How China's Cyber Operations During the COVID-19 Pandemic Worsened the United States Biodefense and National Security

Lieutenant Colonel Regan F. Lyon

INTRODUCTION

Until 2020, biological warfare seemed like a remote threat to military operations and national security. Then, in March 2020, the novel SARS-associated coronavirus (SARS-CoV2) emerged and forced the world, including the Department of Defense (DoD), to acknowledge the calamitous potential of deadly virus pandemics.

The United States 2018 National Biodefense Strategy (NBS) warns of the need to enhance biological threat responses to prevent such detrimental effects.[1] It highlights the natural, isolated outbreaks of Systemic Acute Respiratory Syndrome (SARS), Ebola, and Zika viruses as potential agents on which clandestine bioweapon programs or terrorist groups seeking such programs could capitalize.[2] The NBS outlines a plan to prevent, detect, and respond to biological threats, providing defense and deterrence strategies to avert bioweapon use on American civilians or military personnel.[3] A nation with a strong biological defense decreases its population's vulnerability to pathogens with aggressive exposure mitigation and effective treatment measures, which thereby increase the nation's resiliency to public health crises. Such defense capabilities change an adversary's cost-benefit balance so that it avoids initiating a biological attack, providing deterrence from future threats. The success of these response strategies requires cooperation among government, medical, public health personnel, and the general population.

Lt. Col. Regan F. Lyon is an emergency medicine physician and a recent graduate of the Defense Analysis master's program at the Naval Postgraduate School in Monterey, CA. Lt. Col. Lyon was commissioned after graduation from Texas A&M University in 2006, completed medical school through the Uniformed Services University of the Health Sciences (USUHS), and graduated from the Emergency Medicine Residency at Brooke Army Medical Center. In 2014, she deployed as the medical director of the 83rd Rescue Squadron at Bagram Airfield, Afghanistan. She deployed in support of Operation INHERENT RESOLVE as the Special Operations Surgical Team's emergency medicine physician in 2017 and Team Leader in 2019. Lt. Col. Lyon has specific interests in the employment of battlefield medicine and its impact on operations. In recognition of her academic contributions, she was appointed to an Assistant Professorship at the USUHS Department of Military and Emergency Medicine.

SARS-CoV2's high transmission rate, long incubation period, airborne transmission, and significant morbidity/mortality are the ideal qualities for biological weapons.[4] Just two years after the NBS's publication, the COVID-19 pandemic put it to the test, thus providing an excellent opportunity to evaluate US bioterrorism defense and deterrence strategies.

Cyber-enabled information operations, conducted largely through social media, created confusion, skepticism, resistance, and division within the US population, and thus negatively impacted the US response to the COVID-19 pandemic.[5] A poor pandemic response from the US created an opportunity for China to improve its international reputation and power, consistent with its proclaimed national strategy.[6] This article describes how Chinese cyber-enabled information operations during the pandemic threatened our national security by increasing China's perceived power and undermining democracy.[7] It will also examine the effects of these operations on US' NBS and our increased vulnerability to future biological attacks.

BIOWARFARE AND ITS DEFENSE AND DETERRENCE

The psychological and physical impacts of biological weapons on civilians and military units have been exploited by adversaries throughout history. One of the first recounted biological warfare attacks was the siege of Caffa in 1346.[8] During this conflict, the invading Tartar army fell victim to the plague and sustained numerous casualties as a result. Recognizing the infectious nature of the disease, the Tartars tossed the infected cadavers over the city wall, initiating an outbreak, causing panic in the city, and forcing the opposing force to flee. More recently, the US saw the use of bioweapons in the wake of the September 11, 2001, terrorist attacks on the World Trade Center. The following week, several media outlets and Congressional

offices received anthrax spores through the mail in an attempt to capitalize on and further increase the heightened stress within the US. The overwhelming fear and psychological impact on the US populace underscore bioterrorism's potential for severe disruption even when casualties are limited.[9]

Biological weapons are considered weapons of mass destruction and are prohibited by the 1972 UN Biological Weapons Convention (BWC).[10] Unfortunately, not all potential adversaries adhere to these standards. Terrorists and other non-state actors are also not part of such agreements, and nation states that did ratify the treaty could potentially enlist covert operations or non-state proxies to use bioweapons. While there have been no intentional large-scale attacks by adversarial nation states to date, terrorist groups and covert operations have utilized biological weapons for small operations.[11] To prevent the use of biological weapons and limit their effectiveness when used, the biological defense and deterrence measures outlined in the NBS must be credible and effective.

More commonly used in nuclear warfare strategy, the concepts of defense and deterrence involve protection and security from offensive operations, including biological weapons, by an adversary.[12] Defense refers to the ability of a target to prevent or minimize damage sustained from an adversary action, decreasing the effectiveness of the attack and imposing a high cost-to-benefit burden on the adversary.[13] In the case of bioterrorism, adequate medical responses decreasing the transmissibility, disease severity, and mortality negate the overall weapon effectiveness. Deterrence attempts to prevent an adversary from taking harmful actions. One of the methods to achieve deterrence is deterrence by denial in which mechanisms are already in place that would mitigate an action taken by an adversary.[14] In the case of biological warfare, vaccines prevent susceptibility to a microbe, making the weapon useless against those vaccinated. The challenge with deterrence through vaccination is that a biological agent must be identified and determined to be a threat prior to developing a vaccine against it. An efficient defense response can also provide deterrence of future attacks because the effectiveness of previous attacks was low.

The linchpin for the NBS to be successfully employed is that the public receive reliable and objective communication.[15] Public distrust in the government causes multiple breakdowns in the NBS as it hinders communication to the public, inter-agency cooperation, and compliance with public health measures. Disseminating information regarding an outbreak, infection characteristics, response protocols, and public health measures relies on effective communication between the government and citizens. A lack of trust in the government breeds suspicion of the validity of information and fosters non-compliance, or even resistance, to protective measures. Furthermore, medical professionals skeptical of the government's actions or motivations during an outbreak will not likely reinforce and support the public service announcements. This lack of reinforcement from subject matter experts worsens public skepticism and non-compliance.

The misinformation campaigns that emerged during the COVID pandemic impaired the US' response to the public health crisis, thereby worsening the nation's bioterrorism deterrence and defense strategies. Adversaries, including China, have employed cyber operations against the US during the pandemic to cause chaos and confusion and used these operations to increase distrust in the U.S. Government (USG).[16] As the fruits of their labor have played out, however, third- and fourth-order effects of these misinformation campaigns are shaping a narrative to the world regarding US bioterrorism vulnerability.

CHINA'S CYBER OPERATIONS COVID-19 CASE STUDY

While likely not an original goal of China's cyber operations, the public health crisis and pandemonium that followed the SARS-CoV2 outbreak have highlighted our nation's bioweapon vulnerabilities to the world and may have caused unintended serious national security consequences. Any uncertainty adversaries may have had regarding our biodefense capabilities and weaknesses, which deterred employment of biological weapons prior to the pandemic, no longer exists. This section utilizes the COVID-19 pandemic as a case study to provide examples of China's cyber operations' effects on our bioterror defense and deterrence.

China's status as a reliable global power was called into question because of its initial cover-up of the outbreak in December 2019 and erroneous accusations of accidental release from research laboratories. Chinese misinformation and propaganda campaigns began in February 2020 with two primary objectives: shift blame for the pandemic from China and create dissonance within the finger-pointing democracies to worsen their pandemic management and control.[17]

Official statements, news reports, and social media campaigns attempted to turn speculations of COVID-19's origin outside Chinese borders.[18] Over a year later, China has continued to change the origin narrative through Facebook posts and peer-reviewed medical journals, despite substantiating evidence, to off-load the blame for the catastrophic infection numbers.[19] Through tools such as the Great Cannon, Chinese media highlighted their international humanitarian aid to nations experiencing medical supply shortages, underscoring their superior crisis response capability.[20]

Sowing Distrust

To destabilize democracies, specifically the US, cyber misinformation operations were employed to create domestic division, sow distrust and panic, and further deteriorate outbreak control.[21] Since the first case of COVID-19 was reported in the US on January 19, 2020,[22] Americans have anxiously watched if the government's response would prevent a nation-wide crisis. Case numbers grew over the next few weeks, and with stories of lockdowns across the world filling newsfeeds, concern grew as to how severely the US would restrict its citizens to control virus transmission. Internationally, nations began casting blame on China for downplaying the outbreak, which began the largest global health and economic crisis in recent history.

The reputational damage triggered China's plummet from its recent rise in power, leading Beijing to shift blame and portray its strong, heroic role relative to floundering democratic states.

One of China's cyber operations aimed at discrediting the USG's COVID response occurred almost simultaneously with the "viral origin" propaganda early in the pandemic. Chinese cyber forces amplified a fake news rumor of the White House implementing the Stafford Act and ordering a nation-wide shutdown.[23] In a national crisis, the Robert T. Stafford Disaster Relief and Emergency Assistance Act authorizes the President to mobilize an emergency federal government response, institute rules and regulations, and to utilize Department of Defense assets to assist state and local governments.[24] Martial Law, which is separate from the Stafford Act, refers to military control over domestic populations during wartime or natural disaster. Conspiracists conflated the two terms and speculated President Trump would invoke the Stafford Act for a national lockdown and utilize military force to ensure compliance. While officials do not believe Chinese cyber personnel started these theories, evidence points to China utilizing social media bots to proliferate and highlight them on media platforms to create division and distrust among the US population.[25]

US citizens were significantly confused, discouraged, and fearful when China executed a cyber-enabled information operation to capitalize on the instability. On March 13, 2020, social media posts began circulating that warned of a National Guard deployment to enforce an impending Stafford Act implementation by the White House.[26] No clear evidence suggests the original posts were the result of a cyber-enabled information operation. However, Chinese social media bots spreading these messages attributed the information to close contacts within reputable organizations like the National Guard, Department of Homeland Security, the State Department, FBI, etc., and encouraged wider sharing of the messages.[27] The results reinforced fears of the pandemic's severity and beliefs that the administration was about to exceed its authority. Warnings of a nationwide shutdown supported concerned citizens' speculation of officials minimizing the virus's severity. For citizens already dissatisfied with the current administration, rumors of enacting the Stafford Act deepened their distrust in the government. These two extreme divergent reactions began a chain reaction which demonstrated how China's cyber operations undermined democratic power and increased our bioterror vulnerability.

Most analysts believe that China's primary objective in this campaign was to increase Americans' anti-government sentiments, worsening stability.[28] The threat of invoking a nationwide lockdown with deployed National Guard personnel for enforcement sparked public concern of an abuse of power by the Trump administration and violation of citizens' rights. The social media posts and text messages referencing sources linked to reputable government agencies exploited people's trust in their network and strengthened these allegations. Such civil unrest begins to undermine democratic institutions, worsens other nations' perceptions of our stability, threatens national security, and advances the communist government's argument of superiority.

Defense Breakdown

When the Stafford Act social media posts began to circulate, serious concerns spread that the virus was more dangerous than originally reported. The US public flooded stores to stock up on "essential items" in preparation for a lockdown. In addition to the infamous toilet paper shortage, shelves and online outlets were soon devoid of masks, gloves, and sanitizers, including within healthcare supply chains. Once it was discovered that N95 masks, used to prevent medical personnel from contracting airborne pathogens, were effective against SARS-CoV2, the situation worsened.[29] Demand quickly exceeded supply, leaving frontline medical personnel without the appropriate personal protective equipment (PPE) required to care for infected patients.[30] Healthcare workers began openly complaining of the nation-wide PPE shortage and the risk it brought to their lives.

The strained PPE supply chain exacerbated by the public hoarding caused a ripple effect within the healthcare system. Hospitals began instituting resource conservation policies to extend the life of supplies intended for one-time use since these items were on indefinite backorder. Concurrently, these measures also helped to alleviate costs since hospitals were generating less revenue from the Stay-at-Home campaign. Healthcare workers interpreted these PPE conservation measures as the hospitals jeopardizing their safety and initiated lobbying for government involvement.

The saturation of stories showing pandemic mismanagement by democratic nations and exaggerated success stories of containment at home boosted China's legitimacy on the global stage. US media was swarmed with accounts of disgruntled healthcare workers risking their lives daily due to a lack of PPE. Beijing capitalized on these news reports and recirculated them through the Great Cannon as propaganda illustrating how China was gaining control of viral spread and protecting their healthcare workers better than the western democracies.[31] Chinese cyber accounts and media sources discovered and broadcasted pictures of healthcare workers using garbage bags as PPE.[32] Such stories accused the ill-prepared countries of ignoring the needs of their medical personnel and putting additional lives at risk. Although these claims were mere speculation at the time, prospective studies have since reported healthcare workers with inadequate PPE had a statistically significant increase of COVID-19 infection compared to those with adequate PPE.[33] This Chinese cyber strategy was employed domestically to reinforce the long-time message to citizens that "socialism is good, democracy is bad."

The 2018 NBS mandates robustly mobilizing PPE for frontline healthcare workers and establishing a communication plan on preventive health measures for the public in the event of an attack.[34] The ability to provide adequate PPE for medical personnel is a vital defense tactic, as it increases the efficiency of the healthcare system to treat casualties in response to a biological outbreak. Having the ability to mobilize these resources to hospitals strengthens bioterror deterrence by demonstrating to a potential adversary that a bioterror attack would have a limited effect on a population.

The initial US defense measures against SARS-CoV2 were painted as ineffective through reports of public hoarding, inadequate PPE supply chains, and inappropriate PPE conservation measures by hospitals. While Beijing's primary objective was to increase China's international reputation, its cyber operations highlighting the inadequate public health response worsened US national security by undermining our biodefense strategy.

Deterrence Breakdown

Classic nuclear weapon deterrence focuses on retaliation and what has been called mutually assured destruction, but future bioweapon deterrence relies more on past defensive responses to previous biological outbreaks. Increasing the effectiveness of public health and protective measures in decreasing impacts of a biological attack reduces the incentive for adversary use of biological weapons. Non-compliance with these measures reduces their deterrent value.

America's individualistic nature, amplified by the cyber-induced government distrust, led to significant non-compliance with government-implemented public health policies. One survey indicated that 58% of Americans preferred "freedom...without interference from the state," compared to 30-38% of Europeans.[35] This hindered our ability to "flatten the curve" compared to other countries.[36] The US' inadequate public health measures followed by the rapid spread of COVID-19—especially compared to China—signals to adversaries our vulnerability to biological attacks.

Another bioweapon deterrence strategy is vaccination against the biological agent. Because vaccines cannot be developed until after a threat is identified, vaccines deter the use of a specific agent for future attacks. This strategy only works for a nation with access to vaccines and a population willing to be inoculated.

China's attack on Western-developed vaccines started with cyber operations intended to steal SARS-CoV2 vaccine development information. The US identified both Chinese and Russian cyber espionage attacks against vaccine developers, another indication of China borrowing Russia's playbook.[37] This may have strictly been another example of Chinese intellectual property theft, but US officials raised concerns that these cyber actions could sabotage the target's operations to create defects in the product and dissemination delays.[38] Broken promises of vaccination timelines and effectiveness expanded suspicion towards the government, escalated the anti-vax claims, and exacerbated public division. Operation Warp Speed, however, maintained a reasonable timeline, and China turned to other tactics to reinforce their legitimacy, to undermine democracy, and to weaken our national security and biodefense measures.[39]

Past vaccination resistance, such as during the 19th-century UK smallpox epidemic and the 2019 US measles outbreak, highlights a population's vulnerability to anti-vaxxer campaigns. This is even more of a problem when cyber disinformation reinforces doubts.[40] For example, early in the pandemic, COVID-19 anti-vaccine social media posts warned that future coronavirus vaccines could contain toxic chemicals or tracking devices used by the USG.[41]

China fueled the anti-vax movement by discrediting US vaccines through disinformation campaigns.[42] The Wolf Warriors began spreading conspiracy theories regarding the Pfizer and Moderna vaccines even before they were released to the public.[43] These trolling attacks focused on the vaccines' safety and were echoed by Chinese nationalist media and Chinese officials.[44] Other Chinese blogs claimed the efficacy of the mRNA vaccines was only 29%, significantly lower than what the US claimed and what turned out to be true. Simultaneously, cyber campaigns boasted of China-developed vaccines in attempts to increase international demand and bolster their pandemic reputation.[45]

COVID vaccine speculation and conspiracy theories, exacerbated by cyber disinformation campaigns, created significant resistance to receiving a vaccine. Surveys conducted prior to vaccine release estimated one third of Americans, compared to 14% of UK citizens, would refuse vaccination.[46] By summer of 2021, a few months after a vaccine was available to all citizens 12 years of age or older, only 48.5% of the population was fully vaccinated.[47] The unvaccinated population enabled the Delta variant to become the dominating SARS-CoV-2 strain in August 2021, and hospital systems in less-widely vaccinated populations were once again strained.[48] The unvaccinated then facilitated further mutations that led to the highly-transmissible Omicron variant, which emerged in the US in early December 2021.[49] A population that is not vaccinated increases susceptibility to a biological agent and facilitates its propagation, transmission, and mutations, ultimately decreasing deterrence by denial.

CONCLUSION

The SARS-CoV-2 pandemic panic in 2020, exacerbated by China's misinformation cyber campaign, highlighted a critical vulnerability in the most important US defense strategies against bioterrorism: prevention and resilience. The simultaneous reports of inadequate PPE for healthcare workers reduced faith in the government by affected healthcare workers and concerned citizens alike. The collective effort of the US population began to split just when cohesiveness was most needed to flatten the curve of COVID-19 infections, gain control of the pandemic and economic crises, implore Americans to protect themselves with vaccines, and salvage our international political and biodefense image. The growing impact of mis- and disinformation in the twenty-first century not only made the US a target for exploitation but showcased our inadequate pandemic response measures. Ignoring the role of cyber operations in amplifying the effects of bioterrorism compounds our vulnerability to such attacks.

Any signals that biological deterrence or defense mechanisms were weakened because of China's cyber-enabled information operations will play into the adversary cost-to-benefit considerations of bioweapon employment. This confluence of cyber operations, medicine and public health, and national security is unique, unprecedented, and requires a multi-dimensional counter strategy. The medical community must work with the government to evaluate the pandemic response in relation to the NBS, identify NBS weaknesses and systemic failures, and

strategically signal the rectification of identified vulnerabilities. Concurrently, this pandemic has highlighted evolving Chinese cyber strategies for the cyber and intelligence communities. It has also taught medical professionals to consider cyber threats beyond personal health information hacking efforts. Recognition of China's brazen tactics will assist the US in developing countermeasures for future cyber information operations and in arming US citizens with the tools to identify and discredit such propaganda. Understanding the role of cyber-enabled information operations on our biodefense strategies will enable further research on countering our weaknesses and protecting our national security.

DISCLAIMER

The views expressed herein are those of the author and do not reflect the official policy or opinion of the Naval Postgraduate School, Department of the Air Force, Special Operations Command, Department of Defense, or the U.S. Government.

NOTES

1. White House, *National Biodefense Strategy of the United States of America (*Washington, DC: White House, 2018), i.
2. Ibid, 2–3.
3. Ibid, 1.
4. Yu Chen and Lanjuan Li, "SARS-CoV-2: Virus Dynamics and Host Response," *The Lancet Infectious Diseases* 20, no. 5 (May 1, 2020): 515–16, https://doi.org/10.1016/S1473-3099(20)30235-8.
5. Julian E. Barnes, Matthew Rosenberg, and Edward Wong, "As Virus Spreads, China and Russia See Openings for Disinformation," *The New York Times*, March 28, 2020, sec. U.S., https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html.
6. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: Department of Defense, 2020), https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.
7. Jessica Brandt and Torrey Taussig, "The Kremlin's Disinformation Playbook Goes to Beijing," Brookings, May 19, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/.
8. Stefan Riedel, "Biological Warfare and Bioterrorism: A Historical Review," *Baylor University Medical Center Proceedings* 17, no. 4 (October 2004): 400, https://doi.org/10.1080/08998280.2004.11928002.
9. Robert Roos and Lisa Schnirring, "Public Health Leaders Cite Lessons of 2001 Anthrax Attacks," Center for Infectious Disease Research and Policy, September 1, 2011, https://www.cidrap.umn.edu/news-perspective/2011/09/public-health-leaders-cite-lessons-2001-anthrax-attacks.
10. "Biological Weapons," accessed March 11, 2022, https://www.who.int/westernpacific/health-topics/biological-weapons; Riedel, "Biological Warfare and Bioterrorism."
11. Riedel, "Biological Warfare and Bioterrorism," 404.
12. Glenn Herald Snyder, *Deterrence and Defense* (Princeton University Press, 2015), 3.
13. Ibid, 4.
14. Ibid, 14–15.
15. Abhay B. Kadam and Sachin R. Atre, "Negative Impact of Social Media Panic during the COVID-19 Outbreak in India," *Journal of Travel Medicine* 27, no. 3 (May 18, 2020), https://doi.org/10.1093/jtm/taaa057.
16. Mark Bryan Manantan, "Unleash the Dragon: China's Strategic Narrative during the COVID-19 Pandemic," *The Cyber Defense Review* 6, no. 2 (Spring 2021): 71–89.
17. David Erdahl, Sandy Gitter, and Brock Lu, "China Will Do Anything to Deflect Coronavirus Blame," *Foreign Policy* (blog), accessed September 8, 2020, https://foreignpolicy.com/2020/03/30/beijing-coronavirus-response-see-what-sticks-propaganda-blame-ccp-xi-jinping/.
18. Ibid.
19. Emma Graham-Harrison and Robin McKie, "A Year after Wuhan Alarm, China Seeks to Change Covid Origin Story," *The Guardian*, November 29, 2020, http://www.theguardian.com/world/2020/nov/29/a-year-after-wuhan-alarm-china-seeks-to-change-covid-origin-story.
20. Keith Bradsher and Liz Alderman, "The World Needs Masks. China Makes Them, but Has Been Hoarding Them.," *The New York Times*, March 13, 2020, sec. Business, https://www.nytimes.com/2020/03/13/business/masks-china-coronavirus.html.
21. Brandt and Taussig, "The Kremlin's Disinformation Playbook Goes to Beijing."
22. Michelle L. Holshue et al., "First Case of 2019 Novel Coronavirus in the United States," *New England Journal of Medicine* 382, no. 10 (March 5, 2020): 929–36, https://doi.org/10.1056/NEJMoa2001191.
23. Edward Wong, Matthew Rosenberg, and Julian E. Barnes, "Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say," *The New York Times*, April 22, 2020, sec. U.S., https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html.
24. "H.R.2707 - 100th Congress (1987-1988): Major Disaster Relief and Emergency Assistance Amendments of 1987," November 23, 1988, 1987/1988, https://www.congress.gov/bill/100th-congress/house-bill/2707.
25. Wong, Rosenberg, and Barnes, "Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say."

NOTES

26. Ibid.
27. Ibid.
28. Barnes, Rosenberg, and Wong, "As Virus Spreads, China and Russia See Openings for Disinformation."
29. Kadam and Atre, "Negative Impact of Social Media Panic during the COVID-19 Outbreak in India."
30. World Health Organization, "Shortage of Personal Protective Equipment Endangering Health Workers Worldwide," World Health Organization, March 3, 2020, https://www.who.int/news-room/detail/03-03-2020-shortage-of-personal-protective-equipment-endangering-health-workers-worldwide.
31. Li Yuan, "With Selective Coronavirus Coverage, China Builds a Culture of Hate," *The New York Times,* April 22, 2020, sec. Business, https://www.nytimes.com/2020/04/22/business/china-coronavirus-propaganda.html.
32. Ibid.
33. Long H Nguyen et al., "Risk of COVID-19 among Front-Line Health-Care Workers and the General Community: A Prospective Cohort Study," *The Lancet Public Health* 5, no. 9 (September 1, 2020): e475–83, https://doi.org/10.1016/S2468-2667(20)30164-X.
34. White House, *National Biodefense Strategy of the United States of America.*
35. Alex Fitzpatrick, "Why the U.S. Is Losing the War On COVID-19," *Time,* August 13, 2020, https://time.com/5879086/us-covid-19/.
36. Ibid.
37. Joseph Marks, "The Cybersecurity 202: Russia and China's Vaccine Hacks Don't Violate Rules of Road for Cyberspace, Experts Say," *Washington Post,* July 20, 2020, https://www.washingtonpost.com/politics/2020/07/20/cybersecurity-202-russia-china-vaccine-hacks-dont-violate-rules-road-cyberspace-experts-say/.
38. Julian E. Barnes and Michael Venutolo-Mantovani, "Race for Coronavirus Vaccine Pits Spy Against Spy," *The New York Times*, September 5, 2020, sec. U.S., https://www.nytimes.com/2020/09/05/us/politics/coronavirus-vaccine-espionage.html.
39. Jon Cohen, "With Global Push for COVID-19 Vaccines, China Aims to Win Friends and Cut Deals," *Science,* November 25, 2020, https://www.sciencemag.org/news/2020/11/global-push-covid-19-vaccines-china-aims-win-friends-and-cut-deals.
40. Steven King, "Coronavirus Vaccine: Lessons from the 19th-Century Smallpox Anti-Vaxxer Movement," The Conversation, July 31, 2020, http://theconversation.com/coronavirus-vaccine-lessons-from-the-19th-century-smallpox-anti-vaxxer-movement-143375. Julie Charpentrat, "There's Another Insidious Side Effect of This Pandemic - More Anti-Vaxxer Activity," ScienceAlert, July 5, 2020, https://www.sciencealert.com/anti-vaxxers-seize-virus-moment-to-spread-fake-news.
41. Charpentrat, "There's Another Insidious Side Effect of This Pandemic - More Anti-Vaxxer Activity"; Elizabeth Cohen and Dana Vigue, "US Government Slow to Act as Anti-Vaxxers Spread Lies on Social Media about Coronavirus Vaccine," *CNN*, August 13, 2020, https://www.cnn.com/2020/08/12/health/anti-vaxxers-covid-19/index.html.
42. Barnes and Venutolo-Mantovani, "Race for Coronavirus Vaccine Pits Spy Against Spy."
43. Carmen Paun and Susannah Luthi, "What China's Vax Trolling Adds up to," *POLITICO,* January 28, 2021, https://politi.co/3oqX66H.
44. Yaqiu Wang, "China's Dangerous Game Around Covid-19 Vaccines," Human Rights Watch, March 4, 2021, https://www.hrw.org/news/2021/03/04/chinas-dangerous-game-around-covid-19-vaccines.
45. Paun and Luthi, "What China's Vax Trolling Adds up to."
46. Cohen and Vigue, "US Government Slow to Act as Anti-Vaxxers Spread Lies on Social Media about Coronavirus Vaccine." King, "Coronavirus Vaccine."
47. Hannah Ritchie et al., "Coronavirus Pandemic (COVID-19) Vaccinations," Our World in Data, accessed July 14, 2021, https://ourworldindata.org/covid-vaccinations; Cheyenne Haslett, "FDA Authorizes Pfizer Vaccine for 12-15-Year-Olds," *ABC News*, May 10, 2021, https://abcnews.go.com/Politics/fda-authorizes-pfizer-12-15-year-olds/story?id=77419872.