Policy Design and Practice

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rpdp20

Preparing for future cyber crises: lessons from governance of the coronavirus pandemic

Gareth Mott, Jason R. C. Nurse & Christopher Baker-Beall

POLICY DESIGN AND PRACTICE
https://doi.org/10.1080/25741292.2023.2205764

RESEARCH ARTICLE

OPEN ACCESS

Preparing for future cyber crises: lessons from governance of the coronavirus pandemic

Gareth Mott[a], Jason R. C. Nurse[a] and Christopher Baker-Beall[b]

[a]School of Politics and International Relations, University of Kent, Kent, UK; [b]Disaster Management Centre, Bournemouth University, Bournemouth, UK

ABSTRACT

The SARS-CoV-2 pandemic has had an immense impact on public policy and the management of risks that threaten critical systems, such as national health services. Drawing on perspectives from multiple disciplines, this article considers lessons-learned with respect to mitigating the threats to critical systems and societal harms presented by the proliferation of malware. The article dovetails crisis management with cyber resilience, for the purpose of analyzing transferable good-practices and areas-for-improvement, drawing on preparedness and response strategies deployed in public policymaking in the United Kingdom during the pandemic. Reflecting on key national and local ransomware incidents that have impacted key services, the article offers a post-SARS-CoV-2 review of recent British strategic outputs with respect to cyber resilience; most notably the *National Cyber Security Strategy* and the *Government Cyber Security Strategy*. The article focuses on lessons that may be learned with respect to communications strategies. The article argues that although the recent British cyber-security strategies hold significant promise in terms of improving preparedness, response and recovery in relation to future cyber crisis, nuanced, dynamic and empathetic multi-stakeholder engagement will be required in order to meaningfully implement the measures outlined in the strategy documents.

ARTICLE HISTORY
Received 29 April 2022
Accepted 17 April 2023

KEYWORDS
cyber resilience; crisis management; ransomware; coronavirus; communication

1. Introduction

In both British and international contexts, the SARS-CoV-2 pandemic ushered in dynamic alterations to the risk-conscious discourse that is mediated between state authorities, industry, academic experts and the citizenry. As of writing, the global pandemic is reported to have taken the lives of 203,159 people in the UK (Gov.uk 2022) and an estimated 6,482,338 people globally (WHO 2022). Initially emanating from a localized source, SARS-CoV-2 demonstrated a strident capacity to hijack the

CONTACT Gareth Mott g.mott@kent.ac.uk School of Politics and International Relations, University of Kent, Kent, UK

transnational movement of its human hosts to rapidly spread across an interconnected world.

Across the first and second quarters of 2020, governments sought to constrain the spread of the virus by imposing comprehensive restrictions on the behavioral patterns of society, including economic and social activity. In liberal democratic contexts—for instance, the UK—these restrictions were the first of their kind in living memory; even the iconic "inalienable right" to frequent a public house became a prohibited activity (Stewart and Walker 2020). Wide-ranging behaviors were foregone in the effort to limit infection cases, hospitalizations and deaths, to the extent that fraternization between British households in effect became criminalized through the Coronavirus Act 2020 (Legislation.gov.u). Such pervasive restrictions were imposed to protect two interlinked referent objects to-be-secured; the longevity of human lives and the critical systems and services upon which those lives relied (BBC News 2020).

Through its expansive human kinetic mobility, SARS-COV-2 exploited the vulnerability of interconnected modern societies in its simple objective: to reproduce using living hosts. However, modernity also offered avenues for resilience. A combination of vast state funding (Safi 2021) of modern medical science and international supply chains enabled the rapid development and mass-production of vaccines sufficiently effective to curtail hospitalization and death rates amongst newly-immunized populations. SARS-CoV-2 and its descendants are unlikely to be eradicated, but the resilience of already-infected and immunized populations may in-time, hopefully, relegate the societal impact of the virus to something akin to the common season flu (Phillips 2021).

Resilience, in terms of human society, refers to the ability to "bounce back" following a damaging or disruptive event (Boin and McConnell 2007). As such, some resilience-enhancing practices may remain; particularly with respect to the entwined necessity of ensuring the protection of critical systems and services in addition to the human beings reliant upon them. This will understandably relate to the SARS-CoV-2 template of biological security, but it will also have transferable ramifications for sociotechnical cybersecurity. In the case of SARS-CoV-2, human beings were the vectors of attack and referents of infection. However, with respect to sociotechnical security cybersecurity, computers and networked systems are instead commonly the vectors of attack and infected objects, which display similar traits in terms of their viral spread. The UK government defines critical national infrastructure as the "buildings, networks and other systems that are needed to keep the UK running and provide the essential services upon which we rely (e.g. energy, finance, telecoms and water services) … a significant proportion of our CNI is privately owned" (Cabinet Office, 2017, 5).

Drawing on perspectives from Politics and International Relations, Disaster and Crisis Management, and Computing Science, this article considers lessons-learned from the SARS-CoV-2 pandemic with respect to mitigating societal harms presented by the proliferation of malware, and specifically, ransomware. To accomplish this, the article uses an interpretive approach to the UK's articulation of itself as a cyber resilient actor and society, applying a double-reading methodology (see Bevir, Daddow, and Hall 2013; Ashley 1988; Shepherd 2008). A first reading seeks to identify the key themes underpinning the discourse. This involves asking a series of questions of the sources, in order to ascertain the overarching themes that are exhibited in the partial-fixing of given discourse(s) (Doty, 1998). Firstly, we asked "What are the key words, terms, phrases, labels, metaphors and beliefs in each source?," followed by "What are the main themes of the discourse?" We then asked, "How does the discourse construct the [SARS-CoV-2/ransomware] societal threat warranting risk aversion?" A second reading scrutinizes the relationship between the discourse and the practices that this language enabled or enables (Baker-Beall, 2016; Mott, 2019). Herein, discourse is considered to be performative, and it acquires this performativity through the partial fixation of meaning. Accordingly, we asked a further three questions of the sources. Firstly, "How does the discourse partially fix the meaning of [health/cyber] societal-level threat?" Secondly, "What knowledge and/or practices does the discourse legitimise, and what knowledge and/or practices does it serve to exclude"? Lastly, we asked "To what extent can the construction of the threat—and mitigating measures—relating to SARS-CoV-2 and ransomware, offer space for lessons-learned in the practice of security politics"?

The corpus underpinning the analysis includes British governmental cyber security strategic documents, NCSC guidance and publications, in addition to contextual documentation, news reports and governmental discourse surrounding the SARS-CoV-2 countermeasures and pandemic preparedness. The core purpose of the analysis is to consider whether lessons may be learned from pandemic preparedness and response, in order to inform approaches to cyber resilience with respect to ransomware. Due to space constraints, the article focuses on a particular area of resilience-proofing: communication(s) strategy. It is argued that potential lessons-learned in this area have already been baked into high-level government strategies, but that policy will be required to implement these ambitions for UK cyber resilience. For instance, mandatory reporting of cyber incidents in key sectors is one policy avenue under consideration by British policymakers (DCMS 2022a).

Ransomware is a form of malware that encrypts a computer's file system maliciously, forcing the owner of the system to pay a ransom demand to regain access (CISA nd). Once the victim pays a given ransom demand, in theory criminals will then provide the victim with a decryption key to retrieve their files. Ransomware thus presents a form of malware with a built-in bespoke case-by-case antidote; the cryptographic keys held by crime groups. Nonetheless, as recent ransomware cases have demonstrated—for instance, the JBS and Colonial Pipeline incidents respectively (BBC News 2021; Bing and Kelly 2021)—ransomware in effect serves as an intentional denial of service/information attack (Nurse 2019). This may include denial or disruption of critical services. Freely distributed "cryptographic antidotes" for common historical ransomware are available from repositories including the No More Ransom Project, saving victims an estimated £850 million in avoided ransoms by summer 2021 (Scroxton 2021). However, in much the same way the emergence of SARS-COV-2 variants have left society playing catch-up in terms of the development of new vaccines that are variant specific, the innovation of ransomware gangs and the development of new types of ransomware have also left law enforcement and IT security professionals engaged in continual catch-up. Victims payments of ransom demands to acquire the "antidotes" also encourages further ransomware activity and rewards criminal behavior.

From the perspective of the victim, payment of a given ransom demand may be the most rational action to regain swift access to systems and business function, but on an aggregated basis this also serves to incentivise a potential ransomware pandemic. As such, there must be a vested and concerted push to align upon longer-term resilience-building practices for pre-, through- and post- cyber security breach preparedness. This befits the lens of "anticipatory" security (Anderson 2010); anticipating and mitigating threats *before* they arise. Additionally, SARS-CoV-2 has (re)opened the Pandora's Box with respect to the interlinked nature of system and human security/resilience (Haldane et al. 2021). Although some practices will not be transferable, others may be. In the furtherance of sociotechnical security, it is worth, at least, to commence this discussion.

The article is ordered as follows. First, we outline a broad overview of cyber resilience as a concept and strategy. Second, we analyze best-practice and lessons-learned from the pandemic that may be transferable to matters of sociotechnical security, aligning this discussion with recent national cyber security discourse emanating from the UK government; most notably, the *Cyber Security Strategy* and *Government Cyber Security Strategy*, which respectively outline the UK government's broad-picture roadmap for bolstering British cyber resilience. The article's analysis and proposals are useful from the perspective of reviewing contemporary sociotechnical resilience holistically. Nonetheless, the analysis focuses on the threat posed by ransomware in particular, given the societally-disruptive potential demonstrated by this form of malware in the period between 2017 and 2022.

2. Cyber resilience: a contemporary assessment of the state of play

Resilience as a topic has been discussed in numerous fields, from disaster recovery (Manyena 2006) to mental health (Herrman et al. 2011), and more recently in deliberations against disinformation (Humprecht, Esser, and Van Aelst 2020). While the contexts of these articles differ, they share a core meaning of resilience which stems from the ability to recover or successfully weather challenges, difficulties or periods of unpredictability. In personal health, resilience can translate to adapting and responding positively to significant adversity in one's life, while in business, being resilient may mean effectively navigating a period of financial uncertainty. Coutu (2002) provides a succinct description of resilience: "resilience is neither ethically good nor bad. It is merely the skill and the capacity to be robust under conditions of enormous stress and change." Again, this teases out the key concept of being robust in challenging situations, but also hints to the neutral nature of resilience as a term abstract from its applications. For instance, a virus may be resilient against treatment (a positive for the virus but negative for an infected individual), but an individual may be resilient if infected by a virus (a positive for the individual and a negative for the virus).

Cyber resilience is, broadly speaking, a new term that aims to borrow from learning around resilience. It was coined to emphasize the importance of an organizational strategy to be able to prepare, absorb, recover, and adapt from cyber events (including attacks and incidents) (NCSC 2018a). This goes beyond approaches to dealing with cyber-attacks which have traditionally been centered on prevention, detection and recovery and highlights the need of enterprises to build the ability to absorb a sustained or significant incident, and also, to later adapt. Effectively absorbing an incident involves various factors including ensuring early detection of an incident (which supports early response) and several layers of defenses (also referred to as defence in depth) that raises the bar for attackers gaining full access to systems (NCSC 2018a). Adapting to incidents is another key concept and deals with keeping systems (human and cyber-physical) agile to the extent that they can respond and change when faced with new threats. Biological viruses present a good analogy here, given their ability to adapt and spawn different variants (as observed with the Alpha, Beta, Gamma, Delta and Omicron SARS-CoV-2 variants (CDC 2022a), or develop strains that are resistant to available vaccines and anti-viral medicines.

Across research and industry there have been various frameworks, models and theories proposed to create a cyber resilient environment. Early work concentrated on the problem of engineering cyber resilient systems, as a sub-discipline of mission assurance engineering, and outlined a framework to structure resilience deliberations based on plans, goals and any limiting factors (e.g. costs) (Bodeau et al. 2011). Since then, approaches have explored topics ranging from the role of policy in building the cyber resilience of national infrastructures (Tiirmaa-Klaar 2016) to creation of cyber resilient small-to-medium sized businesses (Carías et al. 2020). And, from methods to ensure resilience based on Catastrophe Theory (Petrenko and Vorobieva 2019) to the future of resilience in a constantly changing technical and political world (Herrington and Aldrich 2013).

Across the cyber resilience domain, however, little concerted attention has been paid to the public as an entity that needs to be cyber resilient, nor has the question of how that cyber resilience should be attained been adequately broached. The primary vehicle of public security education thus far has been national cybersecurity awareness campaigns (e.g. Cyber Aware in the UK, STOP.THINK.CONNECT^{TM} in the US, European Cybersecurity Month in the EU) that aim to raise the citizenry's understanding of how to protect themselves online (Nurse 2021). Although these programmes represent significant efforts to boost awareness across national populations, they often suffer from a lack of targeted messaging which appreciates personal and cultural factors, a focus on increasing awareness with an assumption that behavioral change will naturally follow, and difficulties in accurately measuring their effectiveness (Bada et al. 2015; Van Steen 2020). In sum, they possess notable weaknesses impacting their ability to create a cyber resilient public. This reality further motivates our work and the value of investigating whether lessons from creating a resilient public during the pandemic may be transferable to the public cybersecurity space.

3. Building resilience against ransomware: learning from SARS-CoV-2 amid a (re)envisioning of British cyber security

In the context of the UK's response to the first wave of the SARS-CoV-2 virus in March 2020, the repeated and concerted message to "Stay at Home, Protect the NHS, Save Lives" demonstrates the importance of effective crisis communication. The UK Government's parliamentary committee report on *Coronavirus: Lessons Learned to Date*, from November 2021, was particularly complimentary of the messaging in the early part of the pandemic because it was clearly articulated and "plainly explain[ed] why they [the public] were being asked to change their behavior" (UK Parliament 2021, 54). Indeed, research from UCL during the first phase of the pandemic has shown that the messaging from government was important in ensuring the public followed the rules, with compliance by individuals shown to be very high (ibid).

Significantly, this type of messaging befits the frame of securing the symbiotic relationship between lives, livelihoods and vital systems. In order to maximize longevity of human life in the face of a novel virus, the behaviors of individuals needed to urgently change in order to prevent the health service from becoming so over-subscribed that societally unpalatable aggressive triaging would need to be put in place. The SARS-CoV-2 pandemic was the first instance in living memory when the UK government implemented overt legislation precisely to mandate the population to significantly alter their behavior to protect the health service as a referent object in its own right. We propose that learning from these successes, as well as the failures, can help to inform a more effective approach to the UK in the field of cyber-security.

Importantly, this article does not argue that the SARS-CoV-2 pandemic is directly comparable or equivalent to a cyber crisis caused by ransomware. SARS-CoV-2 has caused tremendous costs to the UK further afield, both in terms of lives and livelihoods. In the UK, mortality data suggests that excess deaths were 14% above the five-year average and that the virus itself was the leading cause of mortality for the year, despite the first officially recorded SARS-CoV-2 death only being registered in March (OfNS 2021). As of September 2022, it is estimated that the combined governmental cost of the pandemic, including operational expenditure, in addition to support for healthcare, social care, public services, businesses and individuals is in the region of £376 billion (NAO 2021), and as noted in the introduction, the estimated fatality rate of the pandemic exceeds 6,482,338 people globally (WHO 2022).

Although known ransomware incidents have caused disruption to key public services—including healthcare provision, local council services, food production, and retail (Ahlander and Menn 2021; BBC News 2021; Bing and Kelly 2021; Palmer 2021; Shah 2021; Sheridan 2021), these have been significantly narrower, less protracted and less costly than the SARS-CoV-2 pandemic. However, the specific argument put forward in this article is that despite the differences in scale, there are lessons to be learned regarding the transferable practices that may be useful to inform future preparedness and responses for disruptive ransomware incidents (see also Kindervag 2020; Slade 2021; Davis and Pipikaite 2020) both in terms of overall strategy and the communication of risk.

As noted above, the *Coronavirus: Lessons Learned to Date* report, prepared by the Health and Social Care and Science and Technology parliamentary committees, highlights 22 overarching lessons in various areas of the emergency response to the Sars-CoV-2 pandemic, as well as specific lessons on preparedness and communication (UK Parliament 2021, see pp. 6–9, 29–31 and 53–56). We want to begin by highlighting what we view as the key transferable lessons from this report for preparedness, in relation to cyber-security threats like ransomware. Specifically, there are three recommendations that are most relevant to the issue of cyber-security preparedness.

First, the drawing of expertise from "a wider range of disciplines" and the development of plans that are informed by international best practice. In particular, the UK government should "ensure comprehensive plans are made for future risks and emergencies," with the aim that the UK should "be a world leader in co-ordinating international resilience planning" (ibid, 30). Second, related to this, is the recommendation that the UK develop capacity that can allow government to "scan the horizon for future threats." Third, the need to ensure "arrangements [are] established and tested to allow immediate flows of data between bodies relevant to an emergency response." This is important—as the report acknowledges—because in the early days of a crisis, "data may be unavailable, knowledge limited and time may be required for analysis to be conducted. In these circumstances it may be appropriate to act quickly, on a precautionary basis, rather than wait for more scientific certainty" (see UK Parliament 2021, 59). Indeed, in a cyber-security incident like a ransomware attack, it is essential that quick action is taken to prevent an initial system breach leading to wider privileged access, which may, in turn, lead to the exfiltration of valuable data or malicious encryption of systems and data. An individual's, organization's, and government's ability to "scan the horizon" for ransomware and cyber threats is problematized by the dynamic nature of the threat, amidst an arms race between cyber criminals and the cyber security industry (Kesan and Hayes 2017; MacColl, Nurse, and Sullivan 2021). Whilst many ransomware strains and initial access toolkits are known, there is a perennial—and implicitly unavoidable—risk of a "zero day" incident. "Zero day" refers to a cyber-attack, toolkits and methods that are previously unknown. In the event of a Zero Day incident, data may be unavailable and knowledge may be limited.

Taking these lessons forward, we can see that the development of various UK cyber-security strategy documents reflects a commitment to planning for future emergencies in this area. For example, the 2021 *Integrated Review of Security, Defence. Development and Foreign Policy* (Cabinet Office 2021a), reflects a significant SARS-CoV-2 era updating of the UK's ambitions for security and resilience. Although the document references ransomware only once, it is important in terms of a post-2020 reframing of security policy. Indeed, meeting the objectives of this *Review* would necessitate "significant changes and shifts in policy," involving better anticipation of crises, as part of a process of "learning from covid-19" (ibid), which reflects the type of recommendations made in the *Coronavirus: Lessons Learned to Date* report.

Furthermore, the *National Cyber Security Strategy* and *Government Cyber Security Strategy*, formally released in 2022, demonstrate the UK government's overt maneuvering toward securing cyberspace through a whole-of-society endeavor, with networked systems articulated as central to UK security and prosperity. "Preparedness" and "resilience" are foundational themes of the strategy documents. For instance, the

National Cyber Strategy has already begun the process of "horizon scanning" for future threats. The document states that it "is our plan to ensure that the UK remains confident, capable and resilient in this fast-moving digital world," with a focus on creating "a more secure and resilient nation, better prepared for evolving threats and risks and using our cyber capabilities to protect our citizens against crime, fraud and state threats," including "ransomware and other cyber attacks" (Cabinet Office 2022a, 8, 11). Ransomware was highlighted as "the most significant cyber threat facing the UK in 2021," and that given "the likely impact of a successful attack on essential services or critical national infrastructure, the NCSC assessed ransomware as potentially as harmful as state-sponsored espionage" (ibid, 26).

Similarly, subtitled "building a cyber resilient public sector," the *Government Cyber Security Strategy* is replete with references to cyber resilience, mentioning resilient/resilience/resiliency 92 times (Cabinet Office 2022b). The *Government* strategy, with an anticipated lifespan of 2022–2030, notes that "we must meet our responsibility to ensure that government's functions and services are resilient to the cyber threats they face," and that British legitimacy and authority as a cyber power is "dependent upon its domestic cyber resilience, the cornerstone of which is government and the public sector organisations that deliver the functions and services which maintain and promote the UK's economy and society" (ibid, 7, 8). Key overarching deliverables anticipated by the *Government* strategy include significant hardening of critical government functions by 2025 and public sector resilience against known cyber vulnerabilities by 2030 (ibid). Strategies, however, are not policy; as the *Integrated Review* noted, domestic legislation and international arrangements are likely to be required to put the intention(s) of the strategies into practice (Cabinet Office 2021a).

With its potential to harm the functioning of critical services, particularly through intentional denial of system functions, ransomware poses an acute challenge to cyber resilience. Both ransomware and SARS-CoV-2 may be regarded as multi-system dilemmas (Hynes et al. 2020; Gjerde 2021a). Recent research has drawn similarities between the two phenomena, suggesting that they represent "creeping crises"; complex threats that develop incrementally (Boin, Ekengren, and Rhinard 2021). Crises and risks can also compound one another; the *Government* strategy emphasized that "the covid-19 pandemic exacerbated [cyber security risks] as well as fundamentally changing how government works" (Cabinet Office 2022b, 16). Similarly, a "dramatic" rise in ransomware attacks, including the targeting of healthcare, education and other essential services, meant that cyber-attacks are themselves posing "a real risk to public safety" (ibid, 17). This befitted the prior framing posed in the *Integrated Review*, wherein transnational challenges—including cyber risks—could overlap and reinforce one another (Cabinet Office 2021a). This is a logical framing of scope of ransomware—and other cyber—risk. Ransomware intentionally leverages disruption and/or data exfiltration against a given electronic system, but the impact of such an incident is unlikely to be restricted to "cyberspace"; cyberspace is, instead, intrinsically linked to tangible critical or societally-functional systems. A ransomware incident that could potentially impact Supervisory Control and Data Acquisition (SCADA) systems for water and sewage networks, for instance, acquires its significance because it is impacting water supplies (Irwin 2022). Preparation for a cyber incident should, therefore, be multi-domain, and vice-versa; i.e. health catastrophe or water resilience preparedness strategies should incorporate preparedness for the reality of the risk of a disruptive cyber incident.

It is also worth highlighting that, whilst initially relatively banal, the severity of ransomware incidents has increased significantly, particularly since the mid-2010s. Between 2019 and 2020, the average ransom value paid by victim organizations in Europe, the USA and Canada trebled, reaching $312,493 (Osborne 2021). There is a concerted risk that ransomware attacks may become more severe in their societal impact, becoming a source of major disruption. This may particularly be the case if criminals or geopolitical actors engage in the strategic targeting of vital systems, a phenomenon that would be emblematic of overlapping, compounding risk(s) (Cabinet Office 2021a). Again, referring back to the lessons drawn from the response to Sars-CoV-2, the need to act preemptively, "quickly, [and] on a precautionary basis" (UK Parliament 2021, 59) when ransomware attacks do occur seems pertinent advice. Ransomware, and cyber threats, thus befit a basket of potential systemic risks, whereby a ransomware incident that ostensibly occurs or begins outside the UK could nonetheless severely impact critical functions inside the UK (Cabinet Office 2021a). Preemptive action to mitigate this risk when it does occur becomes essential, including, but not limited to: network scanning to identify system breaches before perpetrators can navigate to more privileged systems, offline segmented backups (which can be uploaded rapidly to restore a system or data), regular patching cadence, and rapid quarantine of infected systems where malware is identified The UK government has a history of such quarantine running as far back as the first major international cyber security incident, known as the ILOVEYOU worm. The ILOVEYOU worm—an unintentional international cyber event in May 2000—spread via a vulnerability affecting Microsoft Outlook software when users opened a malicious file in a "love letter" email. As a precautionary and preventative measure, the UK Parliament switched off Outlook systems for several hours (White 2020).

As the recent Ransomware Taskforce report highlighted, there is no "silver bullet" to diminish the threat of ransomware (IST 2021). However, in the absence of an easy-fix, and particularly given the potential capacity for ransomware to cause severe disruption to vital systems, there is a clear rationale to consider sociotechnical measures that could improve both preparedness for, and responses to, ransomware breaches. The authors will now focus specifically on some transferable lessons-learned from the SARS-CoV-2 pandemic relating to establishing a clear communication strategy and developing the necessary levels of comprehension amongst stakeholders.

4. Communicating and understanding ransomware risk: case studies

In the event of a significant and disruptive cyber event impacting the general public, effective crisis management benefits from clear and accessible communication (Netten and Someren 2011; Palttala and Vos 2012). Crisis communication ought not to be viewed within a trajectory vacuum of the crisis itself, but is instead a continuum; beginning long before the crisis occurs and continuing once the crisis has abated. More specifically, a crisis communication strategy should incorporate pre-crisis prevention, crisis preparation, crisis response, and evaluation(s) of responses that are triggered (Reynolds and Seeger 2005; Palttala and Vos 2012). A crisis communication strategy befits an "anticipatory security" lens (Anderson 2010), wherein future security threats are modeled in order to put in place measures that either prevent the threat from emerging and/or increase the resilience of the referent object(s).

With respect to the SARS-CoV-2 pandemic, the UK's public health messaging strategy emerged as a result of unfolding events, and was also informed by a cumulative history of pandemic preparedness planning, particularly with respect to influenza strategizing. In 2011, for instance, the government published an *Influenza Preparedness Strategy* (Department of Health). Section 5 of this document was clear regarding the importance of a coherent communication approach, noting that "consistent, clear public messaging, aligned at national and local level, is critical to a successful and collaborative UK-wide response to a pandemic" (ibid, 45). The core purposes of a pandemic strategy were, respectively, to explain the outbreak, establish confidence, and minimize the risk of infection (ibid). This strategy reflected archetypal high-level pandemic plans, which may be expected to focus on communicating information between stakeholders and to the public, in addition to maintaining the viability of health services to provide both routine and pandemic provision (Loveday and Wilson 2021).

Public authorities often use simulations to assess the modalities of preparedness strategies and protocols. In 2016, a three-day exercise took place involving 950 people to assess the pandemic response efficacy of the Department of Health and twelve other government departments. Modeling the seventh week of a significant avian influenza outbreak, this simulation, known as "Exercise Cygnus," identified significant shortfalls in preparedness (The Times 2016). An Institute for Government (2020) report suggested that although Cygnus had highlighted issues with respect to communication strategy, inter-governmental and inter-sector communication had still been inadequately addressed by the time that SARS-CoV-2 reached the UK.

With respect to the beginning stages of the pandemic's spread to European nation-states, the UK government's preparation and communication strategy has been criticized as having been too slow, indecisive and insufficiently alert amidst a "fog of uncertainty" (Boin, Lodge, and Luesink 2020). Situational awareness was initially delegated to the Health Secretary, when prompter Prime Ministerial ownership may have facilitated greater explanatory communication to the British public (Sanders 2020). This assessment would suggest that delayed situational awareness within government propagated a delayed messaging campaign, which, in turn, hampered initial efforts to curtail the spread of the virus. Whilst the UK is not alone in exhibiting inadequacies in its SARS-CoV-2 communication implementation (for instance, see Gjerde 2021b), other states, such as Singapore—which have had previous experience with a SARS virus—have been regarded as having used more effective communication strategies. For states that chose to supress the virus, such as Singapore, this, in turn, reduced the spread and harms caused by SARS-CoV-2 before vaccine programmes commenced (Campbell and McGregor 2020).

This also raises a pertinent point; SARS-CoV-2 is not synonymous with influenza. Whilst the symptoms themselves may be similar, SARS-CoV-2 is more infectious, has a general capacity to induce more severe illness, and can remain contagious for a longer duration (CDC 2022b). Some patients who recover from SARS-CoV-2 also appear to suffer from longer-term complications, including diminished multi-organ function (CDC 2021). An *influenza* pandemic preparedness strategy may have significant transferable protocols, but there may also be points of divergence. A key lesson here then is that pandemic preparedness strategies ought, in this regard, to be adaptable and nuanced. In a similar vein, cyber-incident preparedness strategies should account for the dynamic nature of the threat, the widening scope of the threat landscape, and the varying motivations of threat actors.

For instance, lessons-learned from the WannaCry worm ransomware that impacted NHS Trusts (Department of Health 2017) may not automatically be transferable to another ransomware toolkit or actor. On a basic level, the WannaCry worm was an indiscriminate weapon; the NHS Trusts were impacted because they were using unpatched instances of Microsoft software, not because they were directly and intentionally targeted. Regular patching cadence would, likely, have prevented or at least mitigated the spread of the WannaCry worm in NHS Trusts (NAO 2018), but patching alone would not prevent a well-resourced actor that is intentionally developing a disruptive attack against an NHS Trust or third-party systems upon which the health system relies. In a threat environment where no electronic system can have absolute security (if an attacker is sufficiently determined), and Zero Day exploits are a perennial reality, in the interests of limiting the scope and impact of future ransomware incidents impacting societally-significant systems, it is essential that plans and exercises are in place to ensure that all relevant stakeholders have a plan of action in the event of a breach. Such a plan should work to ensure that vital services can continue (or be restored as soon as possible). They should also seek to prevent wider network infiltration and damage.

In a recent article on effective government communication strategies, Hyland-Wood et al. (2021) propose ten recommendations for effective pandemic communication, including: engage in clear communication; strive for maximum credibility; communicate with empathy; communicate with honesty; recognize that uncertainty is inevitable; account for levels of health literacy; empower people to act; appeal to social norms; consider diverse community needs; and proactively combat misinformation. We argue these recommendations correlate—albeit in nuanced ways—with communication strategies that could be used in a societally-disruptive ransomware crisis.

In principle, malware and viruses are very different; one being comprised of proteins and a nucleic acid core, the other built around binary digits that form computer language. However, it is nonetheless the case there are correlating similarities between the two. As Kostadimas, Kastampolidou, and Andronikos (2021, 7) write, “the correlation between computer viruses and biological viruses offers an alternative look and approach on how to deal with both biological and computer viruses.” Clearly, the communication strategies surrounding biological viruses will differ from those relating to computer viruses, given that the former infects human beings and the latter infects computers. However, given that—taking the example of malware—malware can extend beyond purely technical damage and can cause societal-level disruption (Agrafiotis et al. 2018), there may be instances wherein governmental communication strategies are required to, again, explain the outbreak, establish confidence and minimize the spread of, and harm caused by, the nefarious code.

The UK has already experienced a societally-disruptive ransomware incident that could, possibly, have endangered lives. This was the aforementioned WannaCry incident in May 2017, which indiscriminately spread to unpatched Windows systems, exploiting a flaw in the message block protocol. Impacted systems included some computers in NHS Trusts. A retrospective analysis identified that hospitals with infected machines experienced a 6% drop in admissions and also had to cancel 13,500 outpatient appointments (Ghafur et al. 2019). Whole-of-public government communication relating to the incident was, however, succinct and limited. On the day the breach was first reported, then-Prime Minister Theresa May spoke briefly to the media, reassuring the public that the attack did not specifically target the NHS, that the NCSC was providing support to NHS Digital, and that there was no evidence that patient data had been compromised (The Guardian 2017). Three days later, after accusations of "hiding," the Health Secretary Jeremy Hunt informed the BBC that he had been briefed by GCHQ and NCSC, that the intelligence indicated that there did not appear to be a "second wave" of attacks, and that "everyone" had a responsibility to prevent ransomware incidents (Revesz 2017). Arguably, the government's relatively light-touch communication strategy was given a reprieve by Marcus Hutchins's identification and deployment of WannaCry's "kill switch" (Hern and Levin 2017). A more disruptive ransomware incident may warrant regular national updates from Cabinet Ministers and officials. A July Department of Health (2017) report incorporated a section on lessons-learned from the ransomware attack, including a renewed focus on communications training for staff and leadership.

The UK has also experienced localized societally-disruptive ransomware incidents, which have proven to be more protracted than the WannaCry event. These include the Redcar & Cleveland and Hackney council ransomware incidents of 2020. In February 2020, Redcar & Cleveland experienced a ransomware attack left staff without access to council computers, tablets or mobile devices, depriving 135,000 of online public services (Pidd and Robinson 2020). With respect to Hackney council, the original ransomware attack against the council's systems occurred in October 2020, and impacts to its services, including benefits, council tax payments, council house repairs and enquiries were disrupted for months thereafter (Glanville 2021). In January 2021, the hackers released some council staff and resident sensitive information, including alleged passports and photo identification (Sheridan 2021). Payment information was reportedly unexposed (Stupp 2021). During the WannaCry and local council incidents, there is no allegation that ransoms were paid. Although UK public bodies are not expressly forbidden from paying ransoms, there is understandable anxiety about taxpayers money being used to finance crime.

In contrast to the WannaCry incident, which impacted multiple NHS Trusts, UK Ministers did not issue public-facing crisis communication with respect to the council ransomware cases. Given the degree of disruption to services used by local residents, the councils themselves released information, but—like many archetypal victims of cyber-attacks—also appeared reticent to provide great detail. For instance, Redcar & Cleveland council initially reported that it had been targeted by a cyber-attack, and waited almost three weeks before publicly disclosing that this was a ransomware incident (Palmer 2021). On October 13th, Hackney mayor, Philip Glanville, announced that the council had been targeted by a "serious cyberattack, which is affecting many of our services and IT systems" (2020), but through November, December and into the new year, the council did not disclose the nature of the cyberattack. In this case, disclosure that the attack was ransomware was, in effect, provided by the criminals themselves, after they published stolen data onto a darknet service (Sheridan 2021). At this stage, Glanville decried the deplorable criminality and the releasing of personal data, noted that the council was working closely with the police, and confirmed that further information would be shared as soon as possible (ibid). On both occasions, Glanville highlighted that the cyber-attack compounded an already difficult situation, because of the ongoing SARS-CoV-2 pandemic (ibid; Glanville 2020).

The release of data befits a recent trend in ransomware attacks; "double extortion," wherein perpetrators steal data in advance of delivering their encrypting payload, so that they can leverage the illicit data, by threatening its release or sale, to further persuade victims to pay a demanded ransom (Logan et al. 2021). The Hackney case illustrates a pertinent quandary for victims of cyber-attacks, particularly those handling personal information and providing key services; the victim does not have a monopoly on public-facing communication with respect to the attack, and there may be instances where the criminals will release details to the public themselves.

From the perspective of an essential services organization, becoming a victim of ransomware and handling incident response is an extremely stressful situation. This is intentionally so, to increase likelihood of potential ransom payment. The foremost desire is likely to be to return system functionality as soon as possible. But, clear, timely and balanced communications to the public will be necessary, too. Here, central government can provide not only technical incident response services (i.e. through the NCSC), but can also offer guidance to help shape successful communication strategies before, during, and after an incident occurs. As the *Government* strategy notes in reference to the council ransomware incidents, "despite the relatively small size of these organisations the impact on critical public services was disproportionate and acute" (Cabinet Office 2022b, 16). A successful communication strategy could serve to mediate the public's interaction with the disruption; an unsuccessful strategy could exacerbate it. Aligning upon a successful communication strategy is thus an important element of preparedness and response. Similarly, government entities have a responsibility not only to communicate during a crisis, but also before a crisis occurs; communication about *risk* serves to both help mitigate an incident from occurring, and also to make the public aware of what may happen should an incident take place. Indeed, following a recent UK government call for evidence to inform an upcoming *National Resilience Strategy* (Cabinet Office 2021b), 80% of respondents reported that they believed more could be done to communicate risk at both national and local levels, with broad consensus that there should be greater transparency and accessibility with respect to risk information (Cabinet Office 2021c).

With respect to communicating risk, the SARS-CoV-2 pandemic established a precedent. The government not only used available data to keep the population informed of the scale of the pandemic, but they also actively encouraged public, academic and industry participation in using this data to feedback into the response efforts. For instance, in an unusual step, priority UKRI funding was specifically offered for projects that could innovate improvements in current and future pandemic responses (UKRI 2021). Existing grant holders also had the opportunity to switch their funding from a non-pandemic project to a SARS-CoV-2 focus (ibid). Members of the public were also vested with the opportunity to participate in "hackathons"—free of charge—in which they could experiment with large datasets in order to provide insights on the pandemic and possible innovations (Bolton et al. 2021; Royal Statistical Society 2020). Arguably, where possible, and dependent on data availability, similar initiatives should be encouraged with respect to ransomware. In the absence of a present "silver bullet" to prevent ransomware and its associated harms (IST 2021), improved data availability, sharing and analysis could highlight social or technical tweaks that could serve to reduce the scope for ransomware to be societally disruptive. As outlined in the below analysis of the two substantive cyber-focused *Strategy* documents produced by the UK government in 2022 (Cabinet Office 2022a, 2022b)—the first of their kind since the pandemic—there is evidence that lessons are being learned, for the benefit of societal (cyber) resilience.

5. Communicating and understanding ransomware risk: the strategy documents

The UK government's recent strategy documents indicate a concerted effort toward improving the UK's cyber resilience, including improvements to communicating and understanding cyber risk amongst stakeholders. The *National Cyber Strategy* and *Government Cyber Security Strategy* respectively are instructive in this regard.

With respect to keeping key stakeholders informed and involved in managing cyber risk, the *National* strategy (Cabinet Office 2022a) detailed: the NCSC's "Active Cyber Defence" programme, which includes early warning systems for government bodies; an intention to "embed" cyber security practices and awareness amongst all public sector workers; an intention to establish clear mechanisms for timely information sharing and alerts—including a common reporting process and language within government organizations—and, additionally, an intention to establish a culture in which cyber security "near misses" and minor incidents can be reported without associated embarrassment or blame. Similarly, the *Government* strategy (Cabinet Office 2022b) noted: affirmation of the GBEST scheme, a simulated attack framework designed to assess the efficacy of a government bodies' cyber security standing; the intention to establish the Government Cyber Coordination Center (GCCC), to transform how cyber security data and intelligence can be shared and actioned across government entities; the desire to implement enhanced coordination to gather and use risk data; as well as the intention to adopt the Cyber Assessment Framework (CAF) as a standardized cyber resilience monitoring tool across government.

CAF (NCSC 2022), in essence, is the intended standard language for cyber resilience across government. Government entities may be free to assess their cyber resilience by their own means, but should nonetheless adopt CAF profiles suitable for their organization to enable cross-government visibility and comparability (Cabinet

Office 2022b). The *Government* strategy itself is to be governed by a continually evolving performance framework that reports to senior officials and the National Security Council (ibid). Whilst this framework will not be disclosed publicly, the government will publish public-facing annual progress reports (ibid). Similarly, the risk-oriented National Security Risk Assessment (NRSA)—a document detailing the impact and likelihood of the most severe risks facing the UK—is classified, the government provides a public-facing version in the form of the National Risk Register (Cabinet Office 2021a). The *Integrated* review noted that the methodology of this document was being reevaluated in light of the SARS-CoV-2 pandemic, with a particular need to account for "interdependencies, cascading and compound risks" (ibid).

Understandably, the *National Cyber Strategy* and *Government Cyber Security Strategy* documents are weighted toward high-level stakeholders. Nonetheless, two key non-government bodies are highlighted: the general public and firms (articulated as business, organizations, citizens, sole traders and small organizations) and "network defenders," spanning a "wide variety of sectors" (with whom the NCSC has trialed initiatives for network defence collaboration). Former Health Secretary Jeremy Hunt was correct when he stated, during the WannaCry incident, that everyone has a responsibility to prevent ransomware and cyber-attacks (Revesz 2017). Accordingly, for business and citizen-facing cyber resilience, the government would "ensure messages are consistent, clear and provided through the most effective channels, whether via the Cyber Aware campaign, NCSC website, government, law enforcement networks or partnerships with industry" (Cabinet Office 2022a, 73). Whilst cyber awareness campaigns are a necessity, it is not necessarily clear that they are effective; efforts should be made to assess the efficacy of these campaigns (see Bada, Sasse, and Nurse 2015). Ultimately, cyber awareness campaigns seek to improve the familiarity of a target audience—as broad as the general public—with common cyber risks and measures that may be taken to prevent them occurring. They may, however, be less focused on what stakeholders should do in the event of an incident. Here, exercises and wargaming can take a more prominent role, to improve socio-technical familiarity with the steps that should be taken in the event of a cyber incident, including ransomware. The *Government Strategy* reinforces this, noting that as part of the NCSC's "Active Cyber Defence," organizations could take advantage of a self-service "Exercise in a Box," which presents personnel with realistic scenarios (in a safe environment) to practice and refine cyber incident response (Cabinet Office 2022b, 45). Additionally, the *Strategy* highlights the need to routinely stress-test public sector organizational cyber incident plans on a cross-governmental basis, to account for evolving threats (Cabinet Office 2022b).

Furthermore, with near-universal responsibility for cyber security, communication channels must work both ways; the public must have means to report incidents or concerns. On this point, the *Government* strategy points to the intended replacement of Action Fraud with a new service by 2025, and a general interest in encouraging greater reporting of cyber incidents, particularly amongst regulated sectors (ibid). A perennial current issue with respect to the available breadth and quality of data with respect to ransomware is that organizations who are hit with ransomware may not wish to disclose news of the attack to the general public or to the authorities. Insights may be garnered from the UK's *Cyber Breaches Survey*, with a positive indication of a decline in ransomware incidence, with 17% of attacked organizations reporting that they were hit by ransomware specifically in the 2017 survey, declining to 7% in the 2021 survey and 4% in the 2022 survey (DCMS 2021; DCMS 2022b). However, whilst the survey gives an overarching insight into ransomware incidents generally across a sample of UK organizations, it does not necessarily provide immediately actionable data that could close a shared security loophole or lead to the successful curtailment and prosecution of cyber criminals. This is an area for further improvement. The UK government is active in this space, having recently completed a consultation on mandatory cyber security reporting for essential services (DCMS 2022a).

6. Conclusions

The SARS-CoV-2 pandemic is not directly comparable to a potential societal cyber security crisis induced by ransomware. There are, however, potential crisis management lessons to be learned from the governance of the SARS-CoV-2 response, with an eye to informing the ongoing efforts to improve cyber resilience in the UK, and, indeed, further afield. This is particularly the case given the UK government's recent framing of security threats as increasingly interlinked and cumulative (Cabinet Office 2021a, 2022a, 2022b). Although these potential lessons could be wide-ranging, this article has focused on the lessons that may be learned with respect to crisis communication and understanding between multiple stakeholders. Drawing on the SARS-CoV-2 pandemic, WannaCry worm, Redcar & Cleveland and Hackney council ransomware incidents respectively, this article has sought to bridge potential communication-oriented lessons-learned with the British government's public-facing strategies with respect to cyber resilience.

Although the problems are large—and the article constrained—the key lessons that we have drawn through our comparison between the SARS-CoV-2 pandemic and the scourge of ransomware are as follows. Firstly, stakeholders must continue to create and refine preparedness strategies defining internal and external communication procedures, which account for the dynamism of contemporary ransomware threats. Secondly, given that vulnerabilities may be both social and technical, communication strategies deployed pre-, during-, and post-incident should be multi-layered in their targeting of audiences. The public would require reassurance during a severe ransomware incident impacting local or national essential services—for instance, "Category 4" or above (NCSC 2018b)—and stakeholders would therefore be required to provide regular updates on ongoing impact(s) and the measures being taken to restore functionality. Essential service-providers, or responsible Ministers or local government representatives, should endeavor to avoid giving space for accusations of "hiding," and they should also be conscious that the criminals operating ransomware may themselves post communiques online, to embarrass system-operators or increase pressure to pay. Additionally, the public may also be important actors themselves, in terms of contributing to a society-wide high level of cyber hygiene. Ergo, national and local government, in addition to wider civil society, should continue to develop, review and improve cyber hygiene promotional campaigns. Thirdly, given the potential for overlap between IT security and other societal or national security resilience concerns, cyber resilience communication strategies should be addressed across and within wider resilience strategies, and vice-versa.

Whilst the strategy documents are promising in this regard, domestic policymaking and international negotiation will be required to implement their ambitions. Ultimately, resilience is a continual work-in-progress, particularly with respect to cyber resilience, wherein the threat is intrinsically dynamic. In the interests of securing networked societies and the networks upon which they rely, we should be open-minded and consider lessons from wide-ranging sources. If threats and risks can be interlinked and cumulative, so can the lessons-learned.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Gareth Mott http://orcid.org/0000-0002-8788-769X

References

Agrafiotis, I., J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton. 2018. “A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate.” *Journal of Cybersecurity* 4 (1): 1–15. doi:10.1093/cybsec/tyy006.

Ahlander, J., and J. Menn. 2021. “Major Ransomware Attack Against US Tech Provider Forces Swedish Store Closures.” *Reuters*, 4 July 2021. Accessed 27 September 2021. https://www.reuters.com/article/usa-cyber-kaseya-sweden-idCNL2N2OF0GE.

Anderson, B. 2010. “Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies.” *Progress in Human Geography* 34 (6): 777–798. doi:10.1177/0309132510362600.

Ashley, R. 1988. “Understanding the Sovereign State: A Double Reading of the Anarchy Problematique.” *Millennium* 17 (2): 227–262. doi:10.1177/03058298880170020901.

Bada, M., M. Sasse, and J. R. C. Nurse. 2015. “Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?” In *International Conference on Cyber Security for Sustainable Society*.

Baker-Beall, C. 2016. *The European Union’s ‘Fight against Terrorism’: Discourse, Policies, Identity*. Manchester: Manchester University Press.

BBC News. 2020. “In full: Johnson orders UK to ‘Stay Home’ to Protect NHS from Coronavirus.” 23 March 2020. Accessed 3 September 2021. https://www.bbc.co.uk/news/av/uk-52012583.

BBC News. 2021. “Meat Giant JBS pays $11m in Ransom to Resolve Cyber-attack”. Accessed 3 September 2021. https://www.bbc.co.uk/news/av/uk-52012583.

Bevir, M., O. Daddow, and I. Hall. 2013. “Introduction: Interpreting British Foreign Policy.” *The British Journal of Politics and International Relations* 15 (2): 163–174. doi:10.1111/j.1467-856X.2012.00537.x.

Bing, C., and S. Kelly. 2021. “Cyber Attack shuts down US Fuel Pipeline ‘Jugular’, Biden Briefed.” *Reuters*, 8 May 2021. Accessed 3 September 2021. https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/.

Bodeau, D. J., R. Graubart, J. Picciotto, and R. McQuaid. 2011. "Cyber Resiliency Engineering Framework". *MITRE CORP United States*, 9 January. Accessed 26 April 2022 https://apps.dtic.mil/sti/citations/AD1108457.

Boin, A., and A. McConnell. 2007. "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience." *Journal of Contingencies and Crisis Management* 15 (1): 50–59. doi:10.1111/j.1468-5973.2007.00504.x.

Boin, A., M. Ekengren, and M. Rhinard. 2021. *Understanding the Creeping Crisis*. Cham: Palgrave Macmillan.

Boin, A., M. Lodge, and M. Luesink. 2020. "Learning from the Covid-19 Crisis: An Initial Analysis of National Responses." *Policy Design and Practice* 3 (3): 189–204. doi:10.1080/25741292.2020.1823670.

Bolton, William S., Shu Ng, Angela Lam, James Kinch, Victor Parchment, William P. Foster, Manuela R. Zimmermann, et al. 2021. "Virtual Hackathon to Tackle Covid-19 Unmet Needs." *BMJ Innovations* 7 (2): 284–287. doi:10.1136/bmjinnov-2020-000456.

Cabinet Office. 2017. *Public Summary of Sector Security and Resilience Plans*. London: Cabinet Office.

Cabinet Office. 2021a. *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*. London: Stationary Office.

Cabinet Office. 2021b. "National Resilience Strategy: Call for Evidence." *Gov.uk*, 13 July 2021. Accessed 27 April 2022. https://www.gov.uk/government/consultations/national-resilience-strategy-call-for-evidence.

Cabinet Office. 2021c. "Public Response to Resilience Strategy: Call for Evidence." *Gov.uk*, 15 December 2021. Accessed 27 April 2022. https://www.gov.uk/government/consultations/national-resilience-strategy-call-for-evidence/outcome/public-response-to-resilience-strategy-call-for-evidence.

Cabinet Office. 2022a. *National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK*. London: Stationary Office.

Cabinet Office. 2022b. *Government Cyber Security Strategy: Building a Cyber Resilient Public Sector*. London: Stationary Office.

Campbell, E., and L. McGregor. 2020. "These Five Strategies have helped Singapore fight off the Coronavirus Outbreak. Can then keep it at bay?" *ABC*, 31 March 2020. Accessed 30 September 2021. https://www.abc.net.au/news/2020-03-31/coronavirus-singapore-how-it-fought-the-virus/12100072.

Carías, J., M. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes. 2020. "Systematic Approach to Cyber Resilience Operationalization in SMEs." *IEEE Access*. 8: 174200–174221. doi:10.1109/ACCESS.2020.3026063.

CDC. 2021. "Post-Covid Conditions." *Centers for Disease Control and Prevention*, 16 September 2021. Accessed 27 April 2022. https://www.cdc.gov/coronavirus/2019-ncov/long-term-effects/index.html.

CDC. 2022a. "About Variants." Centers for Disease Control and Prevention 25 February 2022. Accessed 26 April 2022. https://www.cdc.gov/coronavirus/2019-ncov/variants/about-variants.html.

CDC. 2022b. "Similarities and Differences between Flu and Covid-19." *Centers for Disease Control and* Prevention 18 January 2022. Accessed 27 April 2022. https://www.cdc.gov/flu/symptoms/flu-vs-covid19.htm.

CISA. n.d. "Ransomware 101." *Cybersecurity and Infrastructure Security Agency*. Accessed 3 September 2021. https://www.cisa.gov/stopransomware/ransomware-101.

Coutu, D. 2002. "How Resilience Works". *Harvard Business Review*, May 2002. Accessed 26 April 2022. https://hbr.org/2002/05/how-resilience-works#:~:text=Resilience%20is%20a%20reflex%2C%20a,Others%20do%20not.

Davis, N., and A. Pipikaite. 2020. "What the Covid-19 Pandemic Teaches us about Cybersecurity – and how to Prepare for the Inevitable Global Cyberattack." *World Economic Forum*, 1 June 2020. Accessed 30 September 2021. https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus.

DCMS. 2021. “Cyber Breaches Survey 2021.” *Department for Digital, Culture, Media and Sport*, 24 March 2021. Accessed 27 April 2022. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021.

DCMS. 2022a. “Proposal for Legislation to Improve the UK’s Cyber Resilience.” *Department for Digital, Culture, Media and Sport*, 19 January 2022. Accessed 27 April 2022. https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience.

DCMS. 2022b. “Cyber Breaches Survey 2022.” *Department for Digital, Culture, Media and Sport*, 30 March 2022. Accessed 27 April 2022. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022.

Department of Health. 2011. *UK Influenza Pandemic Preparedness Strategy 2011*. London: Department of Health.

Department of Health. 2017. *Your Data: Better Security, Better Choice, Better Care*. London: Department of Health.

Doty, R. 1998. “Immigration and the Politics of Security.” *Security Studies* 8 (2–3): 71–93. doi: 10.1080/09636419808429375.

Ghafur, S., S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin. 2019. “A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS.” *NPJ Digital Medicine* 2 (98): 98. doi:10.1038/s41746-019-0161-6.

Gjerde, L. 2021a. “Governing Humans and ‘Things’: Power and Rule in Norway during the Covid-19 Pandemic.” *Journal of Political Power* 14 (3): 472–492. doi:10.1080/2158379X.2020.1870264.

Gjerde, L. 2021b. “From Liberalism to Biopolitics: Investigating the Norwegian Government’s Two Responses to Covid-19.” *European Societies* 23 (sup1): S262–S274. doi:10.1080/14616696.2020.1824003.

Glanville, P. 2020. “Serious Cyberattack on Council Systems: Statement.” *Hackney Council*, 13 October 2020. Accessed 27 April 2022. https://news.hackney.gov.uk/council-subject-of-serious-cyberattack/.

Glanville, P. 2021. “Services Available, but not back to Normal – Devastating Impact of Cyberattack One Year on.” *Hackney* Council, 5 November 2021. Accessed 27 April 2022. https://news.hackney.gov.uk/services-available-but-not-back-to-normal–devastating-impact-of-cyberattack-one-year-on/.

Gov.uk. 2022. “UK Coronavirus Dashboard.” Accessed 7 September 2022. https://coronavirus.data.gov.uk/details/deaths?areaType=overview&areaName=United%20Kingdom.

Haldane, Victoria, Chuan De Foo, Salma M. Abdalla, Anne-Sophie Jung, Melisa Tan, Shishi Wu, Alvin Chua, et al. 2021. “Health Systems Resilience in Managing the Covid-19 Pandemic: Lessons from 28 Countries.” *Nature Medicine* 27 (6): 964–980. doi:10.1038/s41591-021-01381-y.

Hern, A., and S. Levin. 2017. “Briton who Stopped WannaCry Attack Arrested over Separate Malware Claims.” The Guardian 3 August 2017. Accessed 30 September 2021. https://www.theguardian.com/technology/2017/aug/03/researcher-who-stopped-wannacry-ransomware-detained-in-us.

Herrington, L., and R. Aldrich. 2013. “The Future of Cyber-Resilience in an Age of Global Complexity.” *Politics* 33 (4): 299–310. doi:10.1111/1467-9256.12035.

Herrman, H., D. E. Stewart, N. Diaz-Granados, E. L. Berger, B. Jackson, and T. Yuen. 2011. “What is Resilience?” *Canadian Journal of Psychiatry. Revue Canadienne de Psychiatrie* 56 (5): 258–265. doi:10.1177/070674371105600504.

Humprecht, E., F. Esser, and P. Van Aelst. 2020. “Resilience to Online Disinformation: A Framework for Cross-national Comparative Research”. *The International Journal of Press/Politics*. 25 (3): 493–516. doi:10.1177/1940161219900126.

Hyland-Wood, B., J. Gardner, J. Leask, and U. Ecker. 2021. “Toward Effective Government Communication Strategies in the Era of Covid-19.” *Humanities and Social Sciences Communications* 8 (1): 1–11. doi:10.1057/s41599-020-00701-w.

Hynes, W., B. Trump, P. Love, and I. Linkov. 2020. “Bouncing Forward: A Resilience Approach to Dealing with Covid-19 and Future Systemic Shocks.” *Environment Systems & Decisions* 40 (2): 174–184. doi:10.1007/s10669-020-09776-x.

Institute for Government. 2020. *How Fit Were Public Services for Coronavirus?* London: Institute for Government.

Irwin, L. 2022. “South Staffordshire Water Targeted by Cyber Attack.” *IT Governance*. Accessed 2 September 2022. https://www.itgovernance.co.uk/blog/south-staffordshire-water-targeted-by-cyber-attack.

IST. 2021. *Combating Ransomware: A Comprehensive Framework for Action*. San Francisco: Institute for Security and Technology.

Kesan, J., and C. Hayes. 2017. “Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment.” *Minnesota Law Review* 102: 192–276.

Kindervag, J. 2020. “Cybersecurity Lessons from the Covid-19 Pandemic.” *Palo Alto*. Accessed 30 September 2021. https://www.securityroundtable.org/cybersecurity-lessons-from-the-coronavirus.

Kostadimas, D., K. Kastampolidou, and T. Andronikos. 2021. ” Correlation of Biological and Computer Viruses through Evolutionary Game Theory.” *arXiv*, 1 August 2021. Accessed 27 April 2022. https://arxiv.org/abs/2108.00508.

Logan, M., E. Mendoza, R. Maglaque, and N. Tamana. 2021. “The State of Ransomware: 2020’s Catch-22.” *Trend Micro*, 3 February 2021. Accessed 27 April 2022. https://www.trend-micro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22.

Loveday, H., and J. Wilson. 2021. “Pandemic Preparedness and the Role of Infection Prevention and Control – How Do we Learn?” *Journal of Infection Prevention* 22 (2): 55–57. doi:10.1177/17571774211001040.

MacColl, J., J. Nurse, and J. Sullivan. 2021. *Cyber Insurance and the Cyber Security Challenge*. London: Royal United Services Institute.

Manyena, S. 2006. “The Concept of Resilience Revisited.” *Disasters* 30 (4): 434–450. doi:10.1111/j.0361-3666.2006.00331.x.

Mott, G. 2019. *Constructing the Cyberterrorist*. London: Routledge.

NAO. 2018. *Investigation: WannaCry Cyber Attack and the NHS*. London: National Audit Office.

NAO. 2021. “Covid-19 Cost Tracker.” National Audit Office 22 September 2021. Accessed 7 September 2022. https://www.nao.org.uk/covid-19/cost-tracker/.

NCSC. 2018a. “Cyber Resilience – Nothing to Sneeze at.” *National Cyber Security Centre*, 4 July 2018. Accessed 8 September 2021. https://www.ncsc.gov.uk/blog-post/cyber-resilience-nothing-sneeze.

NCSC. 2018b. “New Cyber Attack Categorisation System to Improve UK Response to Incidents.” *National Cyber Security Centre*, 11 April 2018. Accessed 7 September 2022. https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents.

NCSC. 2022. “NCSC CAF Guidance.” *National Cyber Security Centre*, 11 April 2022. Accessed 27 April 2022. https://www.ncsc.gov.uk/collection/caf.

Netten, N., and M. Someren. 2011. “Improving Communication in Crisis Management by Evaluating the Relevance of Messages.” *Journal of Contingencies and Crisis Management* 19 (2): 75–85. doi:10.1111/j.1468-5973.2011.00636.x.

Nurse, J. R. C. 2019. “Cybercrime and You: how Criminals Attack and the Human Factors That They Seek to Exploit.” In *The Oxford Handbook of Cyberpsychology*, edited by Attrill-Smith, A., Fullwood, C., Keep, M. and Kuss, D. Oxford: Oxford University Press.

Nurse, J. R. C. 2021. “Cybersecurity Awareness.” In *Encyclopaedia of Cryptography, Security and Privacy*, edited by Jajodia, S., Samarati, P., Yung, M. Berlin: Springer.

OfNS. 2021. “Deaths at Home Increased by a Third in 2020, while Deaths in Hospitals fell except for Covid-19.” *Office for National Statistics* 7 July 2021. Accessed 27 September 2021.

Osborne, C. 2021. "Ransomware has been likened to a Hydra – Cut off one Head, and more appear in its Place." *ZDNet*, 7 June 2021. Accessed 27 September 2021. https://www.zdnet.com/article/the-cost-of-ransomware-around-the-globe-to-go-beyond-265-billion-in-the-next-decade/.

Palmer, D. 2021. "Ransomware: Ireland's Health Service Remains 'Significantly' Disrupted Week after Attack." ZDNet 4 June 2021. Accessed 27 September 2021. https://www.zdnet.com/article/ransomware-irelands-health-service-is-still-significantly-disrupted-weeks-after-attack.

Palttala, P., and M. Vos. 2012. "Quality Indicators for Crisis Communication to Support Emergency Management by Public Authorities." *Journal of Contingencies and Crisis Management* 20 (1): 39–51. doi:10.1111/j.1468-5973.2011.00654.x.

Petrenko, S., and D. Vorobieva. 2019. "Method of Ensuring Cyber Resilience of Digital Platforms Based on Catastrophe Theory." In *2019 XXII International Conference on Soft Computing and Measurements (SCM)*, 97–101. doi:10.1109/SCM.2019.8903658.

Phillips, N. 2021. "The Coronavirus is Here to Stay – Here's What that Means". *Nature*, 16 February 2021. Accessed 3 September 2021. https://www.nature.com/articles/d41586-021-00396-2.

Pidd, H., and G. Robinson. 2020. "Ransomware Attack Leaves Council Facing Huge Bill to Restore Services." *The Guardian*, 27 February 2020. Accessed 27 April 2022. https://www.theguardian.com/technology/2020/feb/27/redcar-and-cleveland-council-hit-by-cyber-attack.

Revesz, R. 2017. "Jeremy Hunt breaks Silence on NHS Cyber Attack, Three Days after Hospitals Plunged into Chaos." Independent, 15 May 2017. Accessed on 30 September 2021. https://www.independent.co.uk/news/uk/home-news/jeremy-hunt-nhs-silence-cyber-attacks-no-second-wave-joint-responsibility-a7736906.html.

Reynolds, B., and M. Seeger. 2005. "Crisis and Emergency Risk Communication as an Integrative Model." *Journal of Health Communication* 10 (1): 43–55. doi:10.1080/10810730590904571.

Royal Statistical Society. 2020. "NERC Covid-19 Hackathons and Kaggle Challenge." *Royal Statistical Society*, 3 June 2020. Accessed 27 April 2022. https://rss.org.uk/news-publication/news-publications/2020/member-callouts/nerc-covid-19-hackathons-and-kaggle-challenge/.

Safi, M. 2021. "Oxford/AtsraZeneca Covid Vaccine Research 'was 97% Publicly Funded'." *The Guardian*, 15 April 2021. Accessed 3 September 2021. https://www.theguardian.com/science/2021/apr/15/oxfordastrazeneca-covid-vaccine-research-was-97-publicly-funded.

Sanders, K. 2020. "British Government Communication during the 2020 Covid-19 Pandemic: Learning from High Reliability Organisations." *Church, Communication and Culture* 5 (3): 356–377. doi:10.1080/23753234.2020.1824582.

Scroxton, A. 2021. "No more Ransom Initiative Saves £850 over Five Years." *Computer Weekly*, 26 July 2021. Accessed 3 September 2021. https://www.computerweekly.com/news/252504478/No-More-Ransom-initiative-saves-850m-over-five-years.

Shah, S. 2021. "Patients Fall Victim to Health Ransomware." *Financial Times*, 26 January 2021. Accessed 27 September 2021. https://www.ft.com/content/acf4ac78-c738-48c6-8de1-077697e062d6.

Shepherd, L. 2008. *Gender, Violence and Security: Discourse as a Practice*. London: Zed Books.

Sheridan, E. 2021. "Cyber Attack to Cost Hackney Council 'Roughly' £10m, Mayor Reveals." *Hackney Citizen*, 23 February 2021. Accessed 27 September 2021. https://www.hackneycitizen.co.uk/2021/02/23/cyber-attack-cost-hackney-council-10m/.

Slade, R. 2021. *Cybersecurity Lessons from Covid-19*. Boca Raton: CRC Press.

Stewart, H., and S. Walker. 2020. "UK Coronavirus UK: Boris Johnson Announces Closure of all UK Pubs and Restaurants." *The Guardian*, 20 March 2020. Accessed 3 September 2021. https://www.theguardian.com/world/2020/mar/20/london-pubs-cinemas-and-gyms-may-close-in-covid-19-clampdown.

Stupp, C. 2021. "London Borough of Hackney Struggles with Recovery Months after Ransomware Attack." *The Wall Street Journal*, 16 July 2021. Accessed 27 April 2022. https://

www.wsj.com/articles/london-borough-of-hackney-struggles-with-recovery-months-after-ransomware-attack-11626427801.

The Guardian. 2017. “Theresa May: ‘this is not targeted at the NHS, it’s an International Attack’ – video.” *Youtube*, 12 May 2017. Accessed 27 April 2022. https://www.youtube.com/watch?v=mfELw3A5gCE.

The Times. 2016. “NHS Fails to Cope with Bodies in Flu Pandemic Test.” *The Times*, 27 December 2016. Accessed 28 September 2021. https://www.thetimes.co.uk/article/nhs-fails-to-cope-with-bodies-in-flu-pandemic-test-8pnmdpdfx.

Tiirmaa-Klaar, H. 2016. “Building National Cyber Resilience and Protecting Critical Information Infrastructure.” *Journal of Cyber Policy* 1 (1): 94–106. doi:10.1080/23738871.2016.1165716.

UK Parliament. 2021. “House of Commons Health and Social Care, and Science and Technology Committees. Coronavirus: lessons Learned to Date. Sixth Report of the Health and Social Care Committee and Third Report of the Science and Technology. Committee of.” Session 2021–22.

UKRI. 2021. “Get Funding for Ideas that Address Covid-19.” Research and Innovation, *UK*. 5 August 2021. Accessed 27 April 2022. https://www.ukri.org/apply-for-funding/coronavirus-funding/get-funding-for-ideas-that-address-covid-19/.

Van Steen, T., E. Norris, K. Atha, and A. Joinson. 2020. “What (If Any) Behaviour Change Techniques Do Government-Led Cybersecurity Awareness Campaigns Use?” *Journal of Cybersecurity* 6 (1): 1–8. doi:10.1093/cybsec/tyaa019.

White, G. 2020. “Love Bug’s Creator Tracked Down to Repair Shop in Manila.” *BBC News*. Accessed 2 September 2022 https://www.bbc.co.uk/news/technology-52458765.

WHO. 2022. “WHO Coronarivus Dashboard”. Accessed 7 September 2022. https://covid19.who.int/.