Chapter 7
Cyberbiosecurity and Public Health in the Age of COVID-19

Aaron Adler, Jake Beal, Mary Lancaster, and Daniel Wyschogrod

7.1 Introduction

Cyberbiosecurity, the aspect of biosecurity involving the digital representation of biological data, had already been emerging as a matter of public concern even prior to the onset of the COVID-19 pandemic. Key issues of concern include, among others, the privacy of patient data, the security of public health databases, the integrity of diagnostic test data, the integrity of public biological databases, the security implications of automated laboratory systems and the security of proprietary biological engineering advances.

With the onset of the COVID-19 pandemic, and the importance of digital resources in combatting it, concern about the potential for cyber attacks by state-based or non-state actors has been elevated. To illuminate the challenges, we focus on the cyber vulnerabilities that need to be addressed in public health activities such as disease surveillance and outbreak management. In particular, we examine cyber issues raised by the accelerated pace of development for COVID mitigations, treatments, and vaccines.

Figure 1 illustrates a simplified view of key components and their interactions in this area, as well as vulnerable points where informational attacks can result in significant biosecurity consequences. In particular, the challenges that we consider here are:

1. Privacy of contact tracing data – Contact tracing has been used in one form or another to contain epidemics for centuries. With the widespread adoption of

A. Adler · J. Beal · D. Wyschogrod (✉)
Raytheon BBN, Cambridge, MA, USA
e-mail: dan.wyschogrod@raytheon.com

M. Lancaster
Pacific Northwest National Laboratory (PNNL), Richland, WA, USA

B. D. Trump et al. (eds.), *Emerging Threats of Synthetic Biology and Biotechnology*, NATO Science for Peace and Security Series C: Environmental Security, https://doi.org/10.1007/978-94-024-2086-9_7

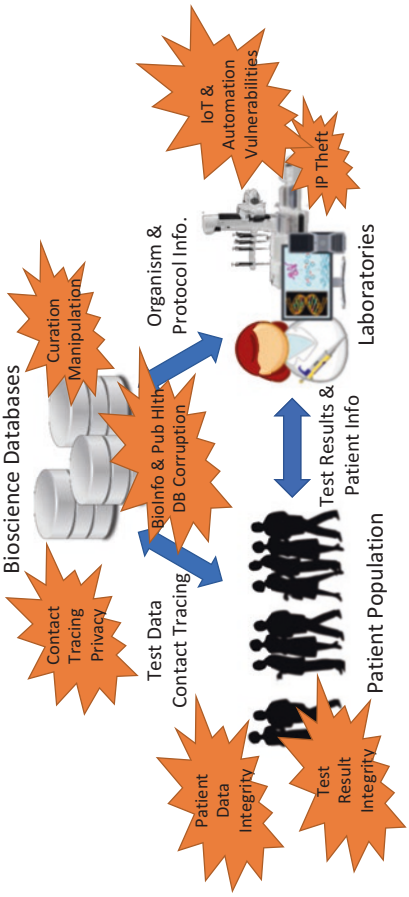

Fig. 1 Key components, interactions, and cyberbiosecurity threats in the surveillance and management of infectious diseases such as COVID-19

smart phones, the potential for automated contact tracing holds significant promise. How can this be done in a manner that protects patient privacy? How can smartphone data be integrated with manual contact tracing? What are the privacy, security and efficacy tradeoffs? What are the implications of patient privacy concerns for the collection of public health data?

2. Integrity of public health and disease surveillance data – As COVID-19 has shown, disease surveillance data is critical both for scientists and policy makers. These data include but are not limited to case counts, diagnostic test results, and general trend information. Various governments, agencies, or other malicious actors might want to manipulate such information to artificially inflate or suppress data. What safeguards against such manipulation can be provided?
3. Data integrity and result validation of self-administered testing – Self-administered tests can provide fast, actionable health information. For COVID-19, a number of at home tests are being proposed, some of which would allow users to receive immediate results, similar to pregnancy tests. Self-administration, however, also allows many more opportunities for data corruption or exposure. How can such results be shared for aggregation into public health statistics and use in contact tracing in such a way that their results can be validated by health care professionals and individual privacy also be preserved?
4. Integrity of public bioinformatic databases – Both researchers and medical personnel rely on public sequence and sample data resources such as those maintained by NCBI. Frequently, mistakes are made in labeling that can cause difficulties. Currently, most such errors appear to be inadvertent rather than malicious, but such data could also be deliberately manipulated to confuse bioinformatic investigations. How can the integrity of public data be maintained and attempts at manipulation detected?
5. Defending against cyberattacks on laboratory automation – Laboratory throughput is increasingly being accelerated through automation involving robotics, laboratory information management systems (LIMS), and network-enabled devices that fall under the general category of Internet of Things (IoT). These systems are often connected to the internet (e.g., for software updates or remote monitoring and control), providing an attack surface by which they may be compromised. Such devices can be used as entry points into laboratory networks or manipulated for their biological effects (e.g., destroying stored specimens by changing temperature settings on a freezer). How can these devices be protected and how can they be prevented from becoming points of entry into critical laboratory computer networks?
6. Protection of intellectual property – Theft of intellectual property by both state and non-state actors is a longstanding problem. The race for COVID-19 vaccinations and treatments has amplified this illicit activity, motivated both by a desire for direct monetary gain and by nations' need to protect their populations and restore their economies. What safeguards need to be provided and how can malicious parties be identified?

In the subsequent sections, we will expand on each of these threats in turn, followed by a summary of their implications.

7.2 Privacy of Contact Tracing Data

Contact tracing is the process of identifying and monitoring persons who have been in contact with an infected person or persons. It has been used in one form or another for centuries.[1] More recently, it has been used effectively in the control of tuberculosis, Severe Acute Respiratory Syndrome (SARS), and Middle East Respiratory Syndrome (MERS).[2] Manual contact tracing has limitations in the number of persons that can be identified and interviewed in a timely manner. With about 8000 SARS infections and 800 deaths[3] and about 2500 instances of MERS and 858 deaths,[4] manual contact tracing proved sufficient. In the case of COVID-19, with 4.3 million confirmed cases and about 300,000 deaths worldwide at the time of this writing, complete and timely manual contact tracing may not be possible in many local jurisdictions.

Early in the COVID-19 pandemic, a number of countries leveraged smart phones to help automate contact tracing. Various types of relevant information are available on a smart phone. GPS and location services, which can add information about nearby WiFi hotspots, can be used with contact tracing apps but raises privacy concerns. In China, people are sent QR codes on their phones indicating their level of risk for COVID-19 and access to public transportation or public areas such as shopping malls is determined by the QR code granted to an individual.[5] These codes are based on self-reported information as well as possibly location services information (though the Chinese government has not been forthcoming on the data used to produce these codes). South Korea does not use such QR health codes, but publicizes details concerning individuals who have tested positive including the person's age range, gender, and places they recently visited. QR codes can also be used to register visitors to businesses and users of public transportation.

---

[1] S. Cohen, M. O'Brian, *The Conversation*, 'Contact tracing: how physicians used it 500 years ago to control the bubonic plague', https://theconversation.com/contact-tracing-how-physicians-used-it-500-years-ago-to-control-the-bubonic-plague-139248, June, 2020 (retrieved August 2020).

[2] K.O. Kwok, A. Tang, V.W.I. Wei, W. H. Park, E.K. Yeoh, and S. Riley, "Epidemic Models of Contact Tracing: Systematic Review of Transmission Studies of Severe Acute Respiratory Syndrome and Middle East Respiratory Syndrome", Comput Struct Biotechnol J., 2019; 17;186–194

[3] CDC, "Fact Sheet: Basic Information about SARS", https://www.cdc.gov/sars/about/fs-SARS.pdf, retrieved August 2020.

[4] WHO, "Middle East respiratory syndrome coronavirus (MERS-CoV)", https://www.who.int/emergencies/mers-cov/en/, retrieved August 2020.

[5] BBC, "China launches coronavirus 'close contact detector' app", https://www.bbc.com/news/technology-51439401, February 2020 (retrieved August 2020).

Another approach that is believed to be more privacy preserving and more secure in a number of respects involves the use of Bluetooth rather than GPS or location services. Singapore has released an app called TraceTogether.[6] TraceTogether attempts to minimize the amount of personal information it gathers, but it does collect the cell phone numbers of users on a voluntary basis.[7]

The ability to use Bluetooth and maintain a high level of privacy has been greatly assisted by the cooperation of Google and Apple in inserting new capabilities in both iOS and Android at the operating system level.[8] The Apple/Google protocol is based on privacy ideas emerging from the MIT-led PACT project[9] and the European DP-3T[10] project.

The goal of the Apple/Google application protocol interface (API) is to provide a set of functions and procedures in the operating system that can be used by state or local authorities and software developers to develop user-level contact tracing apps. The two foundations of this methodology are:

1. Extensions of the Bluetooth protocol to determine "too close for too long"
2. A distributed architecture such that notifications of proximity to a confirmed case of COVID-19 are sent only to the user of a phone and no other parties.

Algorithms to determine "too close for too long," however, are still under development. They have both a physical and biological component. The physical aspect involves the inference of distance between infectious and susceptible individuals from the observed information. The new interface provided by Apple/Google will give the app developer information about Received Signal Strength Indication (RSSI) for each transmission from a nearby (typically tens of meters) source.[11] The RSSI falls off with distance so it can be used to infer distance between phones but also falls off with attenuation due to phones being in pockets or handbags and intervening obstacles (e.g. walls or shelving), making the translation from RSSI to distance complex. The biological issue is how much exposure to an infected person at what distance indicates a high risk of infection. Tuning the criterion for "too close for too long" clearly will affect both the false positive and false negative rates.

The second foundation of this methodology is that only a user of the app is informed of a possible exposure, but no one else. The goal here is to achieve

[6] Singapore Government, "TraceTogether home page", https://www.tracetogether.gov.sg, retrieved August 2020.

[7] Singapore Government, "TraceTogether Privacy Safeguards", https://www.tracetogether.gov.sg/common/privacystatement, retrieved August 2020.

[8] Apple, Inc., "Privacy-Preserving Contact Tracing",https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-CryptographySpecificationv1.2.pdf, retrieved August 2020.

[9] PACT, "PACT: Private Automated Contact Tracing", https://pact.mit.edu, retrieved August 2020.

[10] DP3T, "DP3T – Decentralized Privacy-Preserving Proximity Tracing" https://github.com/DP-3T/documents, retrieved August 2020.

[11] Bluetooth SIG, "Proximity and RSSI", https://www.bluetooth.com/blog/proximity-and-rssi/, September 2015 (retrieved, August 2020).

maximal privacy. The mechanism works as follows. An individual phone creates a seed at a particular time period, say each hour. That seed is used to generate changing values in each "chirp" emitted by the Bluetooth interface. Neighboring phones detect these chirps and record them along with timestamps. If an individual tests positive and they consent, their phone is accessed and the list of seeds over the infection time period are uploaded to a central database. The central database downloads the seeds with time stamps of all infected individuals to all users of the app. The user's phone then generates the seeds of infected persons to generate chirp values, which they check against the user's list of received chirps to see if the user has been exposed to any COVID-19 confirmed case. Thus, the recipient only knows that they have been potentially exposed to confirmed case of COVID-19. They do not know the identity of the person they were exposed to, nor does anyone else know that the user might be infected. The exposed app user is encouraged to seek diagnostic testing and to self-quarantine, but this is voluntary.

An important item to note is that while private information is withheld from unauthorized malicious or just curious agents, it is also withheld from health professionals and public health authorities, including human contact tracers. This information would undoubtedly be useful in determining with whom an infected individual came in contact, many of whom they may have forgotten or not noticed. While individuals who are notified about contact with infected individuals may be encouraged to contact health authorities, it would be voluntary and because of the anonymity protections, much of the work tracing back to previous contacts and forward to successive contacts would have to be repeated by the human contact tracers. Following the chain of individuals who are farther and farther removed from the diagnosed individual would be particularly useful for superspreader events where rapid identification and quarantine of all those exposed in the first several generations is critical. Identifying and isolating individuals with asymptomatic infections is also important. All of this information would have to be re-discovered by the human contact tracer.

A possible solution might be the voluntary submission of information to public health authorities by individuals who have gotten a match on their phone, perhaps through the app itself. The issue then is that more and more potentially private information is entered into the central cloud database.

These are all issues that are under active discussion. Since the Apple/Google interface is at the operating system and API level, however, different countries and regions will be able to choose to make different privacy decisions.

Such issues of privacy versus importance of data collection in emergency situations will apply to future post-COVID situations as well. Depending on the success of automated contact tracing in assisting in opening up commerce and day-to-day life, such apps, and perhaps their extension to wearables, may become more commonplace. Clearly, this is an issue where epidemiologists, infectious disease specialists, privacy and security experts, and medical ethicists must collaborate to identify and address risks and vulnerabilities.

7.3 Protecting Public Health and Disease Surveillance Data

As COVID-19 has shown, disease surveillance data are critical both for scientists and policy makers as well as the general public. These data include but are not limited to case counts, diagnostic test results, and general trend information. Various nation state or other malicious actors might want to either suppress or artificially inflate data.

As we have seen in the COVID-19 pandemic and the West Africa Ebola outbreak,[12] delayed response to outbreak events can result in larger impacts. If false negative diagnostic tests are returned and surveillance data are altered to keep case counts below epidemic thresholds, outbreak control measures may not be implemented until much later, when the outbreak is much larger.

Alternately, creation of disease cases in a surveillance system may create the appearance of an outbreak and result in mobilization of resources to investigate and mitigate an outbreak that does not exist. For example, for some livestock diseases, control measures include depopulation of the affected farms. Failure to properly confirm the presence of an outbreak before control measures are implemented may be catastrophic.

Furthermore, for many livestock and agricultural diseases, trade restrictions may be invoked to prevent the spread of disease across borders. The false creation of an outbreak in surveillance data may result in significant trade losses until the apparent outbreak can be invalidated. Considerable resources may be expended in verifying to trade partners and international organizations that an apparent outbreak was not real and that the animals in a herd or in a geographic area are not infected.

7.4 Integrity and Validation of Self-Administered Testing

Testing for SARS-CoV-2 provides a test case for the use of home diagnostic tests. Some routine tests, e.g., pregnancy tests or glucose tests, have long been available for home use. Some SARS-CoV-2 tests also allow for in-home collection, but specimens must be mailed to a laboratory that processes the results. This is similar to some other at-home testing systems, e.g., via Everlywell.[13] With SARS-CoV-2 testing, there is a public health interest in tracking test results, and integrity and validation are important.

There are four broad categories for handling of at-home testing:

1. Self tests with unreported results;
2. Self tests shared and interpreted via a telehealth appointment;

[12] M. Jeremiah Matson, Daniel S. Chertow, and Vincent J. Munster,"Delayed recognition of Ebola virus disease is associated with longer and larger outbreaks," Emerg Microbes Infect. 2020; 9(1): 291–301.

[13] Everywell, "Everywell home page", https://www.everlywell.com, retrieved August 2020.

3. Self tests interpreted via a cell phone mobile application;
4. Self tests with an internet connected testing device that reports results.

We will address each of these situations in turn. There are two aspects to result interpretation – first, does the patient understand their results, and second, are the results correctly reported to medical or public health personnel.

Self-Tests with Unreported Results In the case of routine home tests, the focus is on providing an interpretable result. There are many ways to provide result interpretation, including a visual indicator on a disposable test (e.g., pregnancy tests), reporting via an accessory device (e.g., digital glucose reading), or a result provided via a cell phone application (e.g., picture interpretation of Vessel Health app[14]). In these cases the focus is on providing a result understandable to the user and not at all reporting the results to anyone else, and any of the solutions is viable.

Self Tests Shared and Interpreted Via a Telehealth Appointment Some at home testing is planned for the near future where results are interpreted remotely (e.g., Vessel Health serology software). In this case, a diagnostic image is sent to a health care professional and analyzed during a telehealth appointment. This solves several of the issues with at-home testing by providing a way to do contact tracing (via the telehealth appointment) and helping to ensure a correct diagnostic. This enables a patient to easily understand their result and allows results to be reported to health officials appropriately. A code may be provided with each test to associate the telehealth appointment with an actual test, though there is no guarantee that the image of the test is authentic or that the person providing information to the telehealth professional is the person who actually took the test. While the latter is a problem with all self tests, the former can be addressed by using something other than just a visual image. For example, a unique RFI tag or barcode could be used with an app or an internet connected device to ensure the authenticity of the test. It should be noted that while malfeasance on the part of individuals is possible with this kind of testing, it would be challenging for malicious actors to greatly affect pandemic statistics in any meaningful way. The down side, however, is that this approach is expensive and does not scale easily due to the need for health professional involvement.

Self Tests Interpreted Via a Cell Phone Mobile Application To decrease cost compared to telehealth, a cell phone mobile app could be used to capture test results. As with the telehealth appointment, the test authenticity could be verified against an online database of test identifiers, and location information from the cell phone could be added to localize the test. As with the telehealth scenario, the app would have no way to verify that the person using the app provided the specimen, or whether the test result was authentic, e.g., not manipulated by an unscrupulous user.

[14]VesselHealth," At-home testing for COVID-19 antibodies", https://vesselhealth.com/coronavirus.html, retrieved August 2020.

Further, compromise of the app or associated cloud resources via the usual range of cyber exploits could be used for large scale corruption or manipulation of data.

Self Tests with an Internet Connected Testing Device That Reports Results The final variant is a testing device that produces the results and directly communicates via the internet to report results. In this case, the authenticity and uniqueness of the test is guaranteed at the expense of complying with necessary data and patient privacy regulations. In this scenario, as long as the specimen being tested is authentic, results are not easily forged. On the other hand, as with the phone app, compromise of the web interface or database are possible.

While security, integrity, and validation for small scale testing may be easily solved with telehealth appointments, larger scale testing will require more complex software security arrangements to provide integrity and validation of test results.

7.5 Integrity of Public Bioinformatic Databases

Numerous public bioinformatics databases have been created.[15] Researchers upload annotated data for global use and sharing with the research community. In addition to the unintentional introduction of errors into the databases, concerns have been raised regarding the intentional manipulation of the content.[16] Regardless of source, database errors can be rapidly propagated through analysis, transformation, and integration of data.[17]

While deliberately malicious modification of data contributed to public databases has not yet, to our knowledge, been detected, there may be significant motives for bad actors to do so. For instance, origins of outbreaks, which can be a political issue, can be determined from genomic sequences[18] and modification of these genomic sequences in databases may be to the advantage of those seeking to discredit other groups or deflect blame from themselves.

Preventing corruption of public databases has other important practical implications as well. For instance, sequence screening, such as that practiced by members of the International Gene Synthesis Consortium (IGSC), verifies that sequences of genes ordered by customers do not contain regulated pathogen sequences or other

[15] See http://www.oxfordjournals.org/nar/database/a/ for a partial listing.

[16] J. Caswell, J.D. Gans, et al., "Defending Our Public Biological Databases as a Global Critical Infrastructure", Front. Bioeng. Biotechnol., 05 April 2019, https://doi.org/10.3389/fbioe.2019.00058

[17] R. Pool, J. Esnayra, "Bioinformatics – Converting Data to Knowledge", National Research Council, Washington, DC: The National Academies Press, 2000. https://doi.org/10.17226/9990

[18] Liangsheng Zhang, Jian-Rong Yang, Zhenguo Zhang, Zhenguo Lin, "Genomic variations of SARS-CoV-2 suggest multiple outbreak sources of transmission', medRxiv, https://www.medrxiv.org/content/10.1101/2020.02.25.20027953v2, March 2020.

potentially dangerous sequences.[19] Thus, maintaining correct sequences for both pathogens and benign species is important.

Further, as shown in the IARPA funded FELIX program,[20] determination of whether a DNA sample shows signs of engineering is performed by comparison with a non-engineered reference sample. If public databases are intentionally polluted with engineered samples, engineering may not be detectable.

Methods and approaches used to detect and correct unintentional errors can also be used to detect intentional manipulation. Rigorous documentation of data provenance can help identify unauthorized changes. Finally, ontology-based approaches can detect inconsistencies in the data and enable data curators to address anomalies.

7.6 Defending Against Cyberattacks on Laboratory Devices

The internet of things (IoT) enables "advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[21] The digital revolution in the life sciences has introduced smart laboratories that automate processes, link instruments and devices to a network, and offer new ways to create, store, share, and manipulate electronic pathogen and disease information. Unfortunately, malicious actors can exploit vulnerabilities arising from weak cyber and biosecurity policies and practices, as well as inadequately secured networks, networked laboratory equipment, automated systems, and electronic data and files. These vulnerabilities expose data to unauthorized access, use, disclosure, disruption, modification, or destruction and ultimately threaten data confidentiality, integrity, and availability. Cyber adversaries include both state and non-state actors.[22]

Adversaries have targeted medical and laboratory devices with malware and exploited vulnerabilities in imaging equipment, and medical and point-of-care diagnostic devices.[23,24] Additionally, it has been shown that malicious actors could use synthetic DNA sequences encoded with malware to gain control of the computers

[19] Gene Synthesis Consortium, "Home Page", https://genesynthesisconsortium.org/, retrieved August 2020.

[20] Adali, et al. "Integrated Decision-Making to Detect DNA Engineering in Yeast", IWBDA 2020, August 2020.

[21] International Telecommunications Union. 2012. Overview of the Internet of Things. http://handle.itu.int/11.1002/1000/11559

[22] Carlin, John P. 2016. "Detect, Disrupt, Deter: A Whole of Government Approach to National Security Cyber Threats." *Harvard National Security Journal* 7: 391–436.

[23] Department of Homeland Security (DHS). 2019. *ICS-CERT Alerts.* December 4. https://www.us-cert.gov/ics/alerts

[24] Enriquez, Jof. 2015. "Medjacking: How Hackers Use Medical Devices to Launch Cyber Attacks." *Med Device Online.* June 10. Accessed December 9, 2019. https://www.meddeviceonline.com/doc/medjacking-how-hackers-use-medical-devices-to-launch-cyber-attacks-0001

processing the sequence.[25] These vulnerabilities can change network permissions to access a device, download sensitive patient information, alter settings, issue commands, or interfere with the intended function of a device.

Any network access point provides an opportunity for adversaries to enter and compromise network components. Research demonstrates how unauthorized users have cloned radio frequency identification cards to gain physical access to laboratory facilities and used building ventilation control systems to access customer records and payment information.[26] Network security policies and practices that permit individuals to connect personal devices (e.g., phones, computers, memory cards, etc.) expose a corporate network to potential vulnerabilities, such as untrusted content, lack of configuration control, and use of location services.[27] In addition, adversaries can manipulate, copy, or destroy laboratory databases, including inventory, sequence, and disease surveillance data. In June 2019, an Iran-based internet protocol (IP) address exploit targeted exposed systems running dnaLIMS, a web-based bioinformatics system, to gain control of the computer system and further penetrate the network.[28]

In a COVID-19 environment where resources are allocated and policies made based on statistical data derived from test data, compromised laboratory data can lead to serious negative consequences in terms of under or over response. Further, exploits can be automated so that a vulnerability in one model of a laboratory device can be used to attack that device wherever it is found throughout the world.

7.7 Protection of Intellectual Property

For quite a number of years, state actors in cyberspace have attempted to steal the intellectual property of companies and government facilities of competing states. Cyber experts have identified such actions from hacker groups such as ACT10,

[25] Ney, P, K Koscher, L Organick, L Ceze, and T Kohno. 2017. "Computer Security, Privacy, and DNA Sequencing: Compromising computers wtih synthesized DNA, privacy leaks, and more." *USENIX Security Symposium.*

[26] Radichel, Teri. 2014. "Case Study: Critical Controls that Could Have Prevented Target Breach." (SANS Instiute Reading Room). Accessed January 8, 2020. https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412-study-critical-controls-prevented-target-breach-35412&usg=A

[27] Simmons, Raphael. 2017. *BYOD Security Implementation for Small Organizations.* SANS Institute. Accessed January 7, 2020. https://www.sans.org/reading-room/whitepapers/mobile/byod-security-implementation-small-organizations-38230

[28] Townsend, Kevin. 2017. *Critical Vulnerabilities Found in Popular DNA Sequencing Software.* March 10. Accessed November 2019. https://www.securityweek.com/critical-vulnerabilities-found-popular-dna-sequencing-software

believed to be sponsored by the Chinese government.[29] During the COVID-19 epidemic, government institutions and commercial biotechnology companies which have been involved in the search for a vaccine or other treatments for COVID have become new targets of cyberspace theft attempts.[30,31,32]

Other attacks in the biotechnology space have come from non-state actors. Different motives have caused hacker groups to attack private biotech firms.[33,34] In one highly publicized incident, a consortium of hacker groups pledged not to attack health care providers during the coronavirus outbreak. However, a member of this consortium, CLOP, launched a ransomware attack on ExecuPharm, a U.S. firm in Vermont, claiming that while they did not attack health care providers, commercial pharmaceutical organizations were fair game.[35] CLOP went one step further, and published personally identifiable information it found on the company servers including social security numbers, some from patient studies.

A number of steps have been advocated for improving the security of biopharmaceutical companies, especially those involved in COVID-19 medical countermeasure research.[36] These include limiting patient data on servers, secure storage of backups against ransomware, and training of personnel in cyber hygiene.

Currently, both government entities as well as private corporations are involved in the development of COVID-19 treatments and vaccines involving extensive scientific data and patient information. Should these facilities be compromised, or even

[29] Z. Doffman, "Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities", Newsweek, https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#5503d1aa6758, August 2019 (retrieved August 2020).

[30] G. Lubold and D. Volz, "U.S. Says Chinese, Iranian Hackers Seek to Steal Coronavirus Research", WSJ, https://www.wsj.com/articles/chinese-iranian-hacking-may-be-hampering-search-for-coronavirus-vaccine-officials-say-11589362205, May 2020 (retrieved August 2020).

[31] C. Corera, "Coronavirus: Cyber-spies hunt Covid-19 research, US and UK warn", BBC https://www.bbc.com/news/technology-52551023, May 2020 (retrieved August 2020).

[32] D.E. Sanger and N. Perlroth, "U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks", NYT, https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html, May 2020 (retrieved August 2020).

[33] D. Bukszpan, "The cyberthreat that could derail the world's race to develop a coronavirus vaccine", CNBC, https://www.cnbc.com/2020/05/12/this-cyberthreat-could-derail-race-to-develop-a-coronavirus-vaccine.html, May 2020 (retrieved August 2020).

[34] D. Winder," COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online",Forbes, https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#9c804ab18e55, March 2020 (retrieved August 2020).

[35] Z. Whittaler, "Hackers publish ExecuPharm internal data after ransomware attack",TechCrunch, https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/, April 2020 (retrieved August 2020).

[36] K. Vermes, "COVID-19 Pandemic Leaves Pharmaceutical Companies Vulnerable to Cyber Criminals", BioSpace, https://www.biospace.com/article/covid-19-pandemic-leaves-pharmaceutical-companies-vulnerable-to-cyber-criminals-/, May 2020 (retrieved August 2020).

worse incapacitated, delaying the release of therapies, there would be global implications.

7.8 Discussion

In this discussion, we have illuminated a range of key cyberbiosecurity threats to infectious disease surveillance and outbreak management. While the COVID-19 pandemic has made these concerns particularly acute, ongoing strategic investments are needed to better understand, mitigate, and defend against these and similar threats. The current pandemic illustrates well the high strategic value of such public health infrastructure, and where there is value, the remote access afforded by cyber methods creates the threat that a wide variety of actors will seek advantage through cyber exploits.

Here, we have discussed what we assess to be the most near-term and high-significance concerns around core public health functions. This is by no means, however, a comprehensive view of potential issues. Experience in other domains shows that we should expect to find other potential areas of vulnerability and potential attack surfaces. Cyber threats are always evolving, and there is no reason to believe that cyberbiosecurity will be different. Likewise, similar threats are likely to obtain in other areas relevant to public health and biosecurity, such as supply chain integrity or biological effects achieved through social media manipulation. Cyberbiosecurity concerns will not go away, and are only likely to continue to increase along with increasing biological capabilities and integration with information systems. The safety of all will depend on increased attention to and investment in mitigating these issues.