European Societies.* 23, no. 1: 1-14.
- Burgess, Matt. 2020a. "Hackers are targeting hospitals crippled by coronavirus". *Wired*. March 22. Accessed April 20, 2021. https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing.
- Burgess, Matt. 2020b. "Chinese hackers targeted major UK companies as coronavirus raged". *Wired*. July 23. Accessed April 20, 2021. https://www.wired.co.uk/article/china-coronavirus-hacking-uk-us.
- Cimpanu, Catalin. 2020a. "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak". *ZDNet*. March 13. Accessed April 20, 2021. https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/.
- Cimpanu, Catalin. 2020b. "Two more cyber-attacks hit Israel's water system". *ZDNet*. 20 July. Accessed April 20, 2021. https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/.
- Consilium. 2020a. "Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic". Council of the EU. April 30. Accessed April 20, 2021. https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.
- Consilium. 2020b. "EU imposes the first ever sanctions against cyber-attacks". Council of the EU. July 30. Accessed on April 20, 2021. https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks.
- Corera, Gordon. 2020a. "Coronavirus: Cyber-spies seek coronavirus vaccine secrets". *BBC*. May 1. Accessed April 20, 2021. https://www.bbc.com/news/technology-52490432.
- Corera, Gordon. 2020b. "Coronavirus: Hackers targeted Covid vaccine supply 'cold chain'". *BBC*. December 3. Accessed April 20, 2021. https://www.bbc.com/news/technology-55165552.

- CSIS. 2021. "Significant Cyber Incidents". *Center for Strategic & International Studies*. Accessed April 20, 2021. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
- Davis, Nicholas, and Algirde Pipikaite. 2020. "What the COVID-19 pandemic teaches us about cybersecurity – and how to prepare for the inevitable global cyberattack". *WEF*. June 1. Accessed April 20, 2021. https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/.
- Dunn Cavelty, Myriam, and Florian J. Egloff. 2019. "The politics of cybersecurity: Balancing different roles of the state". *St. Antony's International Review*. 15, no. 1: 37-57.
- Egloff, Florian J., and Max Smeets. 2021. "Publicly attributing cyber attacks: a framework". *Journal of Strategic Studies*. 1-32.
- ENISA. 2020. "Cybersecurity in the healthcare sector during COVID-19 pandemic". *European Union Agency for Cybersecurity*. May 11. Accessed April 20, 2021. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic.
- European Commission. 2020a. *Cybercrime*. Accessed April 20, 2021. https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en.
- European Commission. 2020b. *Statement by President von der Leyen at the joint press conference with President Michel, following the EU-China Summit videoconference*. Statement, June 22. Accessed April 20, 2021. https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1162/.
- Glosserman, Brad. 2020. "A 'new normal' in cyberwar should scare us to action". *The Japan Times*. June 10. Accessed April 20, 2021. https://www.japantimes.co.jp/opinion/2020/06/10/commentary/world-commentary/new-normal-cyberwar-scare-us-action.
- Greenberg, Andy. 2021. "US Sanctions on Russia Rewrite Cyberespionage's Rules". *Wired*. April 15. Accessed April 20, 2021. https://www.wired.com/story/us-russia-sanctions-solarwinds-svr/.
- Grierson, Jamie, and Hannah Devlin. 2020. "Hostile states trying to steal coronavirus research, says UK agency". *The Guardian*. May 3. Accessed April 20, 2021. https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency.

- Hodges, Duncan, and Sadie Creese. 2015. "Understanding cyber-attacks". In *Cyber Warfare: A multidisciplinary analysis*. ed. James A. Green. 33-60. New York: Routledge.
- Interpol. 2020. "INTERPOL report shows alarming rate of cyberattacks during COVID-19". *News and Events*. August 4. Accessed April 20, 2021. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
- James, William, and Steve Scherer. 2020. "UPDATE 3-Russia trying to steal COVID-19 vaccine data, say UK, U.S. and Canada". *Reuters*. July 16. Accessed April 20, 2021. https://www.reuters.com/article/health-coronavirus-cyber/update-3-russia-trying-to-steal-covid-19-vaccine-data-say-uk-u-s-and-canada-idUSL5N2EN4X6.
- Jolly, Jasper. 2020. "Huge rise in hacking attacks on home workers during lockdown". *The Guardian*. May 24. Accessed April 20, 2021. https://www.theguardian.com/technology/2020/may/24/hacking-attacks-on-home-workers-see-huge-rise-during-lockdown.
- Kharraz, Amin, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. 2015. "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks". *Detections of Intrusions and Malware, and Vulnerability Assessment, 12th International Conference, DIMVA 2015 Milan, Italy, July 9-10, 2015, Proceedings*. ed. Magnus Almgren, Vicenzo Gulisano and Federico Maggi. 3-24. Cham: Springer.
- Lederer, Edith M. 2020. "Top UN official warns malicious emails on rise in pandemic". *AP*. May 23. Accessed April 20, 2021. https://apnews.com/article/c7e7fc7e582351f8f55293d0bf21d7fb.
- Marquardt, Alex, and Eric Levenson. 2021. "Florida water treatment facility hack used a dormant remote access software, sheriff says". *CNN*. February 10. Accessed April 20, 2021. https://edition.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html.
- Martin, Chris, and Gerson Freitas Jr. 2020. "Hackers Are Targeting the Remote Workers Who Keep Your Lights On". *Bloomberg*. July 30. Accessed April 20, 2021. https://www.bloomberg.com/news/articles/2020-07-30/hackers-are-targeting-the-remote-workers-who-keep-your-lights-on.
- Matthews, Lee. 2020. "Microsoft: COVID-19 Cyber Attacks Peaked In March And Fell Off Quickly". *Forbes*. June 17. Accessed April 20, 2021.

https://www.forbes.com/sites/leemathews/2020/06/17/microsoft-covid-19-cyber-attacks-peaked-in-march-and-fell-off-quickly/.

- Naidoo, Rennie. 2020. "A multi-level influence model of COVID-19 themed cybercrime". *European Journal of Information Systems.* 29, no. 3: 306-321.
- NCA. 2020. "National Strategic Assessment of Serious and Organised Crime". National Crime Agency. Accessed April 20, 2021. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file.
- Newman, Lily Hay. 2020a. "Google Sees State-Sponsored Hackers Ramping Up Coronavirus Attacks". *Wired*. April 22. Accessed April 20, 2021. https://www.wired.com/story/google-state-sponsored-hackers-coronavirus-phishing-malware/.
- Newman, Lily Hay. 2020b. "How to Understand the Russia Hack Fallout". *Wired*. December 19. Accessed April 20, 2021. https://www.wired.com/story/russia-solarwinds-hack-targets-fallout/.
- Nye, Joseph S. Jr. 2011. „Nuclear Lessons for Cyber Security?". *Strategic Studies Quarterly.* 5, no. 4: 18-38.
- Pranggono, Bernardi, and Abdullahi Arabo. 2021. "COVID-19 pandemic cybersecurity issues". *Internet Technology Letters.* 4, no. 2: 1-6.
- Reuters. 2020. "Czech hospitals report cyberattacks day after national watchdog's warning". *Reuters*. April 17. Accessed April 20, 2021. https://www.reuters.com/article/us-czech-cyber-ostrava/czech-hospitals-report-cyberattacks-day-after-national-watchdogs-warning-idUSKBN21Z1OH.
- Robertson, Jordan, Kartikay Mehrotra, and Ryan Gallagher. 2021. "China's Microsoft Hack, Russia's SolarWinds Attack Threaten to Overwhelm U.S.". *Bloomberg*. March 9. Accessed April 20, 2021. https://www.bloomberg.com/news/articles/2021-03-09/microsoft-solarwinds-breaches-spark-two-front-war-on-hackers.
- Rowe, Neil C. 2015. "The attribution of cyber warfare". In *Cyber Warfare: A multidisciplinary analysis*. ed. James A. Green. 33-60. New York: Routledge.
- Sabbagh, Dan, and Andrew Roth. 2020. "Russian state-sponsored hackers target Covid-19 vaccine researchers". *The Guardian*, July 16. Accessed April 20, 2021. https://www.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackers-target-covid-19-vaccine-researchers.
- Sanger, David E., Julian E. Barnes, and Nicole Perlroth. 2021a. "Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China". *The New York*

Times. March 7. Accessed April 20, 2021. https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html.

- Sanger, David E., Julian E. Barnes, and Nicole Perlroth. 2021b. "White House Weighs New Cybersecurity Approach After Failure to Detect Hacks". *The New York Times*. March 14. Accessed April 20, 2021. https://www.nytimes.com/2021/03/14/us/politics/us-hacks-china-russia.html.
- Schmitt, Michael N. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
- Staff, Toi. 2020. "6 facilities said hit in Iran's cyberattack on Israel's water system in April". *The Times of Israel*. 19 May. Accessed April 20, 2021. https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/.
- Stein, Shira, and Jennifer Jacobs. 2020. "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak". *Bloomberg*. March 16. Accessed April 20, 2021. https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.
- Strohm, Chris, and Ryan Gallagher. 2020. "U.S. Says China Hackers Stole Secrets, Sought Virus Data". *Bloomberg*. July 22. Accessed April 20, 2021. https://www.bloomberg.com/news/articles/2020-07-21/u-s-accuses-chinese-hackers-of-stealing-virus-trade-secrets.
- Stubbs, Jack. 2020. "Hackers steal Pfizer/BioNTech COVID-19 vaccine data in Europe, companies say". *Reuters*. December 9. Accessed April 20, 2021. https://www.reuters.com/article/uk-ema-cyber/hackers-steal-pfizer-biontech-covid-19-vaccine-data-in-europe-companies-say-idUKKBN28J1VF.
- Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press.
- Walker, Amy. 2020. "UK '95% sure' Russian hackers tried to steal coronavirus vaccine research". *The Guardian*, July 17. Accessed April 20, 2021. https://www.theguardian.com/world/2020/jul/17/russian-hackers-steal-coronavirus-vaccine-uk-minister-cyber-attack.
- WHO. 2021. "WHO Coronavirus (COVID-19) Dashboard". Accessed April 22, 2021. https://covid19.who.int/.
- Wiggen, Johannes. 2020. "Impact of COVID-19 on cyber crime and state-sponsored cyber activities". *Coronaperspectives*. Konrad Adenauer Stiftung.

Accessed April 20, 2021. https://www.kas.de/documents/252038/7995358/The+impact+of+COVID-19+on+cyber+crime+and+state-sponsored+cyber+activities.pdf/b4354456-994b-5a39-4846-af6a0bb3c378?version=1.0&t=1591354291674.

- Willet, Marcus. 2021. "Lessons of the SolarWinds Hack". *Survival.* 63, no. 2: 7-26.
- World Health Organization. 2020. "WHO reports fivefold increase in cyber attacks, urges vigilance". WHO. April 23. Accessed April 20, 2021. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.