Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic

Harjinder Singh Lallie[a,*], Lynsay A. Shepherd[b], Jason R.C. Nurse[c], Arnau Erola[d], Gregory Epiphaniou[a], Carsten Maple[a], Xavier Bellekens[e]

[a] WMG, University of Warwick, Coventry, UK
[b] School of Design and Informatics, Abertay University, Dundee, UK
[c] School of Computing, University of Kent, Canterbury, UK
[d] Department of Computer Science, University of Oxford, Oxford, UK
[e] Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow, UK

ARTICLE INFO

*Article history:*
Received 28 June 2020
Revised 21 November 2020
Accepted 22 February 2021
Available online 3 March 2021

*Keywords:*
Coronavirus
COVID-19
Cyber security
Cyber-attack
Cyber-crime
Attack timeline
Home working

ABSTRACT

The COVID-19 pandemic was a remarkable, unprecedented event which altered the lives of billions of citizens globally resulting in what became commonly referred to as the *new-normal* in terms of societal norms and the way we live and work. Aside from the extraordinary impact on society and business as a whole, the pandemic generated a set of unique cyber-crime related circumstances which also affected society and business. The increased anxiety caused by the pandemic heightened the likelihood of cyber-attacks succeeding corresponding with an increase in the number and range of cyber-attacks.

This paper analyses the COVID-19 pandemic from a cyber-crime perspective and highlights the range of cyber-attacks experienced globally during the pandemic. Cyber-attacks are analysed and considered within the context of key global events to reveal the modus-operandi of cyber-attack campaigns. The analysis shows how following what appeared to be large gaps between the initial outbreak of the pandemic in China and the first COVID-19 related cyber-attack, attacks steadily became much more prevalent to the point that on some days, three or four unique cyber-attacks were being reported. The analysis proceeds to utilise the UK as a case study to demonstrate how cyber-criminals leveraged salient events and governmental announcements to carefully craft and execute cyber-crime campaigns.

## 1. Introduction

Severe Acute Respiratory Syndrome Coronavirus-2 (SARS-CoV-2) is a novel strain of the coronavirus disease first detected in humans in 2019. On 11 February 2020 the World Health Organisation (WHO) announced they would refer to the disease as COVID-19. The pandemic that resulted from the spread of COVID-19 quickly became a global crisis event, resulting in the mass quarantine of 100s of millions of citizens across numerous countries around the world. At the time of writing, the WHO Coronavirus Disease (COVID-19) Dashboard reported over 7.5 million confirmed cases and in excess

[*] Corresponding author.
*E-mail addresses:* HL@warwick.ac.uk (H.S. Lallie), lynsay.shepherd@abertay.ac.uk (L.A. Shepherd), j.r.c.nurse@kent.ac.uk (J.R.C. Nurse), arnau.erola@cs.ox.ac.uk (A. Erola), gregory.epiphaniou@warwick.ac.uk (G. Epiphaniou), CM@warwick.ac.uk (C. Maple), xavier.bellekens@strath.ac.uk (X. Bellekens).

https://doi.org/10.1016/j.cose.2021.102248

of 430,241 deaths (World Health Organisation (WHO), 2020c) globally. As COVID-19 spread across the globe, it also led to a secondary significant threat to a technology-driven society; i.e., a series of indiscriminate, and also a set of targeted, cyber-attacks and cyber-crime campaigns. Since the outbreak, there have been reports of scams impersonating public authorities (e.g., WHO) and organisations (e.g., supermarkets, airlines) (MalwareBytes, 2020; The Times, 2020), targeting support platforms (Krebs on Security, 2020; Smithers, 2020), conducting Personal Protection Equipment (PPE) fraud (Europol, 2020) and offering COVID-19 cures (Norton, 2020; The Guardian, 2020). These scams target members of the public generally, as well as the millions of individuals working from home. Working at home *en-masse* has realised a level of cyber security concerns and challenges never faced before by industry and citizenry. Cyber-criminals have used this opportunity to expand upon their attacks, using traditional trickery (e.g., Nurse (2019)) which also prays on the heightened stress, anxiety and worry facing individuals. In addition, the experiences of working at home revealed the general level of unpreparedness by software vendors, particularly as far as the security of their products was concerned.

Cyber-attacks have also targeted critical national infrastructure such as healthcare services (Wired, 2020). In response to this, on April 8th 2020, the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) published a joint advisory on how cyber-criminal and advanced persistent threat (APT) groups were exploiting the current COVID-19 pandemic (UK's National Cyber Security Centre (NCSC), 2020a). This advisory discussed issues such as phishing, malware and communications platform (e.g., Zoom, Microsoft Teams) compromise. What is arguably lacking here and in research, however, is a broader assessment of the wide range of attacks related to the pandemic. The current state of the art is extremely dispersed, with attacks being reported from governments, the media, security organisations and incident teams. It is therefore extremely challenging for organisations to develop appropriate protection and response measures given the dynamic environment.

In this paper we aim to support ongoing research by proposing a novel timeline of attacks related to the COVID-19 pandemic. This timeline and the subsequent analysis can assist in understanding those attacks and how they are crafted, and as a result, to better prepare to confront them if ever seen again. Our timeline maps key cyber-attacks across the world against the spread of the virus, and also measures such as when lockdowns were put in place. The timeline reveals a pattern which highlights cyber-attacks and campaigns which typically follow events such as announcements of policy. This allows us to track how quickly cyber-attacks and crimes were witnessed as compared to when the first pandemic cases were reported in the area; or, indeed, if attacks preempted any of these events. We expand the timeline to focus on how specific attacks unfolded, how they were crafted and their impact on the UK. To complement these analyses, we reflect more broadly on the range of attacks reported, how they have impacted the workforce and how the workforce may still be at risk. In many ways this timeline analysis also forms a key contribution of our work both in terms of the chronological sequencing of attacks and the representation of campaigns using an accepted attack taxonomy. This therefore provides a platform which aligns with current literature and also provides the foundation which other research can easily build on.

This paper is structured as follows. Section 2 reflects on relevant cyber-attack and cyber-crime literature, and considers how opportunistic attacks have emerged in the past due to real-life crises/incidents. We then present our COVID-19-related cyber-attack timeline in Section 3 as well as a dedicated focus on the United Kingdom as a case study of key-cyber-criminal activity. This is followed by a broader reflection on the attacks (those within and outside of the timeline). In Section 4 we discuss the impact of attacks on those working from home and wider technology risk. Section 5 concludes the paper and outlines directions for future work.

## 2. Literature review

With the broad adoption of digital technologies many facets of society have moved online, from shopping and social interactions to business, industry, and unfortunately, also crime. The latest reports establish that cyber-crime is growing in frequency and severity (Hiscox, 2019), with a prediction to reach $6 trillion by 2021 (up from $3 trillion in 2015) (Cybersecurity Ventures, 2019) and even take on traditional crime in number and cost (Anderson et al., 2019; CBS Netherlands, 2020). Due to its lucrative nature (McGuire, 2018) and low risk level (as cyber-criminals can launch attacks from anywhere across the globe), it is clear that cyber-crime is here to stay.

Cyber-crime, as traditional crime, is often described by the crime triangle (Cross and Shinder, 2008), which specifies that for a cyber-crime to occur, three factors have to exist: a victim, a motive and an opportunity. The victim is the target of the attack, the motive is the aspect driving the criminal to commit the attack, and the opportunity is a chance for the crime to be committed (e.g., it can be an innate vulnerability in the system or an unprotected device). Other models in criminology, such as Routine Activity Theory (RAT) (Yar, 2005) and the fraud triangle (Cressey, 1953) use similar factors to describe crimes, with some replacing the victim by the means of the attacker, which it can be considered otherwise as part of the opportunity.

While attacks today have become more sophisticated and targeted to specific victims depending on attacker's motivation, for example for financial gain, espionage, coercion or revenge; opportunistic untargeted attacks are also very prevalent. We define "opportunistic attacks" as attacks that select the victims based on their susceptibility to be attacked (Dhanjani et al., 2009). Opportunistic attackers pick-up victims that have specific vulnerabilities or use hooks, usually in the form of social engineering, to create those vulnerabilities. Thus, we define as *hook* any mechanism used to mislead a victim into falling prey of an attack.

These hooks take advantage of distraction, time constraints, panic and other human factors to make them work (Nurse, 2019; Stajano and Wilson, 2011). When victims are distracted by what grabs their interest/attention or when they are panicked, they are more susceptible to be deceived. Similarly, time constraints put victims under more pressure which can lead to mistakes and an increased likelihood to fall victim to scams and attacks. Other examples include work pressure, personal change of situation, medical issues, or events that cause deep and traumatic impact in the whole society in general such as fatalities and catastrophes.

Opportunistic attackers always seek to maximise their gain, and therefore, will wait for the best time to launch an attack where conditions fit those mentioned above. A natural disaster, ongoing crisis or significant public event are perfect cases of these conditions (Tysiac, 2018). In the past, several opportunistic attacks have been observed that took advantage of specific incidents; below, we provide few examples:

- Natural disasters: In 2005 Hurricane Katrina caused massive destruction in the city of New Orleans and surrounding areas in the USA (FBI, 2016). Not long after, thousands of fraudulent websites appeared appealing for humanitarian donations, and local citizens received scam emails soliciting personal information to receive possible payouts or government relief efforts. Similar scams and attacks have been witnessed in countless natural disasters since, such as the earthquakes in Japan and Ecuador in 2016 FTC (2016), Hurricane Harvey in 2017 CNET (2017), or the bush fires in Australia in 2020 Elsworthy (2020).
- Notable incidents or events: On 25th June 2009, the tragic death of Michael Jackson dominated news around the world. Only 8 hours after his demise, spam emails claiming knowing the details of the incident were circulating online (Naked Security, 2009). Waves of illegitimate emails echoing the fatality appeared soon after, containing links promising access to unpublished videos and pictures or Jackson's merchandise, that in reality were linked to malicious websites, or emails with malware infected attachments (Hoffman, 2009). Noteworthy public events also attract a range of cyber-crime activities. During the FIFA World Cup in 2018 for instance, there were various attempts to lure individuals with free tickets and giveaways (ESET, 2018). These were, in fact, scams leading to fraud.
- Security incidents: In 2012, 164 million of email addresses and passwords were exposed in a LinkedIn data breach (Jansson, 2018). This data was not disclosed until 4 years later, 2016, when it appeared for sale in the dark market. Soon after that, opportunistic attackers began to launch a series of attacks. Many users experienced scams, such as blackmail and phishing, and some compromised accounts that had not changed their passwords since the breach, were used to send phishing links via private message and InMail (Segura, 2017).

Considering the variety of scams and cyber-attacks occurring around the events above, it is unsurprising that similar attacks have emerged during the ongoing COVID-19 pandemic. The outbreak has caused mass disruption worldwide, with people having to adapt their daily routines to a new reality: working from home, lack of social interactions and physical activity, and fear of not being prepared (NHS, 2020; WHO, 2020). These situations can overwhelm many, and cause stress and anxiety that can increase the chances to be victim of an attack. Also, the sudden change of working contexts, has meant that companies have had to improvise new working structures, potentially leaving corporate assets less protected than before for the sake of interoperability.

Most reports agree that the numbers of scams and malware attacks have significantly risen since the start of the pandemic (Gallagher and Brandt, 2020). There was a reported 600% increase of phishing attacks in March 2020 Shi (2020). The World Economic Forum (WEF) reported that the pandemic led to a 50.1% increase in cyber-attacks and an associated 30,000 cyber-attacks which were specifically COVID-19 related between 31st December 2019 and 14th April 2020 (World Economic Forum, 2020). CGI reported a 30,000% increase in the number of cyber threats specifically due to COVID-19 (Lush, 2020). In the four months between January to April 2020, Interpol detected around *"907,000 spam messages, 737 malware-related incidents, and 48,000 malicious URLs tied to COVID-19"* and found that the *"average ransomware payment for the second quarter of 2020 was $178,254, a 60 percent increase from the first quarter"* (Davis, 2020). The increased ransomware payment demands could indicate that cyber criminals may perceive an increased likelihood of payout because of the extraordinary circumstances presented by the pandemic. To compound these facts, during April 2020, Google reportedly blocked 18 million malware and phishing emails related to the virus daily (Kumaran and Lugani, 2020). To increase likelihood of success, these attacks target sale of goods in high demand (e.g., Personal Protection Equipment (PPE) and coronavirus testing kits and drugs), potentially highly profitable investments in stocks related to COVID-19, and impersonations of representatives of public authorities like WHO and aid scams (Europol, 2020; O'Brien, 2020).

Wide ranges have been specified in terms of the increase in cyber-attacks and in particular specific forms of cyber-attacks such as phishing related and/or ransomware. In some ways, it is not clear as to what proportion of this increase in attacks is specifically due to the pandemic and how these are apportioned by cyber-attack type. Although we can expect that the number of COVID *hooks* in cyber-attacks would rise in the midst of the pandemic, it is difficult to ascertain the level in quantitative terms. It is also challenging to determine the extent to which these *hooks* replaced or supplemented previous *hooks* such as *Brexit*. To illustrate the problem, consider the following. It is difficult to ascertain what proportion of the 50.1% increase reported by the WEF comprised the 30,000 COVID-19 inspired attacks, were there other *hooks* identified, if so what proportion? The figures reported by CGI are from their own experience and there is no reference to figures before the pandemic.

Brute force attacks on the Microsoft Remote Desktop Protocol (RDP) systems have increased as well (Galov, 2020), signaling attacks also on technology, not only on human aspects. It is clear then that attackers are trying to make the most of the disruption caused by pandemic, particularly given it continues to persist. As a consequence, several guidelines and recommendations have also been published to protect against attacks (FTC, 2020; NCSC, 2020a; NIST, 2020). These guidelines are imperative for mitigating the increasing threat, but to strengthen their basis, there first needs to be a core understanding of the cyber-attacks being launched. This paper seeks to address this gap in research and practice by defining a timeline of cyber-attacks and consideration of how they impact citizens and the workforce.

## 3. Timeline of COVID-19 related cyber-attacks

The cyber-crime incidents erupting from the COVID-19 pandemic pose serious threats to the safety and global economy of the world-wide population, hence understanding their mechanisms, as well as the propagation and reach of these threats is essential. Numerous solutions have been proposed in the literature to analyse how such events unfold, ranging from formal definitions to systemic approaches reviewing the nature of threats (Hindy et al., 2018; Kotenko and Chechulin, 2013; Tsakalidis and Vergidis, 2017). While these approaches enable the categorisation of the attack, they often lack the ability to map larger, distributed events such as the ones presented in this manuscript, where numerous events stem from the pandemic are, however, unrelated. To this end, we opted for temporal visualisation, enabling us to map events without compromising the narrative (Kolomiyets et al., 2012). Furthermore, this type of visualisation is used across the cyber-security domain to represent consequent cyber-attacks (Falliere et al., 2011; Horton and DeSimone, 2018; Van Heerden et al., 2016).

### 3.1. *Timeline creation methodology*

In this section, we outline the methodology used to create the timeline. We explain the search terms used to gather relevant COVID-19 cyber-attack data, the data sources (search engines) utilised, the sources of information we chose to focus on, and types of attack. We also acknowledge the potential limitations of the work.

#### 3.1.1. *Nomenclature*

We explore a range of cyber-attacks which have occurred during the COVID-19 pandemic. The novel coronavirus has been referred to by several different terms in the English-speaking world, including Coronavirus, COVID19, COVID-19, 2019-nCoV, and SARS-CoV-2. We use the term COVID-19 to refer to the virus, which falls in line with terminology used by the World Health Organisation (WHO) (2020b).

#### 3.1.2. *Construction of the timeline*

To aid in the construction of the timeline, we initially conducted a number of searches to identify cyber-attacks closely linked to the pandemic. These cyber-attacks were categorised by attack type, delivery method, and were ordered by date. The information gathered has been collated and is presented in Fig. 2 which serves as a baseline for the construction of Table 1.

Information presented in the timeline includes the date China alerted the WHO about the virus, the date the pandemic was officially declared, and cyber-attacks which specifically relate to hospitals or medicine. Additionally, key countries involved in the pandemic were identified, and for those, we present the first identified case, the date lockdown was implemented, and the first cyber-attack they suffered. The table seeks to examine a sub-set of the information from the timeline.

Furthermore, we have chosen to include a number of sources offering reports of attacks. The sources are a mixture of reputable news outlets (such as Reuters, and the BBC), blog articles, security company reports, and social media posts. Though blog articles and social media posts are not considered to be an academic source, in the context of this research where we are examining an emerging threat, they offer important insights into trends of cyber-attacks. It is also important to note that cyber-attacks may first be presented in these domains, before being highlighted by mainstream media outlets. With regards to the inclusion of news reports in the table of attacks and subsequent timeline, it should be acknowledged that these attacks are being presented through a journalistic lens, and as such may be written in an attempt to grab headlines. Nevertheless, these reported cyber-attacks still pose a tangible threat to the general public during the COVID-19 pandemic. The timeline seeks to provide an overview of attacks which have occurred.

The review of reports was performed from mid-March to mid-May 2020. The timeline limits cyber-attacks to those experienced by 31st March. This is because we reached what we believed to be a saturation point comprising a sufficient number of cyber-attacks to be representative. Following the conclusion of the search, the earliest reported attack was on 6th January 2020 (Henderson et al., 2020), whilst the most recently listed attack in the timeline was 31st March 2020 (O’Donnell, 2020). The most recently listed attack in the table was 13th May 2020 (CNET, 2020). The table progresses the time period a bit further as it intends to provide more detail in regards to cyber-attacks experienced during this time. Sources were gathered from a number of locations. The criteria used to locate reports have been defined below and are presented in a similar way to existing reviews in cyber security literature (Chockalingam et al., 2017; Shepherd and Renaud, 2018). The structure of the timeline is described in further detail in Section 3.2.

*Search engines* Several search engines were used in the creation of the table and timeline. These were- Google[1] (US-based and dominates the search engine market share), Baidu[2] (Chinese-based search provider), Qwant[3] (French-based search engine with a focus on privacy), and DuckDuckGo[4] (US-based search engine with a focus on privacy).

*Keywords used* A variety of keywords were used when collating reports of cyber-attacks and cyber-crime. In addition to English language reports, we also searched for results in Chinese, Japanese, French, Italian and Spanish. We limited our scope to focus on countries which reported large clusters of COVID-19 cases during the early stages of the pandemic.

Non-English terms were translated using the Google Translate service (Google, 2020) and additional independent sources were used as a means of validating the translation. When fo-

[1] www.google.com
[2] www.baidu.com
[3] www.qwant.com
[4] www.duckduckgo.com

**Table 1 – Descriptions of COVID-19 related cyber-attacks.**

| ID | Ref. | Country | Attack type | Description | Article date | Attack date |
|---|---|---|---|---|---|---|
| 1 | Henderson et al. (2020) | China | P.M | Vietnam accused of launching a *METALJACK* phishing campaign against the Wuhan district offices | 22/04 | 06/01 |
| 2 | AON (2020) | Global | P.M | International reports that both phishing and smishing campaigns are taking place | 19/01 | - |
| 3 | Forbes (2020) | China, Mongolia | P.M | Chinese hackers accused of distributing the *Vicious Panda* malware to Mongolia through emails purporting to come from the Mongolian ministry of affairs | 12/03 | 20/01 |
| 4 | F-Secure (2020) | Phillipines | P.M.F | *REMCOS* malware distributed to Phillipino citizens | 13/03 | 23/01 |
| 5 | Kaspersky (2020) | Singapore | P | Phishing campaign steals email log-in credentials | 28/01 | - |
| 6 | Walter (2020) | Japan | P.M.F | Safety measures phishing campaign distributes *Emotet* malware | 28/01 | 28/01 |
| 7 | smzdm.com (2020) | China | P.M.F | ’Safety measure’ email from a ’Singaporian specialist’ distributes *Emotet* malware | 06/02 | 29/01 |
| 8 | Kaspersky (2020) | USA | P | Email purporting list of COVID-19 cases in victim’s city takes user to website which steals credentials | 11/02 | 31/01 |
| 9 | CSDN (2020) | China | H | DoS on epidemic prevention units | 09/02 | 02/02 |
| 10 | CSDN (2020) | China | P | Phishing campaign steals email log-in credentials | 09/02 | 02/02 |
| 11 | TechRepublic (2020) | World | P.M.F | First cases of *AZORult* a data theft malware | 10/02 | - |
| 12 | cqgbxa.com (2020) | China | P.M | Email purporting specialist safety measures from WHO prompts malware download | 12/02 | - |
| 13 | F-Secure (2020) | Vietnam | P.M | *LOKIBOT* malware spread through email purporting incorrect invoice payment | 13/03 | 03/02 |
| 14 | Patranobis (2020) | China | P.Ph | Phishing attack on medical groups in China (from India) | 06/02 | 06/02 |
| 15 | freebuf.com (2020) | China | P.M.E | Distribution of *CXK-NMSL* ransomware through COVID-19 themed emails | 18/02 | 09/02 |
| 16 | freebuf.com (2020) | China | P.M.E | Distribution of *Dharma/Crysis* ransomware through COVID-19 themed emails | 18/02 | 13/02 |
| 17 | F-Secure (2020) | Italy | P.M | *Trickbot* malware distributed through email | 13/03 | 02/03 |
| 18 | Stonefly (2020) | Global | P.M.F | MBR wiper malware disguised as contact tracing information | 04/03 | - |
| 19 | F-Secure (2020) | USA | P.M | *FORMBOOK* malware distributed through email purporting parcel shipment advice | 13/03 | 08/03 |
| 20 | The Register (2020) | USA | M | Health systems in Champaign Urbana Public Health District (Illinois) affected by the *netwalker* ransomware | 12/03 | 10/03 |
| 21 | F-Secure (2020) | Spain | P.M | Email purports COVID-19 remedy as mooted by Israeli scientists days in advance | 13/03 | 10/03 |
| 22 | Millman (2020) | Czech | H | Cyber-attack on Czech hospital | 14/03 | 14/03 |
| 23 | Stein and Jacobs (2020) | USA | H | Denial of Service on U.S. Health Agency | 16/03 | - |
| 24 | Rosso (2020) | Libya | P.M | Corona live 1.1 is the *SpyMax* malware which in this case is a trojanised app which exfiltrates user data | 18/03 | - |
| 25 | Desai (2020) | World | P.M | Corona mask offer installs what appears to be a harmless malware which distributes an SMS to all contacts. Presumably an update to the app will mobilise the malware | 19/03 | - |
| 26 | FitzGerald (2020) | Global | P.E | Extortion campaign threatens to infect the recipient with COVID-19 unless a $4,000 bitcoin payment is made | 17/04 | 20/03 |
| 27 | Murica Today (2020) | Spain | P.M | *Netwalker* ransomware attack disguised as an email advising on restroom use | 24/03 | - |
| 28 | Koenig (2020) | USA | P.M | SMS asks recipient to take a mandatory COVID-19 ‘preparation’ test, points to website which downloads malware | 24/03 | 24/03 |
| 29 | Glos Safe Cyber (2020) | UK | P.M | SMS informs recipient to stay at home with a link for more information. Link directs recipient to a malware ridden website | 24/03 | - |

(*continued on next page*)

**Table 1 (*continued*)**

| | | | | | | |
|---|---|---|---|---|---|---|
| 30 | Rodger (2020) | UK | P.Ph.F | Free school meal SMS directs recipient to website which steals payment credentials | 25/03 | 24-03 |
| 31 | Muncaster (2020) | World | M.F | *Ginp* Trojan distributed in an Android app. App charges € 0.75 for information on infected persons in the recipients region. In actual fact, it steals the payment information | 25/03 | - |
| 32 | O'Donnell (2020) | Global | P | Skype credentials stolen through a crafted phishing campaign | 23/04 | 31/03 |
| 33 | Strawbridge (2020) | World | P.Ph.M.F | Free Netflix offer directs users to a malware ridden website | 27/03 | - |
| 34 | de Seguridad del Internauta (2020a) | Spain | P.F | Fake SMS asking to introduce bank details to get the furlough pay | 27/03 | - |
| 35 | Chadwick (2020) | UK | M | Fake NHS website gathers user credentials | 28/04 | - |
| 36 | Magazine (2020) | UK | P.M | Email purports to offer job retention payment as per the UK governmental announcement | 30/04 | 19/04 |
| 37 | Abrams (2020) | Global | M | *Coronalocker* locks a computer and appears to cause rather more annoyance than any real damage | 21/04 | - |
| 38 | Dark Reading (2020) | Global | P.M | Docusign recipients directed to fake website offering COVID-19 information | 08/05 | - |
| 39 | Smithers (2020) | UK | P.M | Recipients are directed to a fake track and trace website which collects user credentials | 13/05 | - |

key: P:Phishing (or smishing); Ph:Pharming; E:Extortion; M:Malware; F:Financial fraud; H:Hacking.

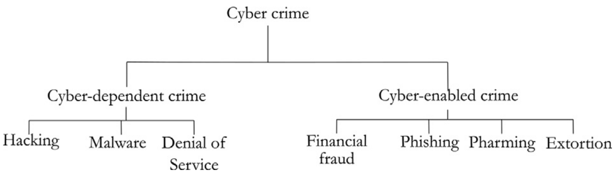


**Fig. 1 – Cyber-dependent and cyber-enabled crimes CPS (2019).**

cussing on the virus itself, the following key words were used: SARS-CoV-2, Covid, COVID19, Coronavirus, 冠状病毒 (Chinese translation for Coronavirus, confirmed by the World Health Organisation (WHO), 2020a), コロナウイルス (Japanese translation for Coronavirus, confirmed by The Ministry of Health, Labour and Welfare, 2020).

When searching for cyber-attacks, the following key phrases were used: 网络攻击 (Chinese translation means Network Attack Wang et al., 2009 or Cyber Attack World Health Organisation (WHO), 2020d), サイバー攻撃 (Japanese translation for Cyber Attack or Hacking Attack Jisho, 2020), Attaque Informatique (French translation for Computer Attack Le Parisien, 2020), Attacco Informatico (Italian translation for Cyber Attack la Repubblica, 2020), Ataque Informático (Spanish translation for Computer Attack Pais, 2020) or Ciberataque (Spanish translation for Cyber Attack de Seguridad del Internauta, 2020b).

*Time range* We attempted to find the earliest reported cyber-attack which was associated with the COVID-19 pandemic. To allow for development of the timeline, and analysis of findings, mid-May 2020 was defined as a cut-off point, with the most recent news article being dated 13th May 2020 (Smithers, 2020).

*Exclusion criteria* Although we have created a comprehensive table and timeline, a number of results were excluded from the research. These included results which (a) were behind a paywall, (b) required account creation before full article was displayed, (c) were duplicates of existing news reports, and d) could not be translated.

### 3.1.3. *Types of cyber-attacks*

To guide our analysis and the creation of a timeline of COVID-19-related cyber-attacks, we decided to define attacks based on their types. This allowed us to examine the prominence in certain types of attacks. Although there exist numerous taxonomies relating to attacks and cyber-crimes (e.g., Cebula and Young, 2010; Ciardhuáin, 2004; Nurse, 2019), there exists no universally accepted model (Hindy et al., 2020). In this work therefore, we relied on the UK's Crown Prosecution Service (CPS) categorisation of cyber-crime. This definition includes cyber security by default and has inspired many international definitions of cyber-crime.

The CPS guidelines categorise cyber-crime into two broad categories: *cyber-dependent* and *cyber-enabled* crimes (CPS, 2019). A cyber-dependent crime is an offence, *"that can only be committed using a computer, computer networks or other form of information communications technology (ICT)"* (McGuire and Dowling, 2013a). Cyber-enabled crimes are, *"traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT)"* (McGuire and Dowling, 2013b). These categories as well as examples of their subcategories can be seen in Fig. 1. Some of the elements described by CPS are often interlinked in a cyber-attack. For instance, a phishing email or text message (e.g., SMS or WhatsApp) might be used to lure a victim to a fraudulent website. The website then may gather personal data which is used to commit financial fraud, or it may install malware (more specifically, ransomware) which is then used to commit extortion. This notion of cyber-attack sequences is explained in further detail in Section 3.2.

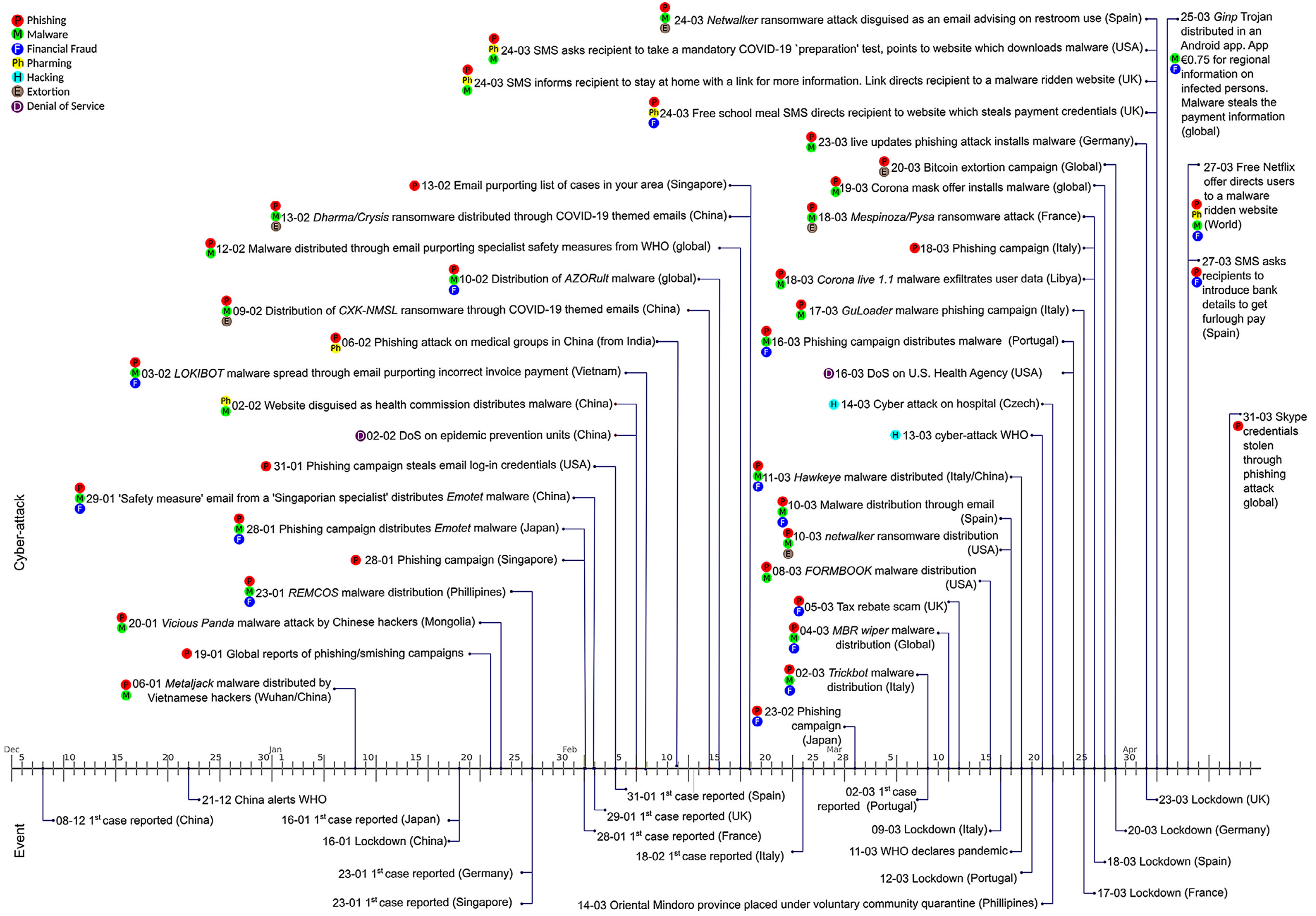

P Phishing
M Malware
F Financial Fraud
Ph Pharming
H Hacking
E Extortion
D Denial of Service
Cyber-attack
Event
P M E 24-03 Netwalker ransomware attack disguised as an email advising on restroom use (Spain)
P Ph M 24-03 SMS asks recipient to take a mandatory COVID-19 `preparation' test, points to website which downloads malware (USA)
P Ph M 24-03 SMS informs recipient to stay at home with a link for more information. Link directs recipient to a malware ridden website (UK)
P Ph F 24-03 Free school meal SMS directs recipient to website which steals payment credentials (UK)
P M 23-03 live updates phishing attack installs malware (Germany)
P E 20-03 Bitcoin extortion campaign (Global)
P M 19-03 Corona mask offer installs malware (global)
P M E 18-03 Mespinoza/Pysa ransomware attack (France)
P 18-03 Phishing campaign (Italy)
P M 18-03 Corona live 1.1 malware exfiltrates user data (Libya)
P M 17-03 GuLoader malware phishing campaign (Italy)
P M F 16-03 Phishing campaign distributes malware (Portugal)
D 16-03 DoS on U.S. Health Agency (USA)
H 14-03 Cyber attack on hospital (Czech)
H 13-03 cyber-attack WHO
P M F 11-03 Hawkeye malware distributed (Italy/China)
P M F 10-03 Malware distribution through email (Spain)
P M E 10-03 netwalker ransomware distribution (USA)
P M 08-03 FORMBOOK malware distribution (USA)
P F 05-03 Tax rebate scam (UK)
P M F 04-03 MBR wiper malware distribution (Global)
P M F 02-03 Trickbot malware distribution (Italy)
P F 23-02 Phishing campaign (Japan)
M F 25-03 Ginp Trojan distributed in an Android app. App €0.75 for regional information on infected persons. Malware steals the payment information (global)
P Ph M F 27-03 Free Netflix offer directs users to a malware ridden website (World)
P F 27-03 SMS asks recipients to introduce bank details to get furlough pay (Spain)
P 31-03 Skype credentials stolen through phishing attack global)
P 13-02 Email purporting list of cases in your area (Singapore)
P M E 13-02 Dharma/Crysis ransomware distributed through COVID-19 themed emails (China)
P M 12-02 Malware distributed through email purporting specialist safety measures from WHO (global)
P M F 10-02 Distribution of AZORult malware (global)
P M E 09-02 Distribution of CXK-NMSL ransomware through COVID-19 themed emails (China)
P Ph 06-02 Phishing attack on medical groups in China (from India)
P M F 03-02 LOKIBOT malware spread through email purporting incorrect invoice payment (Vietnam)
Ph M 02-02 Website disguised as health commission distributes malware (China)
D 02-02 DoS on epidemic prevention units (China)
P 31-01 Phishing campaign steals email log-in credentials (USA)
P M F 29-01 'Safety measure' email from a 'Singaporian specialist' distributes Emotet malware (China)
P M F 28-01 Phishing campaign distributes Emotet malware (Japan)
P 28-01 Phishing campaign (Singapore)
P M F 23-01 REMCOS malware distribution (Phillipines)
P M 20-01 Vicious Panda malware attack by Chinese hackers (Mongolia)
P 19-01 Global reports of phishing/smishing campaigns
P M 06-01 Metaljack malware distributed by Vietnamese hackers (Wuhan/China)
Dec 5 10 15 20 25 30
Jan 1 5 10 15 20 25 30
Feb 5 10 15 20 25 28
Mar 5 10 15 20 25 30
Apr
08-12 1st case reported (China)
21-12 China alerts WHO
16-01 1st case reported (Japan)
16-01 Lockdown (China)
23-01 1st case reported (Germany)
23-01 1st case reported (Singapore)
31-01 1st case reported (Spain)
29-01 1st case reported (UK)
28-01 1st case reported (France)
18-02 1st case reported (Italy)
14-03 Oriental Mindoro province placed under voluntary community quarantine (Phillipines)
02-03 1st case reported (Portugal)
09-03 Lockdown (Italy)
11-03 WHO declares pandemic
12-03 Lockdown (Portugal)
23-03 Lockdown (UK)
20-03 Lockdown (Germany)
18-03 Lockdown (Spain)
17-03 Lockdown (France)

**Fig. 2 – Timeline of key events related to cyber-attacks and the COVID-19 pandemic.**

Similarly Denial of Service (DoS) attacks are increasingly used by cyber-criminals to distract (or, act as 'smokescreens' for) businesses during hacking attempts (Bellekens et al., 2019; Kaspersky, 2016). In what follows, we consider the types of these attacks and reflect on how they have been launched, including any human factors or technical aspects (e.g., vulnerabilities) they attempt to exploit.

Phishing, or Social Engineering more broadly, includes attempts by illegitimate parties to convince individuals to perform an action (e.g., share information or visit a website) under the pretence that they are engaging with a legitimate party. Quite often email messages are used, occasionally SMS or WhatsApp messages are used (referred to as smishing). Pharming is similar to phishing but instead of deceiving users into visiting malicious sites, attackers rely on compromising systems (e.g., the user's device or DNS servers) to redirect individuals to illegitimate sites. This type of attack is less common in general, as it requires more access or technical capabilities. Financial fraud generally involves deceiving individuals or organisations using technology for some financial gain to the attacker or criminal. Extortion refers to actions that force, threaten or coerce individuals to perform some actions, most commonly, releasing finances.

Hacking, Malware and Denial of Service (DoS) attacks are forms of crime that are often favoured by more technical attackers. Hacking involves compromising the confidentiality or integrity of a system, and requires a reasonable amout of skill; its techniques can involve exploiting system vulnerabilities to break into systems. Malware refers to malicious software and can be used for disrupting services, extracting data and a range of other attacks. Ransomware is one of the most common type of malware today (Fruhlinger, 2020; Malwarebytes, 2020), and combines malware with extortion attempts. DoS attacks target system availability and work by flooding key services with illegitimate requests. The goal here is to consume the bandwidth used for legitimate server requests, and eventually force the server offline.

These types of attack provide the foundation for our analysis in the timeline and how we approach our discussion in later part of this research.

#### 3.1.4. *Limitations of the table*

Within Table 1, two columns referring to dates are provided. The first column "Article Date" refers to the date the reference was initially published. We acknowledge that in some cases, the web pages linked to the references continued to be updated with information following its inclusion with the paper. The table has been ordered by "Article Date" to provide a consistent chronological representation of events.

We have also provided a second column,"Attack Date". When examining each reference, if a specific date was provided as to when the attack was executed, it was included. The rational behind including the attack date and report date is that an attack may not surface until several days after it has been carried out.

#### 3.1.5. *Limitations of the timeline*

Two types of cyber-attack reports are considered within this manuscript, those which describe cyber-attacks without providing the date of the attack and those which describe cyber-attacks and include the date of the perpetration. When the date of the attack is not included, the date provided in the timeline refers to the date of the publication. The rationale behind the inclusion of both types of reports is based on providing a chronological representation of events. Furthermore, while the table provides an extensive overview of the threat landscape, it is by no means an exhaustive list of all the attacks carried out in relation to the pandemic, as gathering such information would not be possible in this context due to the lack and quality of reporting, the number of targeted incidents, the number of incidents targeted at the general public, the global coverage of the pandemic and the number of malicious actors carrying out these attacks.

However, despite these limitations we have explored all resources available to depict the threat landscape as accurately as possible.

### 3.2. *The timeline*

In this section, we examine the cyber-attacks in further detail. Fig. 2 provides a detailed temporal representation of the chain of key cyber-attacks induced by the COVID-19 pandemic. The timeline includes the first reported cases in China, Japan, Germany, Singapore, Spain, UK, France, Italy, and Portugal and then the subsequent lockdown announcements. The timeline presents 44 cyber-attacks categorised using the CPS taxonomy described in Section 3.1.3 and abbreviated as: *P:phishing* (or *smishing*), *M:malware. Ph:pharming, E:extortion, H:hacking, D:denial of service* and *F:financial fraud*. The events related to the crisis were validated against WHO timeline of events to ensure an accurate temporal reproduction.

Table 1 describes a number of cyber-attacks in further detail. Within the table, cyber-attacks have been organised by attack date. If the attack date was not available within the reference, then the article date has been used. The target-country of each cyber-attack has been listed, alongside a brief description of the methods involved. Finally, the attack type has also been classified in accordance with the CPS taxonomy described earlier where it has been mentioned within the reference.

Both the figure and the table present specific cyber-attacks and incidents and exclude: general advisories (e.g. from governmental departments), general discussions and summaries of attacks, and detailed explanations of techniques and approaches utilised by the attackers.

### 3.3. *COVID-19 cyber-attacks in the United Kingdom*

The extent of the cyber-security related problems faced in the UK was quite exceptional, and in this section we use the UK as a case study to analyse COVID-19 related cybercrime. The discussion herein demonstrates that as expected and outlined above, there was a loose correlation between policy/news announcements and associated cyber-crime campaigns. The analysis presented herein focuses only on cybercrime events specific to the UK. So for example, although many of the incidents identified in the previous section and particularly in Mimecast (2020) are global cyber-attacks, the discussion herein ignores these. Consequently, numerous announcements purportedly coming from reputed or-

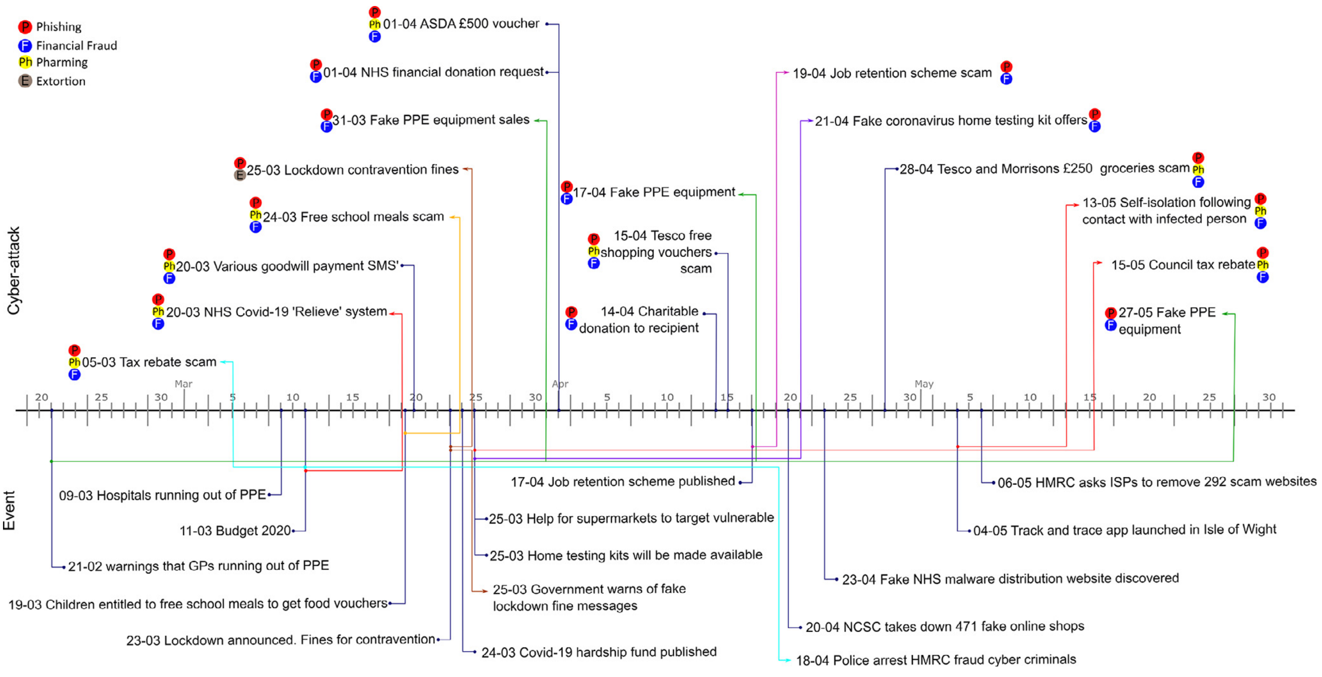


**Fig. 3 – UK timeline.**

ganisations such as WHO and a plethora of malware which reached UK citizens is ignored as these were not UK specific issues.

Indications of the extent of the UK cyber-crime incident problem experienced during the pandemic are provided by the reported level of suspect emails and fraud reported. By early May (07-05-20), more than 160,000 'suspect' emails had been reported to the NCSC (2020b) and by the end of May (29-05-20), £4.6 m had been lost to COVID-19 related scams with around 11,206 victims of phishing and / or smishing campaigns (Sky News, 2020). In response, the National Cyber Security Centre (NCSC) took down 471 fake online shops (Tidy, 2020) and HMRC (Her Majesty's Revenue and Customs) took down 292 fake websites (Hill, 2020).

The timeline in Fig. 3 shows a series of UK specific events and cyber-crime incidents. The timeline indicates a direct and inverse correlation between announcements and incidents.

*Direct correlations* are instances where perpetrators appear to follow announcements or events, they may have drawn on these events and carefully configured cyber-attacks around policy context. These are shown in the figure with a solid coloured connecting arrow.

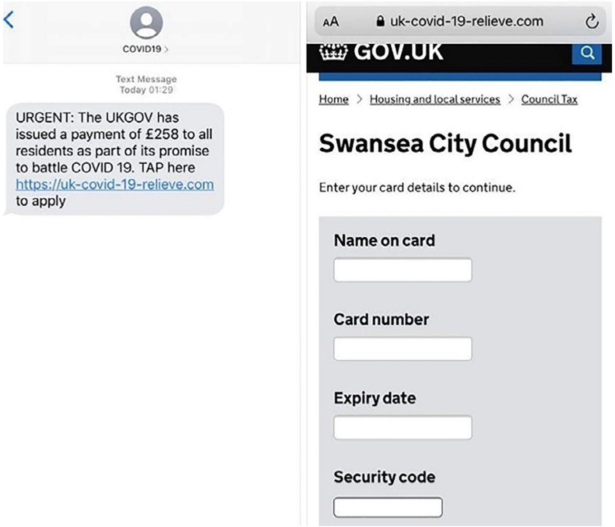
*Inverse correlations* are instances where an incident has no clear correlation with an event or announcement. Although inverse correlations do not appear to have a direct correlation, these may exist because a number of events were being actively highlighted in the media. For example, the issue of personal protective equipment (PPE) was in active discussion well before the UK government gave this priority consideration. Similarly, the likelihood of a tax rebate scheme was in active consideration in early March before the budget announcement on 11-03-20. The first tax rebate phishing campaigns were in active circulation before the budget announcement. In both cases, we should emphasise that these are loose correlations and more work needs to be done in terms of whether a predictive model can be built using this data and data around the world as examples.

On 11th March 2020, the UK government made a number of important budgetary announcements (Government, 2020) which included: a £5bn emergency response fund to support the NHS and other public services in England; an entitlement to statutory sick pay for individuals advised to self-isolate; a contributory Employment Support Allowance for self-employed workers; a £500m hardship fund for councils to help the most vulnerable in their areas; a COVID-19 Business Interruption Loan Scheme for small firms; and the abolishment of business rates for certain companies.

Soon after, the government continued to make announcements to support the citizenry and economy. These announcements included: a scheme to support children entitled to receive free school meals (19-03-20); a hardship fund (24-03-20); help for supermarkets to target vulnerable people (25-03-20); the potential availability of home test kits (25-03-20); a job retention scheme (17-04-20); and the launch of the much awaited *track and trace* app (04-05-20).

Events such as these increase the likelihood of a positive response to a cyber-criminal campaign and perpetrators are very likely to hook onto events. Although there appears to be a link between some of the events and incidents, a number of scams cannot easily be traced to a single event or announcement. Examples of this include a *goodwill* payment of £250 (21-03-20), an NHS financial donation request (02-04-20), vouchers for UK supermarkets (02-04-20, 15-04-20, 28-04-20), and a charitable donation to the recipient. None of these events have associated governmental announcements or even general public speculation.

Examples supporting our notion of a correlation between events and cyber-security campaigns are provided in


COVID19 >

Text Message
Today 01:29

URGENT: The UKGOV has issued a payment of £258 to all residents as part of its promise to battle COVID 19. TAP here https://uk-covid-19-relieve.com to apply

AA uk-covid-19-relieve.com

GOV.UK

Home > Housing and local services > Council Tax

Swansea City Council

Enter your card details to continue.

Name on card

Card number

Expiry date

Security code

**Fig. 4 – The COVID-19-relieve scam (Swansea Council, 2020).**

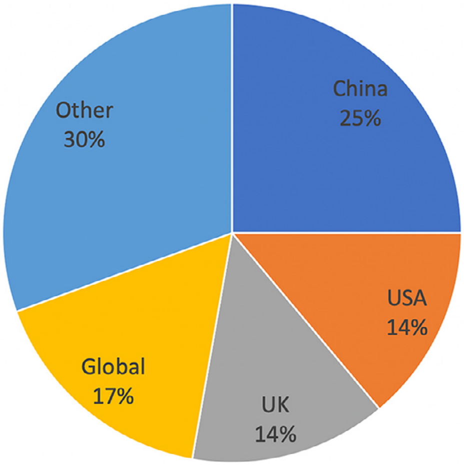


**Fig. 5 – Cyber-attack distribution across countries examined.**

Table 2 and illustrated in Fig. 3. These examples indicate a loose correlation between events and cyber-criminal campaigns. Many of the cases outlined in Table 2 and Fig. 3, were very simple. Potential victims were provided URLs through email, SMS, or Whatsapp. An example of this is provided in Fig. 4. In this case, the URL pointed to a fake institutional website which requests credit/debit card details. Although there are elements of this process which are obviously suspicious to a more experienced computer user, for example, spelling errors (*relieve* instead of *relief* in the COVID-19 relief scam), suspect reply email addresses and clearly incorrect URLs, these are not immediately obvious to many users.

### 3.4. *Analysis of cyber-attacks and associated risks*

The timeline shown in Fig. 2 and the UK case study above creates an ideal platform through which to analyse the cyber-attacks that have occurred in light of the pandemic. From the point that the first case was announced in China (08-12-19), the first reported COVID-19 inspired cyber-attack took 30 days. The next reported cyber-attack was 14 days (19-01-20). From this point onwards, it is clear that the timeframe between events and cyber-attacks reduces dramatically.

The 43 cyber-attacks presented in the timeline can be further categorised as follows:

- 37 (86%) involved phishing and / or smishing
- 2 (5%) involved hacking
- 2 (5%) involved denial of service
- 28 (65%) involved malware
- 15 (34%) involved financial fraud
- 6 (13%) involved pharming
- 6 (15%) involved extortion

Whilst this analysis is useful, the sequence of events in the complete attack can also provide key attack insights. The timeline reveals these sequences and shows the complete campaign comprising of, for instance, the distribution of malware (*m*) through phishing (*p*) which steals payment credentials which are used for financial fraud (*f*). We can describe this cyber-attack sequence as p,m,f. Analysing cyber-attacks in this way is important because this indicates multiple points in a cyber-attack where protections could be applied. The timeline reveals the following cyber-attack sequences:

- p,m: *n*=8, *19%*
- p,m,f: *n*=10, *23%*
- ph,m: *n*=1, *2%*
- p,ph: *n*=1, *2%*
- p.m.e: *n*=5, *12%*
- p,ph,m: *n*=2, *5%*
- p,ph,f: *n*=1, *2%*
- p,e: *n*=1, *2%*
- p,ph,m,f: *n*=1, *2%*

This analysis does not include the sequence of events that took place in the two hacking and two denial of service incidents. It should be noted that although financial fraud is the most likely goal in most of the cyber-attacks described in the timeline, financial fraud was only recorded in the timeline where reports have clearly indicated that this was the outcome of a cyber-attack. In reality, the p,m,f and p,ph,f cases are likely to be higher.

Fig. 5 provides a summary of the countries that were the target of early cyber-attacks during the pandemic, organised by attack date. As shown, China and the USA account for 39% of the attacks reported. It is also clear from Table 1 that both of these countries were primary target from the start of the pandemic. The attacks then spread to the United Kingdom and more other countries. By March 2020 however, a vast majority of the attacks are targeted at the whole world, with a reminder of attacks specifically focused at events in a single country, such as tax rebates due to COVID-19, or contact tracing phishing messages.

It is useful to consider this in the context of UK specific cyber-attacks. This examination reveals that phishing was a component of all ($n = 17$) the cyber-attacks analysed. One in-

**Table 2 – Selected correlations between events and cyber-criminal campaigns.**

| Event date | Event | Incident date & type | Incident |
|---|---|---|---|
| 21-02-20, | Doctors warn GPs are running out of PPE; | 17-04-20 `p,ph,f` | Fake PPE offers through email. Link to URLs which capture credit card and other details |
| 09-03-20 | Hospitals running out of PPE | 27-05-20 `p,ph,f` | |
| 11-03-20 | Government announces a range of financial assistance packages in the budget | 20-03-20 `p,ph,f` | Smishing campaign promising a COVID-19 financial relief payment. Respondents are directed to a fake *gov.uk* website which requests credit/debit card details |
| 19-03-20 | Government announces a scheme which entitles children who qualify for a free school meal to a food voucher or alternatives if they are not able to continue attending school. | 24-03-20 `p,ph,f` | A smishing campaign which targeted parents with a promise of help with their free school meals in return for banking details. Banking details are defrauded |
| 23-03-20 | Lockdown announced. £60 contravention fine, later (10-05-20) increased to £100 | 27-03-20 `p,e` | Lockdown contravention SMS |
| 24-03-20 | COVID-19 hardship fund enables councils to reduce council tax bills by £150 for residents of working age and who have had their bill reduced by an award of council tax reduction | 15-05-20 `p,ph,f` | Council tax rebate scam |
| 25-03-20 | Government announce intention to make home testing kits available | 31-03-20 `p,f`,<br>17-04-20 `p,f`,<br>27-05-20 `p,f` | Phishing campaigns in England and Scotland direct victims to fake websites which claim to sell PPE equipment |
| 17-04-20 | Government announces job retention scheme | 19-04-20 `p,f` | Fake job retention scheme phishing campaign. |

volved extortion as the final goal, the remaining 16 involved financial fraud. Nine cyber-attacks comprised the sequence: `p,ph,f`, seven comprised the sequence `p,f`, the remaining one comprised of `p,e`.

It is notable that although an NHS malware distribution website was discovered and removed on 23-04, none of the cyber-attacks we analysed appeared to involve malware in the same way that the global analysis reveals. There may be a number of reasons for this. Launching a malware connected campaign requires more sophistication and time. There may be less opportunity to directly connect it to a specific event or announcement. The time delay between some of the announcements and the associated campaigns was remarkably short. For instance, the time delay between the lockdown announcement (23-03-20) and the 'lockdown contravention fine' (25-03-20) was 2 days, and the time delay between the job retention scheme announcement (17-04-20) and the job retention scam (19-04-20) was also two days.

To reflect more generally on the cyber-attacks discovered, we can see that phishing (including smishing) were, by far, the most common based on our analysis. In total, it was involved in 86% of the global attacks. This is however, unsurprising, as phishing attempts are low in cost and have reasonable success rates. In the case of COVID-19, these included attempts at impersonating government organisations, the WHO, the UK's National Health Service (NHS), airlines, supermarkets and communication technology providers. The specific context of the attacks can be slightly different however the underlying techniques, and the end goal is identical.

For instance, in one email impersonating the WHO, attackers attach a zip file which they claim contains an e-book that provides, "*the complete research/origin of the corona-virus and the recommended guide to follow to protect yourselves and others*" (Bellekens et al., 2016a; MalwareBytes, 2020). Moreover, they state: "*You are now receiving this email because your life count as everyone lives count*". Here, attackers are using the branding of WHO, posing as helpful (the remainder of the email contains legitimate guidance), and appealing to people's emotions in crafting their attack email (Iuga et al., 2016; Nurse, 2019). Similar techniques can be seen in a fake NHS website created by criminals detected online, which possesses identical branding but is riddled with malware (Daily Mail, 2020), and a malicious website containing malware which also presents the legitimate Johns Hopkins University COVID-19 dashboard (Krebs on Security, 2020). It is notable that the fake WHO email contains spelling/grammatical errors. The discussion in Section 3.3 provides further specific examples of this.

To further increase the likely success of phishing attacks cyber-criminals have been identified registering large numbers of website domains containing the words ‘covid’ and ‘coronavirus’ (Check Point, 2020). Such domains are likely to be believable, and therefore accessed, especially if paired with reputable wording such as WHO or Centers for Disease Control and Prevention (CDC) or key words (e.g., Corona-virusapps.com, anticovid19-pharmacy.com, which have been highlighted as in use Forbes, 2020)). Communications platforms, such as Zoom, Microsoft and Google, have also been impersonated, both through emails and domain names (Check Point, 2020). This is noteworthy given the fact that these are the primary technologies used by millions across the world to communicate, both for work and pleasure. These facts, in combination with convincing social engineering emails, text messages and links, provide several notable avenues for criminals to attack. Pharming attacks were much less common but did occur in 13% of cases. As can be seen Table 1, these often occur alongside other attacks.

COVID-19-inspired fraud has leveraged governmental/scientific announcements to exploit the anxieties of users and seek financial benefit. From our analysis, fraud was typically committed through phishing and email attacks—we also can see this in our sequencing above. In one case, criminals posed as the CDC in an email and politely requested donations to develop a vaccine, and also that any payments be made in Bitcoin (Tidy, 2020). Typical phishing techniques were used, but on this occasion these included requests for money: “*Funding of the above project is quite a huge cost and we plead for your good will donation, nothing is too small*”. A notable point about this particular attack is that it also ask recipients to share the message with as many people as possible. This is concerning given that people are more likely to trust emails they believe have been vetted by close ones (Nurse, 2019).

There were a range of other fraud attempts, largely based on threats or appeals. For instance, our analysis identified offers of investment in companies claiming to prevent, detect or cure COVID-19, and investment in schemes/trading options which enable users to take advantage of a possible COVID-19 driven economic downturn (US Department of Justice (DOJ), 2020). There were offers of cures, vaccines, and advice on effective treatments for the virus. The Food and Drugs Administration (FDA) issued 16 warning letters between 6th March and 1st April 2020 to companies *“for selling fraudulent products with claims to prevent, treat, mitigate, diagnose or cure”* COVID-19 (Bellekens et al., 2016b; Food and Drugs Administration (FDA), 2020). The European Anti-Fraud Office (OLAF) has responded to the flood of fake products online by opening an enquiry concerning imports of fake products due to COVID-19 pandemic (European Anti-Fraud Office (OLAF), 2020), and in the UK, the Medical and Healthcare products Regulatory Agency (MHRA) has began investigating bogus or unlicensed medical devices currently being traded through unauthorised and unregulated websites (UK Government, 2020).

Extortion attacks were witnessed in our analysis but were less prevalent (appearing in only 13% of cases) compared to the others above. The most prominent case of this attack was an extortion email threatening to infect the recipient and their family members with COVID-19 unless a Bitcoin payment is made (Sophos, 2020). To increase the believability of the message, it included the name of the individual and one of their passwords (likely gathered from a previous password breach). After demanding money, the message goes on to state: “*If I do not get the payment, I will infect every member of your family with coronavirus*”. This attempts to use fear to motivate individuals to pay, and uses passwords (i.e., items that are personal) to build confidence in the criminal’s message.

Malware related to COVID-19 increased in prominence during the pandemic and impacted individuals and organisations across the world. As shown above, it was the second largest cyber-attack type, appearing in 65% of cases. *Vicious panda* and *MBR Loader* were the only new malware discovered in this period. The remaining malware attacks were variants of existing malware and included *Metaljack, REMCOS, Emotet, LOKIBOT, CXK-NMSL, Dharma-Crysis, Netwalker, Mespinoza/Pysa, SpyMax* (disguised as the *Corona live 1.1* app) *GuLoader, Hawkeye, FORMBOOK, Trickbot* and *Ginp*. Ransomware, in particular, was a notable threat and an example of such was COVIDLock, an Android app disguised as a heat map which acted as ransomware; essentially locking the user’s screen unless a ransom was paid (Domain Tools, 2020).

At the organisational level, ransomware has significantly impacted healthcare services—arguably the most fragile component of a country’s critical national infrastructure at this time. Attacks have been reported in the United States, France, Spain and the Czech Republic (Incisive Media: Computing, 2020; Wired, 2020), and using ransomware such as *Netwalker*. Such attacks fit a criminal modus operandi if we assume that malicious actors will target areas where they believe they stand to capitalise on their attacks; i.e., health organisations may be more likely to pay ransoms to avoid loss of patient lives. Interestingly there have since been promises from leading cyber-crime gangs that they will not (or stop) targeting healthcare services. In one report, operators behind CLOP Ransomware, DoppelPaymer Ransomware, Maze Ransomware and Nefilim Ransomware stressed that they did not (normally) target hospitals, or that they would pause all activity against healthcare services until the virus stabilises (BleepingComputer, 2020).

Other notable malware examples during the pandemic include: *Trickbot*, a trojan that is typically used as a platform to install other malware on victims’ devices—according to Microsoft, *Trickbot* is the most prolific malware operation that makes use of COVID-19 themed lures for its attacks (InfoSecurity, 2020); a Master Boot Record (MBR) rewriter malware that wipes a device’s disks and overwrites the MBR to make them no longer usable (SonicWall, 2020); and *Corona Live 1.1*, an app that leveraged a legitimate COVID-19 tracker released by John Hopkins University and accessed device photos, videos, location data and the camera (CNET, 2020). As the pandemic continues, there are likely to be more strains of malware, targeting various types of harm, e.g., physical, financial, psychological, reputational (for businesses) and societal (Agrafiotis et al., 2018).

During the COVID-19 pandemic our analysis only identified a very small amount (5%) of DoS attacks, but there were several reports of hacking. These reports suggested that hacking was not indiscriminate but instead, targeted towards institutions involved in research on coronavirus.

In one report, FBI Deputy Assistant Director stated, "*We certainly have seen reconnaissance activity, and some intrusions, into some of those institutions, especially those that have publicly identified themselves as working on COVID-related research*" (Reuters, 2020). This was further supported by a joint security advisory a month later from the UK's NCSC and USA's CISA (UK's National Cyber Security Centre (NCSC), 2020b). In this advisory, Advanced Persistent Threat (APT) groups—some of which may align with nation states—were identified as targeting pharmaceutical companies, medical research organisations, and universities involved in COVID-19 response. The goal was not necessarily to disrupt their activities (as with the ransomware case), but instead to steal sensitive research data or intellectual property (e.g., on vaccines, treatments).

While a detailed analysis of these attacks has not yet surfaced, password spraying (a brute-force attack which applying commonly-used passwords in attempting to login to accounts) and exploiting vulnerabilities in Virtual Private Network (VPN) have been flagged (UK's National Cyber Security Centre (NCSC), 2020b). Attribution is another important consideration during such attacks. Determining the true origin of cyber-attacks has always been difficult, however, in response to these COVID-19-related threats, the US openly named the People's Republic of China (PRC) as a perpetrator in a joint FBI/CISA announcement (The Federal Bureau of Investigation (FBI), 2020).

## 4. Impact on workforce

The effects of the pandemic, the mass quarantine of staff and the measures put in place to facilitate remote working and resilience of existing cyber-infrastructures, against the attacks and timelines previously described, had a profound effect on the workforce – the people engaged in or available for work. The pandemic also had an effect on the resilience of technology, socio-economic structures and threatened, to a certain degree, the way people live and communicate. Fig. 6 illustrates the COVID-19 impact on the workforce across eight different categories. All categories seemingly integrate with cyber-enabled assets and tools and different categories may be impacted differently. The pandemic created risk conflicts, for example, strict compliance with security standards which discourage data sharing, could be more harmful than sharing the data. So, whilst there may be strict requirements for patient data not to be accessed at home by GPs (general practitioners), this causes a greater harm during quarantine than enabling GPs to access patient data. Also, the way confidential patient information is processed requires a data protection impact assessment (DPIA) to enable further NHS support where needed. This can have an impact in terms of the timely delivery of medical interventions in response to COVID-19.

In traditional risk classification, elements like asset registration and valuation, threat frequency and vulnerability probability are at greater risk of cyber threat. We, therefore, anticipate changes on the way the workforce accesses those information assets and how strategic, tactical and operational tasks are executed to generate socio-economical outputs. These changes can be captured by the development and testing of risk statements capturing: (1) threat agents; (2) vulnerabilities; (3) Policy/process violation; and (4) overall asset exposure on all emerging threat landscapes as illustrated in Fig. 6. These changes unavoidably cascade further changes to the threat landscapes associated with remote workforce activities and the increasing frequency of weaponised attack vectors related to the coronavirus spreading. Given the current climate, it is difficult to predict whether these changes will have a long-lasting effect on the workforce, but their significance is already recorded (Pipikaite and Davis, 2020). Therefore, it is increasingly important that the control of information (storage, processing, transmission) has an elevated importance given the increase of cyber-attacks on important infrastructures.

Governments, private and public sectors throughout Europe currently consider measures to contain and mitigate COVID-19 impact on existing data structures and information governance frameworks (for example, Data Protection Commission, 2020). Particular emphasis is placed upon the implications of the pandemic in the processing of personal data. Europe's General Data Protection Regulation (GDPR) dictates that personal data must be processed only for the specific and explicit purposes for which it has been obtained (The Information Commissioner's Office, 2020). In addition, data subjects should always receive explicit and transparent information with regard to the processing activities undertaken, including that of features and nature of the activity, retention period and purpose of processing. There are challenges related to the governance legal and regulatory compliance landscape in terms of conformance versus rapid access and processing of data by different entities. This is quite apparent in cases where public authorities seek to obtain PII to reduce the spread of COVID-19. Typical examples also include contact tracing applications and platforms in which the data is aggregated online for post-processing (Downey, 2020b). Specific legislative measures have to be re-deployed or introduced to safeguard public security while maintaining privacy at scale, while legal and regulatory principles continue to upheld (NHSXIG Team, 2020).

With the rapid increase of COVID-19 symptoms, governments had to derive a plan that would enable them to understand epidemiological data further and identify positive interventions to contain and mitigate the impact of the pandemic. Research shows a high correlation between the use of big data that includes private identifiable information in the effectiveness of these epidemiological investigations (Price and Cohen, 2019). That meant that in most cases, citizens had to provide this information voluntarily and that quickly resulted in discussions and debates on the trade-offs between public safety versus personal privacy (Ahn et al., 2020). The information has also been obtained through internet communication technology. Medical testing equipment and coronavirus testing at a large-scale were used as instruments for data collection in the fight to reduce mortality rates. The legal and regulatory compliance frameworks differ between countries; thus, managing personal information was subject to different privacy protection measures.

The de-identification of personal information was another component that governments had to exercise to satisfy personal privacy requirements and increase the trust of human

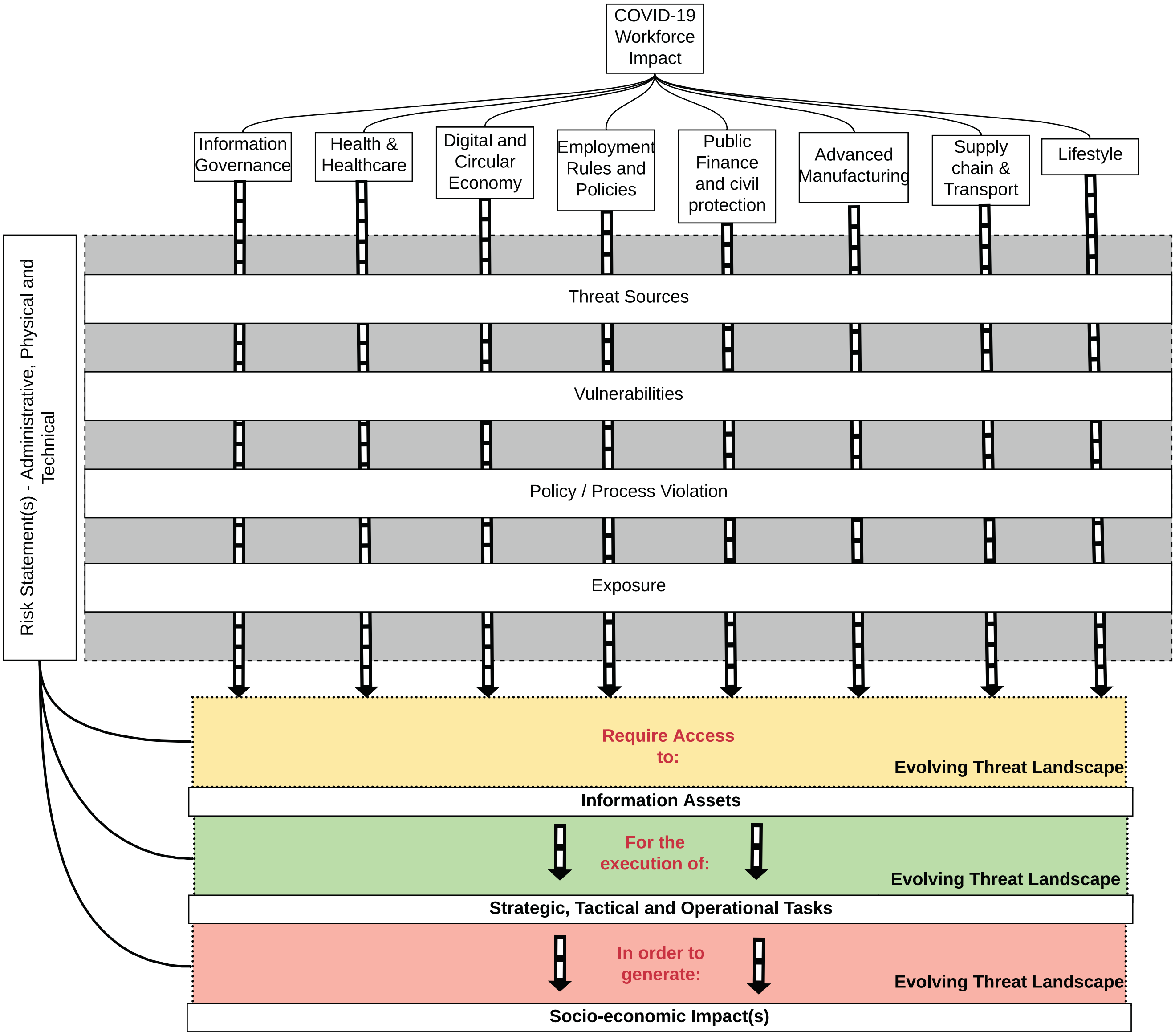

COVID-19 Workforce Impact
Information Governance
Health & Healthcare
Digital and Circular Economy
Employment Rules and Policies
Public Finance and civil protection
Advanced Manufacturing
Supply chain & Transport
Lifestyle
Risk Statement(s) - Administrative, Physical and Technical
Threat Sources
Vulnerabilities
Policy / Process Violation
Exposure
Require Access to:
Evolving Threat Landscape
Information Assets
For the execution of:
Evolving Threat Landscape
Strategic, Tactical and Operational Tasks
In order to generate:
Evolving Threat Landscape
Socio-economic Impact(s)

Fig. 6 – COVID-19 impact on workforce.

participants during the epidemiological investigations. The process of collecting and processing personal information by applying de-identification technologies raised technical challenges with regards to accuracy and consent, safe and legally defensive data disposal and robustness of associated policies of data processing and management for epidemiological research. The urgency of the situation and the speed at which the data had to be acquired and processed, created a sense of distrust amongst citizens and challenged the efficacy of the existing processes in place (Ahn et al., 2020). The extensive lockdown periods introduced in many countries (described in Section 3) have also tested their ability to deploy strategies for business recovery after these periods. These strategies had to ensure smooth and phased out recovery within an ongoing pandemic, which has proved to be a challenging task. However, there is an unprecedented speed and scale on the R&D activities in response to the COVID-19 outbreak forcing cross-organizational multilateral collaborations (AstraZeneca, 2020; Downey, 2020a).

There is currently a challenge across Europe to orchestrate information sharing in a timely and accurate manner as even mainstream media sources seem to have propagated false information (Gagne, 2020). The increase on both frequency and impact of these attacks will test further our existing monitoring and auditing capabilities, logical and physical access controls, authentication and verification schemes currently deployed. Also, as part of the current enterprise risk management approaches the way organisations sanitise incident reporting, media disposal and data destruction and sharing processes will also be tested alongside to traditional defence-in-depth principles currently established as de-facto. The finance sector is also affected as the predicted financial recession will leverage the sophistication and scale of targeted attacks as threat actors grow their capabilities (Cook, 2020).

## 5. Conclusion and future work

The COVID-19 pandemic has generated remarkable and unique societal and economic circumstances leveraged by cyber-criminals. Our analysis of events such as announcements and media stories has shown what appears to be a loose correlation between the announcement and a corresponding cyber-attack campaign which utilises the event as a hook thereby increasing the likelihood of success.

The COVID-19 pandemic, and the increased rate of cyber-attacks it has invoked have wider implications, which stretch beyond the targets of such attacks. Changes to working practises and socialization, mean people are now spending increased periods of time online. In addition to this, rates of unemployment have also increased, meaning more people are sitting at home online- it is likely that some of these people will turn to cyber-crime to support themselves. The combination of increased levels of cyber-attacks and cyber-crime means there may be implications for policing around the World- law enforcement must ensure it has the capacity to deal with cyber-crime (Collier et al., 2020).

The analysis presented in this paper has highlighted a common modus-operandi of many cyber-attacks during this period. Many cyber-attacks begin with a phishing campaign which directs victims to download a file or access a URL. The file or the URL act as the carrier of malware which, when installed, acts as the vehicle for financial fraud. The analysis has also shown that to increase the likelihood of success, the phishing campaign leverages media and governmental announcements.

Although this analysis is not necessarily novel, we believe this is the first time that this has been supported with a context of actual live events. This analysis gives rise to the recommendation that governments, the media and other institutions should be aware that announcements and the publication of stories are likely to give rise to the perpetration of associated cyber-attack campaigns which leverage these events. The events should be accompanied by a note / disclaimer outlining how information relating to the announcement will be relayed.

Our research presents opportunity for further work. This article has shown what can best be described as a loose direct and inverse correlation between events and cyber-attacks. Further research should investigate this phenomenon and outline whether a predictive model can be used to confirm this relationship. There is an abundant supply of cyber-attack case studies relating to countries around the world and a wider analysis of the problem can help in affirming this phenomenon.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## CRediT authorship contribution statement

**Harjinder Singh Lallie:** Writing - review & editing, Writing - original draft. **Lynsay A. Shepherd:** Writing - review & editing, Writing - original draft. **Jason R.C. Nurse:** Writing - review & editing, Writing - original draft. **Arnau Erola:** Writing - review & editing, Writing - original draft. **Gregory Epiphaniou:** Writing - review & editing, Writing - original draft. **Carsten Maple:** Writing - review & editing, Writing - original draft. **Xavier Bellekens:** Writing - review & editing, Writing - original draft.

## REFERENCES

Abrams, L., 2020. New coronavirus screenlocker malware is extremely annoying. https://www.bleepingcomputer.com/news/security/new-coronavirus-screenlocker-malware-is-extremely-annoying/ (Accessed 30 May 2020).

Ahn, N.-Y., Park, J. E., Lee, D. H., Hong, P. C., 2020. Balancing personal privacy and public safety in COVID-19: Case of Korea and France.

Agrafiotis I, Nurse JRC, Goldsmith M, Creese S, Upton D. A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. J. Cybersecur. 2018;4(1):1–15.

Anderson R, Barton C, Bölme R, Clayton R, Ganán C, Grasso T, Levi M, Moore T, Vasek M. In: Workshop on the Economics of Information Security (WEIS). Measuring the changing cost of cybercrime; 2019.

AON, 2020. Social engineering attacks and COVID-19. https://www.aon.com/cyber-solutions/thinking/social-engineering-attacks-and-covid-19/ (Accessed 17 June 2020).

AstraZeneca, 2020. AstraZeneca Advances Response to Global COVID-19 Challenge as it Receives First Commitments for Oxford's Potential New Vaccine. https://www.astrazeneca.com/media-centre/press-releases/2020/astrazeneca-advances-response-to-global-covid-19-challenge-as-it-receives-first-commitments-for-oxfords-potential-new-vaccine.html (Accessed on 20 June 2020).

Bellekens X, Hamilton A, Seeam P, Nieradzinska K, Franssen Q, Seeam A. Pervasive eHealth services a security and privacy risk awareness survey. In: 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA). IEEE; 2016. p. 1–4.

Bellekens X, Jayasekara G, Hindy H, Bures M, Brosset D, Tachtatzis C, Atkinson R. From cyber-security deception to manipulation and gratification through gamification. In: International Conference on Human-Computer Interaction. Springer; 2019. p. 99–114.

Bellekens, X. J., Nieradzinska, K., Bellekens, A., Seeam, P., Hamilton, A. W., Seeam, A., 2016b. A study on situational awareness security and privacy of wearable health monitoring devices..

BleepingComputer, 2020. Ransomware Gangs to Stop Attacking Health Orgs During Pandemic. https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/ (Accessed 15 June 2020).

CBS Netherlands, 2020. Less traditional crime, more cybercrime. https://www.cbs.nl/en-gb/news/2020/10/less-traditional-crime-more-cybercrime (Accessed 9 May 2020).

Cebula JL, Young LR. In: Technical Report. A Taxonomy of Operational Cyber Security Risks. Carnegie Mellon University, Software Engineering Institute; 2010.

Chadwick, J., 2020. Cyber criminals create a spoof copy of the nhs website in the midst of the coronavirus pandemic to trick users into downloading dangerous malware that can steal their passwords and credit card data. https://www.dailymail.co.uk/sciencetech/article-8250737/Kaspersky-detects-fake-NHS-site-steals-credit-card-data.html (Accessed 30 May 2020).

Check Point, 2020. Coronavirus Cyber-attacks Update: Beware of the Phish. https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/ (Accessed 17 May 2020).

Chockalingam S, Pieters W, Teixeira A, van Gelder P. Bayesian network models in cyber security: a systematic review. In: Nordic Conference on Secure IT Systems. Springer; 2017. p. 105–22.

Ciardhuáin SÓ. An extended model of cybercrime investigations. Int. J. Digit. Evid. 2004;3(1):1–22.

CNET, 2017. Watch Out For Hurricane Harvey Phishing Scams. https://www.cnet.com/news/hurricane-harvey-charity-donations-scam-phishing-attack/ (Accessed 15 June 2020).

CNET, 2020. Fake Coronavirus Tracking Apps Are Really Malware That Stalks You. https://www.cnet.com/news/fake-coronavirus-tracking-apps-are-really-malware-that-stalks-its-users/ (Accessed 15 June 2020).

Collier B, Horgan S, Jones R, Shepherd L. In: Research Evidence in Policing: Pandemics. The implications of the COVID-19 pandemic for cybercrime policing in Scotland: a rapid review of the evidence and future considerations. Scottish Institute for Policing Research; 2020. Number 1

Cook, A., 2020. COVID-19: Companies and verticals at risk for cyber attacks. https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/ (Accessed 17 June 2020).

CPS. In: Technical Report. Cybercrime - Prosecution Guidance. The Crown Prosecution Service (CPS); 2019. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance(Accessed 17 June 2020)

cqgbxa.com, 2020. Fighting the spread of coronaviruses who faces severe cybersecurity threats. www.cqgbxa.com/newshy/67936.html (Accessed 30 May 2020).

Cressey, D. R., 1953. Other people's money; a study of the social psychology of embezzlement..

Cross M, Shinder DL. Scene of the cybercrime.. Syngress Pub.; 2008.

CSDN, 2020. Take advantage of the fire! "the epidemic is a bait" cyber attack. https://blog.csdn.net/weixin_43634380/article/details/104237121 (Accessed 30 May 2020).

Cybersecurity Ventures, 2019. 2019 official annual cybercrime report. https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report (Accessed 17 June 2020).

Daily Mail, 2020. Cyber Criminals Create a Spoof Copy of the NHS Website in the Midst of the Coronavirus Pandemic to Trick Users Into Downloading Dangerous Malware That Can Steal Their Passwords and Credit Card Data. https://www.dailymail.co.uk/sciencetech/article-8250737/Kaspersky-detects-fake-NHS-site-steals-credit-card-data.html (Accessed 15 June 2020).

Dark Reading, 2020. Docusign phishing campaign uses COVID-19 as bait. https://www.darkreading.com/attacks-breaches/docusign-phishing-campaign-uses-covid-19-as-bait/d/d-id/1337776 (Accessed 30 May 2020).

Data Protection Commission, 2020. Data Protection and COVID-19. https://dataprotection.ie/en/news-media/blogs/data-protection-and-covid-19 (Accessed on 20 June 2020).

Davis, J., 2020. COVID-19 Impact on Ransomware, Threats, Healthcare Cybersecurity. https://healthitsecurity.com/news/covid-19-impact-on-ransomware-threats-healthcare-cybersecurity (Accessed on 10 November 2020).

Desai, S., 2020. New android app offers coronavirus safety mask but delivers sms trojan. https://www.zscaler.com/blogs/research/new-android-app-offers-coronavirus-safety-mask-delivers-sms-trojan (Accessed 30 May 2020).

de Seguridad del Internauta, O., 2020a. Detectada una campaña fraudulenta de mensajes sms con asunto "erte". https://www.osi.es/es/actualidad/avisos/2020/03/detectada-una-campana-fraudulenta-de-mensajes-sms-con-asunto-erte (Accessed 20 November 2020).

de Seguridad del Internauta, O., 2020b. Guia de ciberataques. https://www.osi.es/es/guia-ciberataques (Accessed 20 November 2020).

Dhanjani N, Rios B, Hardin B. Hacking: The Next Generation: The Next Generation. O'Reilly Media, Inc.; 2009.

Domain Tools, 2020. Covidlock update: Deeper analysis of coronavirus android ransomware. https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware (Accessed 15 June 2020).

Downey, A., 2020a. COVID-19: Collaboration is the Engine of Global Science – Especially for Developing Countries. https://www.weforum.org/agenda/2020/05/global-science-collaboration-open-source-covid-19/ (Accessed on 20 June 2020).

Downey, A., 2020b. NHS contact-tracing app 'falls short of data protection law'. https://www.digitalhealth.net/2020/05/nhs-contact-tracing-app-falls-short-of-data-protection-law/ (Accessed on 20 June 2020).

Elsworthy, E., 2020. Hundreds of bushfire donation scams circulating. https://www.abc.net.au/news/2020-02-07/australia-fires-sees-spike-in-fraudster-behaviour/11923174 (Accessed 15 June 2020).

ESET, 2018. You Have NOT Won! A Look at Fake FIFA World Cup-themed Lotteries and Giveaways. https://www.welivesecurity.com/2018/06/06/fake-fifa-world-cup-themed-lotteries-giveaways/ (Accessed 15 June 2020).

European Anti-Fraud Office (OLAF), 2020. OLAF Launches Enquiry into Fake COVID-19 Related Products. https://ec.europa.eu/anti-fraud/media-corner/news/20-03-2020/olaf-launches-enquiry-fake-covid-19-related-products_en (Accessed 17 May 2020).

Europol, 2020. Pandemic Profiteering: How Criminals Exploit COVID-19 Crisis. https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (Accessed 15 June 2020).

F-Secure, 2020. Coronavirus email attacks evolving as outbreak spreads. https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/ (Accessed 30 May 2020).

Falliere N, Murchu LO, Chien E. W32. Stuxnet dossier. White Paper Symantec Corp. Secur. Response 2011;5(6):29.

FBI, 2016. Hurricane katrina fraud. https://www.fbi.gov/history/famous-cases/hurricane-katrina-fraud (Accessed 9 May 2020).

FitzGerald, N., 2020. Scams, lies, and coronavirus. https://www.welivesecurity.com/2020/04/17/scams-lies-coronavirus/ (Accessed 30 May 2020).

Food and Drugs Administration (FDA), 2020. Fraudulent coronavirus disease 2019 (COVID-19) products. https://www.fda.gov/consumers/health-fraud-scams/fraudulent-coronavirus-disease-2019-covid-19-products (Accessed 15 June 2020).

Forbes, 2020. Chinese hackers 'weaponize' coronavirus data for new cyber attack: Here's what they did. https://www.forbes.com/sites/zakdoffman/2020/03/12/chinese-hackers-weaponized-coronavirus-data-to-launch-this-new-cyber-attack/#196851b03861 (Accessed 30 May 2020).

Forbes, 2020. There Are Now More Than 40,000 'High-Risk' COVID-19 Threats On The Web. https://www.forbes.com/sites/thomasbrewster/2020/04/22/there-are-now-more-than-40000-high-risk-covid-19-threats-on-the-web/ (Accessed 17 May 2020).

freebuf.com, 2020. Analysis and suggestions on several types of network security threats during the epidemic prevention and control period. https://www.freebuf.com/company-information/227585.html (Accessed 30 May 2020).

Fruhlinger, J., 2020. Recent ransomware attacks define the malware's new age. https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html (Accessed 30 May 2020).

FTC, 2016. How to help the earthquake victims in Ecuador and Japan. https://www.consumer.ftc.gov/blog/2016/04/how-help-earthquake-victims-ecuador-and-japan (Accessed 15 June 2020).

FTC, 2020. Online security tips for working from home. https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home (Accessed 9 May 2020).

Gagne, M., 2020. The danger of mainstream media infections with viral and fake information. https://alibi.com/news/60740/The-Danger-of-Mainstream-Media-Infections-with-Vir.html (Accessed 18 June 2020).

Gallagher, S., Brandt, A., 2020. Facing down the myriad threats tied to COVID-19. https://news.sophos.com/en-us/2020/04/14/covidmalware (Accessed 9 May 2020).

Galov, D., 2020. Remote spring: the rise of rdp bruteforce attacks. https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820 (Accessed 9 May 2020).

Glos Safe Cyber, 2020. Our @glospolice_fcr have had calls asking if COVID-19 texts like the below are genuine. https://twitter.com/GlosSaferCyber/status/1242525105508532225 (Accessed 30 May 2020).

Google, 2020. Google Translate. https://translate.google.co.uk/ (Accessed 30 May 2020).

Government, U., 2020. Budget 2020: What You Need to Know. https://www.gov.uk/government/news/budget-2020-what-you-need-to-know, (Accessed 10 June 2020).

Henderson, S., Roncone, G., Jones, S., Hultquist, J., Read, B., 2020. Vietnamese threat actors apt32 targeting Wuhan government and Chinese ministry of emergency management in latest example of COVID-19 related espionage. https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html (Accessed 17 June 2020).

Hill, M., 2020. HMRC Shuts Down Almost 300 COVID19 Phishing Scam Sites. https://www.infosecurity-magazine.com/news/hmrc-covid19-phishing-scams/, (Accessed 10 June 2020).

Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., Bellekens, X., A taxonomy and survey of intrusion detection system design techniques, network threats and datasets. arXiv preprint arXiv:1806.03517

Hiscox, 2019. The hiscox cyber readiness report 2019. https://www.hiscox.co.uk/cyberreadiness (Accessed 9 May 2020).

Hoffman, S., 2009. Michael Jackson's death spurs spam, malware campaigns. https://www.crn.com/blogs-op-ed/the-channel-wire/218101623/michael-jacksons-death-spurs-spam-malware-campaigns.htm (Accessed 9 May 2020).

Hindy H, Brosset D, Bayne E, Seeam A, Tachtatzis C, Atkinson R, Bellekens X. A taxonomy of network threats and the effect of current datasets on intrusion detection systems. IEEE Access 2020;8:104650–75.

Horton N, DeSimone A. In: Technical Report. Sony's Nightmare Before Christmas: The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace. JHUAPL Laurel United States; 2018.

Incisive Media: Computing, 2020. Spanish Hospitals Targeted With Coronavirus-themed Phishing Lures in Netwalker Ransomware Attacks. https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware (Accessed 15 June 2020).

InfoSecurity, 2020. Trickbot Named Most Prolific #COVID19 Malware. https://www.infosecurity-magazine.com/news/trickbot-named-most-prolific/ (Accessed 15 June 2020).

Iuga C, Nurse JRC, Erola A. Baiting the hook: factors impacting susceptibility to phishing attacks. Hum.-Centric Comput. Inf. Sci. 2016;6(1):8.

Jansson, T., 2018. Blackmailing and passwords leaks. https://www.linkedin.com/pulse/blackmailing-passwords-leaks-thomas-jansson (Accessed 17 June 2020).

Jisho, 2020. Cyber attack. https://jisho.org/search (Accessed 30 May 2020).

Kaspersky, 2016. Research Reveals Hacker Tactics: Cybercriminals Use DDoS as Smokescreen for Other Attacks on Business. https://www.kaspersky.com/about/press-releases/2016_research-reveals-hacker-tactics-cybercriminals-use-ddos-as-smokescreen-for-other-attacks-on-business (Accessed 15 June 2020).

Kaspersky, 2020. Coronavirus phishing. https://www.kaspersky.com/blog/coronavirus-phishing/32395/ (Accessed 30 May 2020).

Koenig, B., 2020. Covid sms phishing attempt. https://twitter.com/BigBenKoenig/status/1242503232527589376 (Accessed 30 May 2020).

Kolomiyets O, Bethard S, Moens M-F. Extracting narrative timelines as temporal dependency structures. In: Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics: Long Papers-Volume 1. Association for Computational Linguistics; 2012. p. 88–97.

Kotenko I, Chechulin A. A cyber attack modeling and impact assessment framework. In: 2013 5th International Conference on Cyber Conflict (CYCON 2013). IEEE; 2013. p. 1–24.

Krebs on Security, 2020. Live Coronavirus Map Used to Spread Malware. https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/ (Accessed 15 June 2020).

Kumaran, N., Lugani, S., 2020. Protecting businesses against cyber threats during COVID-19 and beyond. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond (Accessed 17 June 2020).

Le Parisien, 2020. Municipal: "massive" computer attack at the town hall of marseille. http://www.leparisien.fr/elections/municipales/municipales-attaque-informatique-massive-a-la-mairie-de-marseille-15-03-2020-8280114.php (Accessed 30 May 2020).

Lush, R., 2020. Helping defend against a 30,000% increase in phishing attacks related to COVID-19 scams. https://www.cgi-group.co.uk/en-gb/blog/cyber-security/helping-defend-against-a-30000-increase-in-phishing-attacks-related-to-covid-19-scams (Accessed on 10 November 2020).

Magazine, D. C. R., 2020. Hackers exploit hmrc coronavirus job retention scheme with phishing email scam. https://datacentrereview.com/news/1680-hackers-exploit-hmrc-coronavirus-job-retention-scheme-with-phishing-email-scam (Accessed 30 May 2020).

Malwarebytes, 2020. 2020 state of malware report. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf (Accessed 30 May 2020).

MalwareBytes, 2020. Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book. https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/, (Accessed 15 June 2020).

McGuire M. In: Understanding the Growth of Cybercrime Economy. Bromium. Into the web of profit; 2018.

McGuire M, Dowling S. In: Technical Report. Chapter 1: Cyber-Dependent Crimes; 2013. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf(Accessed 18 June 2020)

McGuire M, Dowling S. In: Technical Report. Chapter 2: Cyber-Enabled Crimes - Fraud and Theft; 2013. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf(Accessed 18 June 2020)

Millman, R., 2020. Coronavirus test results delayed by cyber-attack on czech hospital. https://www.scmagazineuk.com/coronavirus-test-results-delayed-cyber-attack-czech-hospital/article/1677194 (Accessed 30 May 2020).

Mimecast, 2020. New Threat Intelligence Report:100 Days of Coronavirus. https://www.mimecast.com/blog/2020/05/100-days-of-coronavirus/, (Accessed 15 June 2020).

Muncaster, P., 2020. Android malware takes payment for 'coronavirus finder' map. https://www.infosecurity-magazine.com/news/android-malware-payment/ (Accessed 30 May 2020).

Murica Today, 2020. Cyber-attack threatens spanish hospital computer systems. https://murciatoday.com/cyber_attack_threatens_spanish_hospital_computer_systems_1367723-a.html (Accessed 30 May 2020).

Naked Security, 2009. Michael Jackson's death sparks off spam. https://nakedsecurity.sophos.com/2009/06/26/michael-jackson-harvesting-email-addresses (Accessed 9 May 2020).

NCSC, 2020a. Home working: preparing your organisation and staff. https://www.ncsc.gov.uk/guidance/home-working (Accessed 9 May 2020).

NCSC, 2020b. NCSC Shines Light on Scams Being Foiled via Pioneering New Reporting Service. https://www.actionfraud.police.uk/news/cyber-experts-shine-light-on-online-scams-as-british-public-flag-over-160000-suspect-emails, (Accessed 7 May 2020).

NHS, 2020. 10 tips to help if you are worried about coronavirus. https://www.nhs.uk/oneyou/every-mind-matters/coronavirus-covid-19-anxiety-tips (Accessed 9 May 2020).

NHSXIG Team, 2020. COVID-19 information governance advice for ig professionals. https://www.nhsx.nhs.uk/covid-19-response/data-and-information-governance/information-governance/covid-19-information-governance-advice-ig-professionals/ (Accessed 18 June 2020).

NIST, 2020. Security for enterprise telework, remote access, and bring your own device (byod) solutions. https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf (Accessed 9 May 2020).

Norton, 2020. Coronavirus Phishing Emails: How to Protect Against COVID-19 Scams. https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html (Accessed 15 June 2020).

Nurse JRC. In: The Oxford Handbook of Cyberpsychology. Cybercrime and you: how criminals attack and the human factors that they seek to exploit. OUP; 2019.

O'Brien, T. L., 2020. Covid aid scams and dodgy deals could have been avoided. https://www.bloomberg.com/opinion/articles/2020-05-01/coronavirus-trillions-in-aid-draws-scams-and-dodgy-deals (Accessed 9 May 2020).

O'Donnell, L., 2020. Skype phishing attack targets remote workers' passwords. https://threatpost.com/skype-phishing-attack-targets-remote-workers-passwords/155068/ (Accessed 30 May 2020).

Pais, E., 2020. Ataques informaticos. https://elpais.com/noticias/ataques-informaticos/ (Accessed 20 November 2020).

Patranobis, S., 2020. Indian Hackers Targeting Chinese Medical Institutes Amid Coronavirus Outbreak, Says Report. https://www.hindustantimes.com/world-news/indian-hackers-targetting-chinese-medical-institutes-amid-coronavirus-outbreak-says-report/story-piDHQeY4UfTVy8BWa2GG3O.html, (Accessed on 12 June 2020).

Pipikaite, A., Davis, N., 2020. Why cybersecurity matters more than ever during the coronavirus pandemic. https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/ (Accessed 18 June 2020).

Price W, Cohen I. Privacy in the age of medical big data. Nat. Med. 2019;25. doi:10.1038/s41591-018-0272-7.

la Repubblica, 2020. Cyber attack on easyjet, compromised the data of nine million customers. https://www.repubblica.it/tecnologia/sicurezza/2020/05/19/news/attacco_informatico_a_easyjet_compromessi_i_dati_di_nove_milioni_di_clienti-257099879/ (Accessed 30 May 2020).

Reuters, 2020. FBI official says foreign hackers have targeted COVID-19 research. https://uk.reuters.com/article/us-health-coronavirus-cyber/foreign-state-hackers-target-u-s-coronavirus-treatment-research-fbi-official-idUKKBN21Y3GL (Accessed 15 June 2020).

Rodger, J., 2020. The school meals coronavirus text scam which could trick parents out of thousands. https://www.birminghammail.co.uk/news/midlands-news/school-meals-coronavirus-text-scam-17975311 (Accessed 30 May 2020).

Rosso, K. D., 2020. New threat discovery shows commercial surveillanceware operators latest to exploit COVID-19. https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19 (Accessed 30 May 2020).

Segura, J., 2017. Compromised linkedin accounts used to send phishing links via private message and inmail. https://blog.malwarebytes.com/threat-analysis/2017/09/compromised-linkedin-accounts-used-to-send-phishing-links-via-private-message-and-inmail (Accessed 9 May 2020).

Shepherd L, Renaud K. How to design browser security and privacy alerts. In: AISB 2018. Society for the Study of Artificial

Intelligence and Simulation for Behaviour (AISB); 2018. p. 21–8. 2018 AISB Convention : Symposium on Digital Behaviour Intervention for Cyber Security

Shi, F., 2020. Threat spotlight: Coronavirus-related phishing. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing (Accessed 9 May 2020).

Sky News, 2020. Coronavirus: Fraud victims have lost more than £4.6m to virus-related scams. https://news.sky.com/story/coronavirus-fraud-victims-have-lost-more-than-4-6m-to-virus-related-scams-11996721, (Accessed 10 June 2020).

Smithers, R., 2020. Fraudsters use bogus nhs contact-tracing app in phishing scam. https://www.theguardian.com/world/2020/may/13/fraudsters-use-bogus-nhs-contact-tracing-app-in-phishing-scam (Accessed 30 May 2020).

smzdm.com, 2020. Hackers are using the "coronavirus" fear for phishing, please pay attention to prevention!https://post.smzdm.com/p/a07ol5x0/ (Accessed 30 May 2020).

SonicWall, 2020. Coronavirus Trojan Overwriting The MBR. https://securitynews.sonicwall.com/xmlpost/coronavirus-trojan-overwriting-the-mbr/ (Accessed 15 June 2020).

Sophos, 2020. Dirty little secret extortion email threatens to give your family coronavirus. https://nakedsecurity.sophos.com/2020/03/19/dirty-little-secret-extortion-email-threatens-to-give-your-family-coronavirus/ (Accessed 15 June 2020).

Stajano F, Wilson P. Understanding scam victims: seven principles for systems security. Commun. ACM 2011;54(3):70–5.

Stein, S., Jacobs, J., 2020. Cyber-attack hits U.S. health agency amid COVID-19 outbreak. https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response (Accessed 30 May 2020).

Stonefly, 2020. Coronavirus and ransomware infection - what's the connection?https://stonefly.com/blog/coronavirus-ransomware-infection-whats-the-connection (Accessed 12 June 2020).

Strawbridge, G., 2020. Warning over coronavirus netflix scam. https://www.metacompliance.com/blog/warning-over-coronavirus-netflix-scam/ (Accessed 30 May 2020).

Swansea Council, 2020. Coronavirus Scams. https://www.swansea.gov.uk/coronavirusscam, (Accessed 10 June 2020).

TechRepublic, 2020. Global shipping industry attacked by coronavirus-themed malware. https://www.techrepublic.com/article/global-shipping-industry-attacked-by-coronavirus-themed-malware/ (Accessed 30 May 2020).

The Federal Bureau of Investigation (FBI), 2020. People's Republic of China (PRC) Targeting of COVID-19 Research Organizations. https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations (Accessed 15 June 2020).

The Guardian, 2020. US Authorities Battle Surge in Coronavirus Scams, From Phishing to Fake Treatments. https://www.theguardian.com/world/2020/mar/19/coronavirus-scams-phishing-fake-treatments (Accessed 15 June 2020).

The Information Commissioner's Office, 2020. General data protection regulation (gdpr): Principle (b): Purpose limitation. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (Accessed 19 June 2020).

The Ministry of Health, Labour and Welfare, 2020. Latest information on Coronavirus disease 2019 (COVID-19).https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000164708_00001.html (Accessed 30 May 2020).

The Register, 2020. Fresh virus misery for illinois: Public health agency taken down by... web ransomware. great timing, scumbags. https://www.theregister.co.uk/2020/03/12/ransomware_illinois_health/ (Accessed 30 May 2020).

The Times, 2020. Fraudsters impersonate airlines and Tesco in coronavirus scams. https://www.thetimes.co.uk/article/fraudsters-impersonate-airlines-and-tesco-in-coronavirus-scams-5wdwhxq7p, (Accessed 15 June 2020).

Tidy, J., 2020. Coronavirus: Israel enables emergency spy powers. https://www.bbc.co.uk/news/technology-51930681 (Accessed 30 May 2020).

Tsakalidis G, Vergidis K. A systematic approach toward description and classification of cybercrime incidents. IEEE Trans. Syst. Man Cybern. 2017;49(4):710–29.

Tysiac, K., 2018. How cybercriminals prey on victims of natural disasters. https://www.journalofaccountancy.com/news/2018/sep/cyber-criminals-prey-on-natural-disaster-victims-201819720.html (Accessed 9 May 2020).

UK Government, 2020. UK Medicines and Medical Devices Regulator Investigating 14 Cases of Fake or Unlicensed COVID-19 Medical Products. https://www.gov.uk/government/news/uk-medicines-and-medical-devices-regulator-investigating-14-cases-of-fake-or-unlicensed-covid-19-medical-products (Accessed 17 May 2020).

UK's National Cyber Security Centre (NCSC) and the US' Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), 2020b. Advisory: APT groups target healthcare and essential services. https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services-advisory (Accessed 15 June 2020).

UK's National Cyber Security Centre (NCSC) and the US' Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), 2020a. Advisory: COVID-19 Exploited by Malicious Cyber Actors. https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory (Accessed 15 June 2020).

US Department of Justice (DOJ), 2020. COVID-19 fraud. https://www.justice.gov/usao-edky/covid-19-fraud-1 (Accessed 15 June 2020).

Van Heerden R, Von Soms S, Mooi R. Classification of cyber attacks in south africa. In: 2016 IST-Africa Week Conference. IEEE; 2016. p. 1–16.

Walter, J., 2020. Threat Intel:Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic. https://labs.sentinelone.com/threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/, (Accessed 10 June 2020).

WHO, 2020. #healthyathome. https://www.who.int/news-room/campaigns/connecting-the-world-to-combat-coronavirus/healthyathome (Accessed 9 May 2020).

Wired, 2020. Hackers Are Targeting Hospitals Crippled by Coronavirus. https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing (Accessed 15 June 2020).

World Economic Forum, 2020. COVID-19 Risks Outlook: A Preliminary Mapping and its Implications. https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-itsimplications (Accessed on 10 November 2020).

World Health Organisation (WHO), 2020a. Coronavirus disease (COVID-19) pandemic. https://www.who.int/zh/emergencies/diseases/novel-coronavirus-2019 (Accessed 18 June 2020).

World Health Organisation (WHO), 2020b. Naming the coronavirus disease (COVID-19) and the virus that causes it. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it (Accessed 15 June 2020).

World Health Organisation (WHO), 2020c. WHO Coronavirus Disease (COVID-19) Dashboard. https://covid19.who.int/, (Accessed 15 June 2020).

World Health Organisation (WHO), 2020d. Who reports fivefold increase in cyber attacks, urges vigilance. https://www.who.int/zh/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (Accessed 18 June 2020).

Wang G-y, Wang H-m, Chen Z-j, Xian M. Research on computer network attack modeling based on attack graph. J. Natl. Univ. Defense Technol. 2009;4:816–19.

Yar M. The novelty of 'cybercrime' an assessment in light of routine activity theory. Eur. J. Criminol. 2005;2(4):407–27.

**Dr. Harjinder Singh Lallie** is an Associate Professor at the University of Warwick and a visiting academic at the University of Oxford. Harjinder holds a Ph.D. in cyber security, an M.Phil, an M.Sc., and a BSc. Harjinder has more than twenty years of teaching experience and currently leads the M.Sc.Cyber Security and Management degree. Harjinder's research focuses on the area of complex cyber-attack modelling, digital forensics and the use of AI in digital forensics. He has published numerous research papers in the world's top cyber security journals. Harjinder has held numerous conference committee memberships, he acts as an external examiner and has conducted a number of national and international institutional reviews. Recently, he acted as consultant to the International Atomic and Energy Agency (IAEA) at the United Nations in Vienna.

**Dr Lynsay A. Shepherd** is a Lecturer in Cybersecurity and Human-Computer Interaction at Abertay University, Dundee, and works within the School of Design and Informatics. Lynsay holds a Ph.D. in Usable Security, an M.Sc. in Internet Computing, and a B.Sc. (Hons) in Computing. Lynsay's research interests currently focus on the human aspects of cybersecurity, examining end-user security behaviour, and exploring methods to improve security awareness.

**Dr Jason R. C. Nurse** is an Associate Professor in Cyber Security in the School of Computing at the University of Kent, UK and the Institute of Cyber Security for Society (iCSS), UK. He also holds the roles of Visiting Academic at the University of Oxford, Visiting Fellow in Defence & Security at Cranfield University, UK and Associate Fellow at the Royal United Services Institute for Defence and Security Studies (RUSI). His research interests include security risk management, corporate communications and cyber security, secure and trustworthy Internet of Things, insider threat and cybercrime. Jason was selected as a Rising Star for his research into cybersecurity, as a part of the UK's Engineering and Physical Sciences Research Council's Recognising Inspirational Scientists and Engineers (RISE) awards campaign. Dr Nurse holds a Ph.D. in cyber security, an M.Sc. in Internet Computing and a B.Sc. in Computer Science and Accounting. He has published over 100 peer-reviewed articles in internationally recognised security journals and conferences.

**Dr Arnau Erola** is a Senior Research Associate at the Department of Computer Science of the University of Oxford, working on cyber insurance and better understanding the cyber-threat landscape. His research interests include, but are not limited to, enterprise security, defence systems and economics of cyber security. Dr Erola holds a Ph. D., M. Sc. and B.Sc. in Computer Science from the Universitat Rovira i Virgili (Tarragona). He is author of several international journal articles on online privacy, anonymity protocols and intrusion detection mechanisms.

**Dr Gregory Epiphaniou** currently holds a position as an Associate Professor of security engineering at the University of Warwick. His role involves bid support, applied research and publications. He led and contributed to several research projects funded by EPSRC, IUK and local authorities totalling over 3M. He was previously holding a position as a Reader in Cybersecurity and acted as deputy director of the Wolverhampton Cybersecurity Research Institute (WCRI). He has taught in many universities both nationally and internationally a variety of areas related to proactive network defence with over 80 international publications in journals, conference proceedings and author in several books and chapters. He holds several industry certifications around Information Security and worked with several government agencies including the UK MoD in Cybersecurity related projects. He acts as a technical committee member for several scientific conferences in Information and network security and serves as a key member in the development of WS5 for the formation of the UK Cybersecurity Council

**Professor Carsten Maple** is the Principal Investigator of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research at the University and Professor of Cyber Systems Engineering in WMG. He is also a co-investigator of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity where he leads on Transport & Mobility. Carsten is a Fellow of the Alan Turing Institute, where he is Principal Investigator of the $5 million Trustworthy Digital Infrastructure project. He has an international research reputation and extensive experience of institutional strategy development and interacting with external agencies. He has published over 250 peerreviewed papers and is co-author of the UK Security Breach Investigations Report 2010, supported by the Serious Organised Crime Agency and the Police Central e-crime Unit. Carsten is also co-author of Cyberstalking in the UK, a report supported by the Crown Prosecution Service and Network for Surviving Stalking. His research has attracted millions of pounds in funding and has been widely reported through the media. He has given evidence to government committees on issues of anonymity and child safety online. Additionally he has advised executive and non-executive directors of public sector organisations and multibillion pound private organisations. Professor Maple is a Past Chair of the Council of Professors and Heads of Computing in the UK, a member of the Zenzic Strategic Advisory Board, a member of the IoTSF Executive Steering Board, an executive committee member of the EPSRC RAS Network and a member of the UK Computing Research Committee, the ENISA CarSEC expert group, the Interpol Car Cybercrime Expert group and Europol European Cyber Crime Centre.

**Dr Xavier Bellekens** is a Chancellor's Fellow Assistant Professor with the Department of Electronic and Electrical Engineering at the University of Strathclyde and a Nonresident Fellow of the Scowcroft Center for Strategy and Security at the Atlantic Council. His current research interests include critical infrastructure protection, defence as well as cyber deception and deterrence. Xavier is also the Chair of the IEEE Cyber Science collocated conferences, the Education Cyber-Security Thematic Leader, the Chair of the Blockchain Group and the Vice-Chair of Cyber-Security Group for IEEE UK and Ireland. He frequently appears in the media to provide commentary to international press – on radio, tv and newspapers on major cyber-events.