A Concept of Operations to Embody the Utilization of a Distributed Test, Track and Track System for Epidemic Containment Management

David Bird

Abstract The severe acute respiratory syndrome coronavirus 2 pandemic revealed that many countries had insufficient strategies to conduct test, track, and trace of the viral transmission once infected people entered a country’s borders. Computer science could be used to understand the seats of infection, and hotspots that may fuel potential outbreaks. As well as the added benefit of steering on-the-ground epidemiological surveillance activities to contain further outbreaks. However, there is more to a computerized solution than an architectural design of an end-to-end distributed test, track, and trace system and its use of machine learning technologies. A successful implementation encompasses a number of key areas that include people, processes, and technology. Comparisons are drawn with cyber security operations center use-cases in support of a strategy and concept of operations to enable: (a) front-end test teams at the border chokepoints to collect test samples; (b) cloud processing of test subject records and laboratory test results; (c) emergency operations center containment monitoring; (d) data analysis of test subject groupings to identify hotspot areas; (e) use of epidemiological trends to direct further testing; and (f) conduct epidemiological monitoring to detect new chains of transmission.

Keywords Cloud · Concept of operations · Incident and operations management · Cyber security operations center model

1 Introduction

South Korea learned from their Severe Acute Respiratory Syndrome (SARS) experience when it came to SARS coronavirus 2 (SARS-Cov-2). Because of this they were able to develop and deploy operational polymerase chain reaction (PCR) tests within two weeks at scale [23]. Borders were closed at the start of the pandemic, and epidemiological surveys were prioritized [17]. The South Korean government deployed a track and trace system that utilized multi-source data from the government
as well as medical records and cellular data; hence, locations of credit card transactions and geo-location tracking were used which has consequently been deemed intrusive by the West [9, 30]. Thus, a "big data" approach was used that utilized testing, tracking, and tracing and proved successful in coordinated containment activities. Localized epidemiological response teams were able to contain outbreaks in the community, and this enabled the country to avoid a country-wide lockdown [30]. More recently, SARS-Cov-2 disease of 2019 (COVID-19) outbreaks were still occurring with 76% imported from abroad and 24% sourced domestically from within the country [3, 4]. For a country that has a population that is three quarters the size of the United Kingdom (U.K.), they have had only 441 deaths [46]. South Korea, as well as Germany and New Zealand, all used regional epidemiological teams to root out SARS-Cov-2 and COVID-19 [4].

From a U.K. perspective, the Scientific Advisory Group for Emergencies (SAGE) relied on modeling that was fine tuned for influenza predictions rather than COVID-19 [15, 18]. Several months into the pandemic, University College London highlighted this deficiency, and models were honed using COVID-19 data; the outcomes indicated that because of the U.K.’s initially flawed control plan, closing the border by March would have postponed the inevitable arrival of the pandemic en masse by only 5-days [39]. Subsequently, epidemiology capabilities were overwhelmed and abandoned, and the borders were kept open well into the peak of the pandemic enabling at least 20,000 infected people to enter the country [19, 20, 27]. Consequently, the government changed tact and began to favor “herd immunity by infection” which received critical disparagement [31, 33, 36]. Hence, a country-wide lockdown was instigated [19] followed by a slow response in the scaling up of PCR swab testing that was also labored by a shortage of test laboratories [1]. This was followed by a late reinstatement of epidemiological surveys some six weeks after the “lockdown”.

Precious time was apportioned to the development and testing of a U.K. National Health Service (NHS) Digital Service (NHSX) contact tracing smartphone application (app) which was intended to be used for centralized track and trace efforts. The original NHSX app worked with the android operating system but was inoperable using Apple’s iOS; so, the government changed tact and abandoned this NHSX app variant in preference for the decentralized version that relied on Google and Apple collaborative technology; this capability was only realized in the autumn of 2020 [4]. During the intervening period, the U.K. approach depended upon a call center-orientated trace approach in order to contact people who may have encountered someone suspected of having COVID-19. What has become apparent is better diagnostics are required ideally before the start of a pandemic but certainly as part of a country’s recovery from the ensuing health crisis and critically in preparation for the next epidemic.

This chapter continues the justification for a Distributed Test, Track and Trace System (DTTTS) authored by Bird [3]. Motivated by the difficulties encountered by the U.K. to implement a successful test, track and trace system, this chapter presents a novel approach for implementing such a system that is supported by a service wrap. This chapter is dedicated to justifying the approach of a DTTTS and provides an argument that the concept can be developed further into a useable concept
of operations (CONOPS). The pertinent points from Bird [3] are discussed further, followed by an expansion of ideas comparing this system concept to the analogy of the Cyber Security Operations Center (CSOC). Both approaches are in principle incident response orientated even though the contexts of use and data sources are different. Incident response principles could be used to contribute to epidemic containment management. The related work section presents a case for a DTTTS. This is followed by a discussion section that provides a comparative analysis of a DTTTS in relation to CSOC models. The further work section articulates dependencies that need to be considered and resolved to ensure a DTTTS approach can be achieved.

2 Related Work

The NHS test and trace system had to be instituted without a tracking component and is heavily dependent on the British Public self-notifying the central call center by telephone. In August 2020, the NHS test and trace advisors reached nearly 80 percent people who had tested positive, and 80 percent of these people declared their contacts from which only 66% were further reachable by the service [4]. By October 2020, the U.K. government’s scientific community admitted that they had little confidence in the existing test and trace system—even though it had been augmented by the new NHSX COVID-19 app; still only two thirds of close contacts of people who tested positive could effectively be reached [10,11].

The cloud 2.0 era offers society an opportunity to re-think traditional medical strategies; and adapt our thinking to provide new approaches and methods for epidemic containment in a bid to avert widespread infection and a repeat of this global health crisis. In light of the U.K. Government’s test and trace strategy debates were fueled about its inadequacy, and this section presents a case for a DTTTS, which is proposed as a more reliable systematic approach and crucially has an enabling trackable capability.

2.1 The Case for a Distributed Test, Track and Trace System

A cloud-based DTTTS would bring a “big data” approach to the COVID-19 problem and could enable the U.K. to pursue containment measures in a similar vein to those used by South Korea. Testing would be initially conducted at the borders and this would be less resource intensive and more efficient than testing at scale across the country’s population; thereby lessening the impact on NHS resources. Test subject details would be collected at transport hubs; swab tests would be taken and then dispatched to laboratories, where test outcomes would be centrally appended to records [3]. Test subjects would then be instructed to quarantine at their declared addresses until the results are received. An Emergency Operations Center (EOC) would then monitor this data store using Machine Learning (ML) algorithms [21] to
keep an eye on hotspot clusters of positively tested subjects and utilize trending to notify regional authorities of greater congregations; as well as direct concentrated and targeted epidemiological surveillance activities [3]. Moreover, Smith [41] showed how cyber defense principles could provide insights for the medical profession. Bird [3] provided a comparison of cyber versus epidemic incident response measures, which compares the two disparate domains revealing their relatable similarities.  

- **Cyber security domain:**
  - Active defense: Proactively lessens the attack landscape (e.g., patching, active sensor monitoring, network traffic filtering, protocol blocking, and so forth). Derived and shared threat intelligence reduces the opportunities for attackers to gain a foot hold and persist.
  - Protective monitoring: Reacts to passive sensor alerts, applies technical controls, minimizing impact, and re-occurrence using processes/procedures. The aim is to minimize the opportunities afforded to attackers to deny them from completing their objectives.

- **Medical domain:**
  - Reactive testing: Implements swab tests and records the details of test subjects. Collated positive results are used to identify clusters for further monitoring by epidemiologists. Data provides a steer to track and trace in the community using epidemiological surveillance teams on the ground.
  - Epidemiological surveillance and monitoring: Monitoring is used to produce statistics of positive infection rates in the community. This can be used to proactively break the chains of transmission by tracking hotspots and the tracing the seats of infections in society.

The use of a centralized system populated by definitive data—rather than the crowd-sourced and decentralized app sourced data—would provide a reliable record of potential hotspots and provide intelligence on pockets of infection from which a virus could spread. Admittedly, this type of system will process both personal and medical data of multiple test subjects and would need to comply with the European Union’s general data protection regulations. Pseudo anonymization and full anonymization techniques are permissible under this regulation [3].

Bird [3] proposed that the DTTTS concept could use public cloud platforms to provide an adequate and resilient design that is compliant with NHSX and international standards for cloud and UK government guidelines. Applying secure-by-design principles for secured endpoint to back-end connectivity facilitates secure infrastructure that would underpin the service to monitor test, track, and trace activities at pre-, intra-, and post-pandemic stages of a national health crisis. The system would require multi-factor authentication for user access, front-end application level authentication, and back-end data validation processes. The system could be developed using a cold standby use-case until it is required, alleviating the costs of a hot-standby solution. Service management approaches can be applied to ensure performance, capacity planning, change, and configuration management.
By using a DTTTS approach, an operational model can be articulated on how this distributed solution could be utilized and operated as part of an epidemic containment strategy. In the following section, the DTTTS concept is taken to the next stage; specifically, how it could be used in practice by being enshrined with an outline CONOPS.

3 Discussion

Even though Public Health England (PHE) tried to redeploy their epidemiological surveillance resources in response to SARS-Cov-2, it became apparent that they were overwhelmed partly due to the lack of initial testing capabilities. So consequently, the U.K.’s containment strategy was abandoned by mid-March [20, 27, 32]. The U.K. Government has recently decided to disband the PHE blaming the organization for a number of failings early on in the pandemic [5, 44]. In reality, an over reliance on the failed NHSX app compromised on-the-ground epidemiological efforts and subsequently track and trace coordination.

The U.K. Government has instigated the Joint Biosecurity Center (JBC). The JBC has taken ownership of the PHE alert monitoring system [37]. In addition, a new service called the national institute for health protection has been stood-up to combine the existing PHE and NHS test and trace capabilities under a single-public health service umbrella [6].

In this section, comparisons are drawn from CSOC use-cases in support of a strategy and CONOPS to enable: (a) front-end test teams at the border chokepoints to collect test samples; (b) cloud processing of test subject records and laboratory test results; (c) EOC containment monitoring; (d) data analysis of test subject groupings to identify hotspot areas; (e) use of epidemiological trends to direct further testing, and (f) conduct epidemiological monitoring to detect new transmission chains.

3.1 Distributed Test, Track, and Trace System Comparative Analogy to Cyber Security Operations Center Models

The JBC has a remit to lead the U.K. disease monitoring efforts using real-time analysis of infection outbreaks. Therefore, the JBC is an EOC derivative tasked to inform SAGE by conducting: (a) data analysis to understand infection rates; and (b) advise on how the government should respond to spikes in infections [12]. But the JBC is significantly constrained by the NHS test and trace system being a significant contributory data source and its inability to effectively track infections in a similar manner to the South Korean example.

To remedy this predicament and continuing the cyber security versus medical domain comparison from the previous section, there is in principle a direct correlation
between a CSOC and the required functions of an EOC; they are both based around centralized data collection [34] but use different data sets to provide leading threat intelligence. Generally, CSOCs are implemented by organizations at enterprise scale as part of infrastructure defense strategies, for the purposes of monitoring operational network and system level functions across the enterprise real estate. Following the anatomy of cyber defense monitoring performed by CSOCs, the following benefits are provided [2]:

- System logs and network flow statistics can be reliably processed in a timely manner.
- A combination of specialist tools and deployed agents can be used to drive patching and configuration remediation activities in order to minimize vulnerabilities.
- Ingress and egressing network traffic and application activities can be trended in order to detect abnormal or suspicious activities.
- Events analytics can be used to discern true positives and enable false positives from inadvertent sensor firing to be tuned out.

The functions of the CSOC have been likened to data management principles comprising the following contributory activities as part of a workflow: (a) data collection; (b) parse and normalize; (c) store data from collect/parse and normalize; (d) analyze data; and (e) report information derived from the data to generate an appropriate response [29]. In addition, the Observe, Orient, Decide, and Act (OODA) loop has been adopted from its militaristic origin [26] and is pertinent for CSOC operations to assimilate tactically derived threat intelligence [29]:

1. Observe: Collect, monitor, and store data.
2. Orient: Analyze the data to identify potentially suspicious events.
3. Decide: Based on loop iterations, define a course of action based on the facts.
4. Act: Perform the pre-determined action.

Both the data management workflow and the OODA loop are complementary in this context, where the following are asserted to be true:

1. Observe → Collect/parse and normalize/store alerts, logs, and netflow data.
2. Orient → Analyze data to detect a cyber threat.
3. Decide → Report on an identified cyber security event.
4. Act → Undertake response activities to perform mitigating and remedial actions to minimize the impact from the detected cyber threat.

This chapter required the functional analysis of CSOC tools to discern end-to-end structures pertaining to Security and Incident Event Monitoring (SIEM) technologies; and to learn how to adapt these principles into a DTTTS-based solution. A background study was therefore performed that compared renowned enterprise-level SIEM technologies employed by CSOCs. Vendor technologies comprise Hewlett Packard’s Arcsight [28], LogRhythm Nextgen SIEM Platform [25], Splunk [43], and SolarWinds Orion Platform [42]. The output is shown in Table 1.
Table 1  Comparison of cloud SIEM technology functions

| Vendor       | Data source | Data aggregation | Data accumulation | Analytics                  |
|--------------|-------------|------------------|-------------------|----------------------------|
| Arc sight    | Smart agents Connectors | Logger                   | Management center | Third-party tooling         |
| LogRhythm    | Application Programming Interfaces (API) System monitor agents | Data indexer | Data processor | Platform manager |
| Splunk       | Forwarders  | Indexer cluster(s) | Search head cluster | Search head Cluster master |
| SolarWinds   | Cloud native APIs Connectors | Orion database server | Network traffic or log analyzer(s) | Server and application monitor Log analyzer client |

The SIEM functions shown in Table 1 focus on cloud product deployments using the infrastructure-as-a-service model with platform-as-a-service elements. What became apparent by comparing these different vendor approaches is that in order to fulfill these functions CSOCs rely on the following prerequisite criteria: (a) originating data source; (b) data aggregators; (c) data accumulators; and (d) analytics capabilities. Of note, this study does not include SIEM-as-a-Service cloud technologies provided by some of these vendors because of the similarity to the software-as-a-service model; in these cases, the entire service and underlying nodal deployments are supplied by vendors and therefore does not correlate to the DTTTS IaaS-based analogy.

These four discerned criteria are in fact the essential ingredients for the DTTTS to function adequately in a health incident response context. As a distributed computerized system, it requires an ecosystem that in principle follows the key criteria of a CSOC, the only difference is that it will use different source data, and it operates for a different purpose. In the case of CSOCs, the tooling and processes already exist requiring trained, competent, and qualified staff as an absolute necessity [38]. In the case of the DTTTS concept, salient tools will need to be researched and purchased or developed and provisioned; teams would need to be trained and salient processes designed and implemented.

Henceforth, the wider system of interest, shown diagrammatically in Fig. 1, will be needed to perform the following: (1) compulsory swab testing of selected test subjects at border chokepoints and onward distribution of personal details pertaining to test subjects via endpoint devices to an exposed cloud application programming interface, (2) testing of swab samples at medical laboratories, distribution of the results, and updates appending test subject records; (3) centralized cloud processing/storage of definitive personal/medical data on positively diagnosed test subjects; (4) analytics and trends analysis to be used to centrally monitor hotspots within society; and (5) provide intelligence to trace transmission in the community.
emanating from hotspot clusters and coordinate epidemiological surveillance teams to conduct ad hoc tests that are further recorded by the system [3].

This approach, thereby provides the people, processes and technology to support containment operations during a public health event; by using OODA loop decision-making within a health setting similarly to how CSOCs employ measures to respond to cyber threats. A service wrap is also required in order to use this capability in the real world. Fitzsimmons et al. [13] identified the following pertinent aspects of service operations: (a) services are generally widely dispersed; (b) services are perishable; and (c) services are intangible requiring government regulation. These aspects are pertinent for health security operations, where parliament would need to pass laws to enforce a DTTTS health-based strategy and compel people transiting the U.K.’s borders to comply with the testing regime. From a governance perspective, the Department of Health and Social Care would need to oversee the DTTTS. The service wrap would be the enabler for the coordination and cooperation of decision-making activities in support of health crisis incident response.

In the CSOC analogy coordination can be facilitated by SIEM analysts but a cyber security incident response team [47] is also required to react to a security event in order to apply mitigations and remediations—remotely accessing components of the enterprise information technology infrastructure and on the ground as first responders interacting with assets. In the DTTTS context, an EOC is required to facilitate communication and intelligence, command and control and incident coordination to vector epidemiological teams into areas of potential infection within the community [14].

The use of the CONOPS outline provided in Fig. 2 would fuse and define the inter-relationships that are needed after test samples have been processed by laboratories.
In the lower area of the diagram, test results from collected test samples provide elaborating data to EOC staff, the EOC activities in the upper area inform tracking and trace activities and undertake coordination efforts of deployed epidemiological surveillance teams to identify any outbreaks from known hotspots. The epidemiological approach might necessitate further swab tests, and these are fed back into the laboratory test process. In a similar vein to a CSOC, the DTTTS could be used as part of the EOC ecosystem for operational management to: (a) correlate and corroborate test data; (b) identify infected/socially isolated residences; (c) monitor and track outbreaks from known hotspot locales; and (d) drive epidemiological surveillance to detect and trace transmission [3].

4 Further Research

The following dependencies need to be resolved to achieve the DTTTS concept and outline CONOPS [3]:

- Pass legislation so test subjects comply with the testing, track, and trace regime.
- Ability to rapidly deploy trained testing staff to border crossing points.
- Ability to speedily distribute front-end testing kits to transport hubs.
- Develop new methods to reliably screen passengers reducing inconvenience.
- Ensure sufficient laboratory capacity is maintained to process swab tests.
- Maintain a resourced cadre of epidemiological surveillance teams.
- DTTTS design is to be scalable to monitor, contain, and respond effectively.
• Create EOC processes to monitor, report, and coordinate with local government authorities.

5 Conclusion

The U.K. prime minister has conceded the country’s overall response was probably too slow. Thus, compared to South Korea, it was a catalyst to produce a comparative U.K. death rate ratio of 1:98.5 [3, 4, 46]. Professor Shridhar, medical advisor to the devolved Scottish Assembly, has always advocated a test, trace, and isolate strategy from the outset of the pandemic [40]. The incumbent chief scientific advisor regrets that testing could not have been implemented sooner at the start of the pandemic [45]. Thus, it is becoming widely accepted that the failure of an early testing program and slow contact tracing process was counterproductive as a means of understanding the seats of infection.

Local councils have subsequently received new powers to implement stricter local lockdown measures [7], and the U.K. Government has also retrospectively implemented travel restrictions and quarantine measures since late July in an attempt to avoid the inevitable “second wave” being brought in from overseas [4]. However, Sir King [24], the former U.K. Chief Scientific Advisor, stated that containment has always been required from the start rather than at end of the pandemic. Consequently, there is proof that for the “first wave” and “second wave” countries who attacked the virus early reaped the benefit of a lower death toll. This certainly appears to be the case for Germany, New Zealand, and South Korea who successfully used regional epidemiological teams [4]. Meanwhile, other nations have surmised that testing at the borders is part of an effective strategy to identify the ingress of SARS-CoV-2 or COVID-19; these countries and autonomous regions include at least Iceland, Greece, Austria, Jersey, Madeira who test passengers on entry. France and Germany also started testing passengers entering their countries from high-risk destinations [22].

There are two trains of thought regarding the pandemic: The World Health Organization believes that it will take up to two years to defeat COVID-19 with a vaccination program, whilst a preeminent SAGE scientist thinks that SARS-CoV-2 may never be eradicated [8]. This is a particularly important consideration when continual in-country outbreaks provide a warning of the resulting risks from COVID-19; especially considering the recently identified coronavirus mutation D614G that potentially facilitates faster propagation across the populace [16]—albeit it in a weakened state [35].

Resultantly, computer science could greatly contribute to the betterment and sustainability of human health by contributing to the DTTTS concept and outline CONOPS; thereby providing a capability to perform better epidemic containment management. Therefore, the case for a DTTTS is even more justifiable in the sense that pre-emptive tracking and tracing provides a means to detect and track epidemics from the border inwards. The utilization of service operations can conjoin the test,
track, and trace facets under a common umbrella. The DTTTS concept and supporting CONOPS would facilitate coordinated monitoring and containment intelligence, as well as inform better epidemic containment management. Albeit a limitation, and dependency for success, is changes would be necessary to legislation in order to make test subjects comply with the test, track, and trace regime.

References

1. J. Aston, Sky News 24 (2020), https://www.news.sky.com. Accessed 12 April 2020
2. D. Bird, The age of the SoC. Digital Leaders 1(2), 22–23 (2016)
3. D. Bird, Distributed Test, Track and Trace System as a Contributor to Epidemic Containment Management. in Proceedings of 4th World Conference on Smart Trends in Systems, Security and Sustainability (IEEE Xplore, 27–28 July 2020)
4. British Broadcasting Corporation, BBC News (2020a), https://www.bbc.co.uk/news. Accessed 12 June 2020, 18 July 2020, 20 July 2020, 24 July 2020, 25 July 2020, and 15 August 2020
5. British Broadcasting Corporation, Coronavirus: Public Health England ‘to be replaced (2020b), https://www.bbc.co.uk/news/health-53799854. Accessed 17 Aug 2020
6. British Broadcasting Corporation, New public health body ‘vigilant for viral threat (2020c), https://www.bbc.co.uk/news/health-53813480. Accessed 18 Aug 2020
7. British Broadcasting Corporation, Coronavirus Councils in England get new powers for local shutdowns (2020d), https://www.bbc.co.uk/news/uk-53453720. Accessed 18 July 2020
8. British Broadcasting Corporation, Coronavirus will be with us forever, Sage scientist warns (2020e), https://www.bbc.co.uk/news/uk-53875189. Accessed 22 August 2020
9. J. Calvert, G. Arbuthnott, L. Leake, Coronavirus: 38 days when Britain sleepwalked into disaster (2020), https://www.thetimes.co.uk/article/coronavirus-38-days-when-britain-sleepwalked-into-disaster-hq3b9tlgh. Accessed 25 April 2020
10. S. Coates, Sky News 24 (2020), https://www.news.sky.com. Accessed 12 Oct 2020
11. E. Conway, Sky News 24 (2020), https://www.news.sky.com. Accessed 15 Oct 2020
12. N. Davies, Joint Biosecurity Centre (2020), https://www.instituteforgovernment.org.uk/explainers/joint-biosecurity-centre. Accessed 22 Aug 2020
13. J. Fitzsimmons, M. Fitzsimmons, S. Bordoloi, Service Management: Operations Strategy and Technology (McGraw-Hill, New York, 2014).
14. Georgia Department of Public Health, Function and Form of the Command Center: Advanced Healthcare Emergency Management Course (Department of Public Health, Georgia, n.d.)
15. G. Guru-Murthy, A. Costello, H. Lee, The country that beat the coronavirus (2020), https://www.channel4.com/programmes/the-country-that-beat-the-virus. Accessed 20 May 2020
16. J. Hardy, New Covid-19 mutation ‘helping outbreaks spread faster around the world (2020) https://www.telegraph.co.uk/news/2020/07/22/infectious-covid-19-mutation-dominant-globally-fueling-faster/. Accessed 22 Aug 2020.
17. J. Hunt, Sky News 24 (2020a), www.news.sky.com. Accessed 17 April 2020
18. J. Hunt, Sky News 24 (2020b), www.news.sky.com. Accessed 29 March 2020
19. C. Hymas, At least 20,000 people with coronavirus arrived in UK before lockdown amid lack of restrictions (2020), https://www.telegraph.co.uk/news/2020/05/05/least-20000-people-infected-coronavirus-arrived-uk-lockdown/. Accessed 20 May 2020
20. P. Ingram, COVID-19 an Intelligence assessment (2020), https://greyharemedia.com/covid-19-an-intelligence-assessment/. Accessed 25 April 2020
21. S. Johnson, Confidential Computing (2020), https://www.cheltenhamfestivals.com/science/. Accessed 3 June 2020.
22. R. Joshi, Sky News (2020), https://news.sky.com. Accessed 29 July 2020
23. D. King, BBC News (2020a), www.bbc.co.uk/news. Accessed 30 April 2020.
24. D. King, (2020b) Sky News. www.news.sky.com. Accessed 6 June 2020.
25. LogRhythm, LogRhythm NextGen SIEM Platform 7.4.9 (2020), https://aws.amazon.com/marketplace/pp/B085CGKMNR?ref_=srh_res_product_title. Accessed 23 August 2020.
26. A. Luft, The OODA loop and the half-beat (2020), https://thestra tegybridge.org/the-bridge/2020/3/17/the-ooda-and-the-half-beat. Accessed 22 August 2020.
27. A. McClaine, Coronavirus: Daily Briefing (2020), https://www.bbc.co.uk/news. Accessed 19 May 2020
28. Microsoft, ArcSight ArcMC 2.90 (2020), https://azuremarketplace.microsoft.com/en-us/marketplace/apps/micro-focus.arcsight-arcmc?tab=Overview. Accessed 23 August 2020.
29. J. Muniz, G. McIntyre, N. Alfragan, Security Operations Center: Building Operating and Maintaining Your SOC (Cisco Press, Indianapolis, 2016).
30. J. Newton, Coronavirus: Daily Briefing (2020) https://www.bbc.co.uk/news. Accessed 4 May 2020.
31. C. O’Grady, The U.K. backed off on herd immunity. To beat COVID-19, we’ll ultimately need it (2020), https://www.nationalgeographic.com/science/2020/03/uk-backed-off-on-herd-immunity-to-beat-coronavirus-we-need-it/. Accessed 25 April 2020
32. Public Health England, New surveillance system for early detection of COVID-19, https://www.gov.uk/government/news/new-surveillance-system-for-early-detection-of-covid-19. Accessed 25 April 2020
33. T. Pueyo, Coronavirus: The Hammer and the Dance (2020), https://medium.com/@tomaspueyo/coronavirus-the-hammer-and-the-dance-be9337092b56. Accessed 25 April 2020
34. G. Rasche, Guidelines for Planning an Integrated Security Operations Center (Electronic Power Research Institute, California, 2013).
35. Reuters, More Infectious Coronavirus Mutation May Be ‘a Good Thing’, Says Disease Expert (2020) https://www.nytimes.com/reuters/2020/08/17/world/asia/17reuters-health-coronavirus-mutation.html. Accessed 17 August 2020.
36. K. Rushton, D. Foggo, Neil Fergusen, The scientist who convinced Boris Johnson of UK coronavirus lockdown, criticised in past for flawed research (2020) https://www.telegraph.co.uk/news/2020/03/28/neil-fergusen-scientist-convinced-boris-johnson-uk-coronavirus-lockdown-criticised/. Accessed 25 April 2020
37. D. Sabbagh, I. Sample, Senior counter-terror official put in charge of new UK biosecurity centre (2020) https://www.theguardian.com/world/2020/may/12/former-counter-terror-official-tom-hurd-put-in-charge-new-uk-biosecurity-centre-coronavirus. Accessed 12 May 2020
38. S. Schinagle, K. Schoon, R. Paans, A framework for Designing a Security Operations Centre. in Proceedings of the 48th Hawaii International Conference on System Sciences. Kauai, Hawaii 5–8 January 2015. https://doi.org/10.1109/HICSS.2015.270
39. G. Shapps, The Andrew Marr Show (2020) https://www.bbc.co.uk/iplayer/episode/m000hyq2/the-andrew-marr-show-03052020. Accessed 20 May 2020
40. D. Shridhar, BBC News (2020), www.bbc.co.uk/news. Accessed 4 June 2020
41. F. Smith, Malware and Disease: Lessons from Cyber Intelligence for Public Health Surveillance. In: Health Security Journal (October 2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5041502, Accessed 22 Aug 2020
42. S. SolarWinds, Core Cloud Monitor Cloud (2020), https://documentation.solarwinds.com/en/success_center/orionplatform/Content/Core-Cloud-Monitor-Cloud.htm. Accessed 23 Aug 2020
43. Splunk, Topology of Splunk on Azure (n.d.) https://www.splunk.com/content/dam/splunk-blogs/images/2016/02/Topology-of-Splunk-on-Azure.png. Accessed 23 Aug 2020
44. Z. Tidman, Government accused of ‘passing the buck’ with reported plan to scrap Public Health England (2020), https://www.independent.co.uk/news/health/public-health-england-scarep-phe-matt-hancock-coronavirus-a9672891.html/. Accessed 22 Aug 2020
45. P. Valance, BBC News (2020), www.bbc.co.uk/news. Accessed 5 May 2020
46. Worldometers, COVID-19 Coronavirus Pandemic (2020), https://www.worldometers.info/coronavirus/. Accessed 23 Aug 2020
47. C. Zimmerman, *Ten Strategies of a World-Class Cybersecurity Operations Center* (The MITRE Corporation, Bedford, 2014).