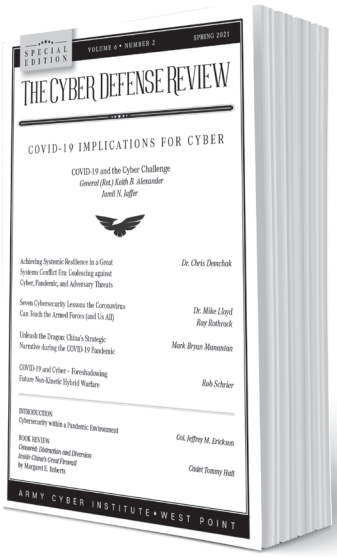
VOL. 6 ◆ NO. 2

The Cyber Defense Review: Cybersecurity within a Pandemic Environment

Colonel Jeffrey M. Erickson



Welcome to the COVID-19 Special Edition of *The Cyber Defense Review* (CDR). In this issue, we are examining how the pandemic has impacted cybersecurity, and how pandemics may impact it in the future.

The genesis of this issue occurred in early Spring 2020. The COVID-19 pandemic was emerging, infection numbers were rising, and the world began shifting to a telework-focused workplace to mitigate the spread. Immediately, the cyber threat space became much more complex as attack surfaces multiplied. Organizational information security officers and IT departments had to immediately focus on employees' home systems, networks, and Internet Service Providers (ISP) while maintaining the security of existing company networks. Teleconference capability providers, such as Zoom, instantly became household names and experienced unprecedented growth (Zoom, for example, saw a 30-fold increase in its use),[1] and Virtual Private Networks became commonly used among the growing teleworking population.

Colonel Jeffrey M. Erickson is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. As Director, COL Erickson leads a 60-person, multi-disciplinary research institute focused on expanding the Army's knowledge of the cyberspace domain. He began his Army career as an Armor officer before transitioning to the Simulation Operations functional area, where for the last 15 years, he has been using simulations to train from the individual to the Joint and Combatant Command levels. He has a B.S. in Computer Science from the United States Military Academy, an M.S. in Management Information Systems from Bowie State University, and an M.S. in National Resource Strategy from the Eisenhower School (formerly the Industrial College of the Armed Forces). His fields of interest are simulations for live-virtual-constructive training, testing, and wargaming.

In addition to the technical challenges of this environment, we witnessed many interesting second and third-order effects that impact cybersecurity, including:

- Scammers intent on grifting money implemented some of the principles of Information Operations (IO) by appealing to users' emotions through powerful narratives such as fake charity funds for first responders.[2]
- The merging of work and home life (which had been happening over the last few decades with the addition of home PCs, e-mail, smartphones, etc.) suddenly shot forward. Now, it is common for employees to be just as productive from home as in the office. Still, the expectation for responding to taskings (even after hours or on weekends) has almost obliterated the boundary between the private and work worlds.
- As telework became widely accepted, many companies began to realize potential savings by reducing high-cost office space.[3] Likewise, employees realized some cost savings with reduced commutes and the ability to move to lower cost of living areas.
- The e-commerce economy saw impressive growth as consumers avoided in-store shopping. In many cases, this was the deathblow for many brick-and-mortar stores (with closings up to 10,000 by one estimate).[4]
- As the pandemic continued, it became more politicized so that simple actions, even one such as wearing a mask, became divisive.[5] Hostile actors (both domestic and foreign) leveraged these divisions to sow further dissent.
- The Anti-Vaxxer movement found new life as issues surrounding vaccination hesitancy, the US history of unethical medical testing, and government distrust came to the forefront.[6]

As we look forward, it is possible (even likely) that we will be in an annual cycle of pandemic responses. Even with widespread vaccinations, it is probable that the annual flu season (usually a minor inconvenience for most Americans) will become a more significant event with widespread implications across the networked economy.

In this VUCA (Volatile, Uncertain, Complex, and Ambiguous) environment, our authors have produced a series of fascinating articles to help provide deeper understanding of the cybersecurity challenges and potential solutions. At the strategic level, in "COVID-19 and the Cyber Challenge," GEN (Ret.) Keith Alexander and Mr. Jamil Jaffer assess the current situation's complexity and reinforce the need for a whole-of-society approach, including the public and private sectors. Additionally, they highlight the need for clearly communicated and enforceable rules of behavior when dealing with threats.

Considering that a crisis to one is an opportunity to another, Mr. Rob Schrier asserts that future asymmetrical hybrid attacks could be used in the pandemic environment and similarly argues for a whole-of-nation approach in "COVID-19 and Cyber – Foreshadowing Future Non-Kinetic Hybrid Warfare." In "Seven Cybersecurity Lessons Coronavirus Can Teach the Armed Forces (and Us All)," Mr. Ray Rothrock and Dr. Mike Lloyd use the current viral pandemic as an analogy for cybersecurity best practices, the application of cyber hygiene, and some insights into building resiliency.

In our Special Edition Research Articles, Dr. Chris Demchak argues that, in a rapidly changing world, we face a paradigm shift from Great Power Competition to Great Systems Conflict, and the need to build cyber resilience domestically and with allies. For those interested in understanding how the cyber environment can be used to support strategic narratives, Mr. Mark Bryan Manantan describes how the COVID-19 pandemic provided China the opportunity to further its strategic narrative using information warfare in "Unleash the Dragon: China's Resilience in a Great Systems Conflict Era." Continuing with a focus on China is United States Military Academy Cadet Tommy Hall's book review of *Censored: Distraction and Diversion Inside China's Great Firewall* by Margaret Roberts.

For a more holistic look at medical technology, Ms. Nataliya Brantley takes a broader look at the use of medical devices and their potential risks and vulnerabilities in "Homefront to Battlefield: Why the U.S. Military Should Care About Biomedical Cybersecurity." Finally, in "The Initiation of State-Sponsored Cyberattacks," Dr. Lance Hunter, Dr. Craig Albert, and Eric Garrett conduct an analysis of the factors that may indicate which types of states, in terms of capability and governance, are most likely to initiate cyberattacks against competitors. The authors provide some exciting results regarding asymmetrical conflict by looking at the Council on Foreign Relations Cyber Operations Tracker. You might be surprised who the likely aggressors are.

My hope is that you find these articles thought-provoking and perhaps motivate the larger community to apply these concepts not only to our current environment but to potential pandemics of the future. I want to thank and recognize the creativity and dedication of Michelle Marie Wallace, Sergio Analco, Gina Daschbach, LTC Mark Visger, SGM Jeff Morris, and Courtney Gordon-Tennant. The brilliant editing of the West Point Class of '70: Joe Reeder, Bill Spracher, Chip Leonard, and Bill Lane decidedly enhanced this special edition with their scholarly commitment and tireless effort.

Stay safe, stay alert, and stay informed.

NOTES

1. N. Sherman, "Zoom sees sales boom amid pandemic," British Broadcasting Corporation (BBC), June 2, 2020, accessed April 5, 2021, https://www.bbc.com/news/business-52884782.
2. "Coronavirus scams – consumer resources," Federal Communications Commission (FCC), accessed April 5, 2021, https://www.fcc.gov/covid-scams.
3. R. Kailath, "Do I really need this much office space? Pandemic emptied buildings, but for how long?" NPR, September 1, 2020, accessed April 5, 2021, https://www.npr.org/2020/09/01/906767790/do-i-really-need-this-much-office-space-pandemic-emptied-buildings-but-how-long.
4. "US and UK Store Closures Review 2020 and US Outlook 2021," Coresight Research, January 28, 2021, accessed April 5, 2021, https://coresight.com/research/us-and-uk-store-closures-review-2020-and-us-outlook-2021/.
5. E. Rabinovitch-Fox, "The battle over masks has always been political," The Washington Post, November 18, 2020, accessed April 5, 2021, https://www.washingtonpost.com/outlook/2020/11/18/battle-over-masks-has-always-been-political/.
6. D. Thompson, "Anti-vaxxers wage campaigns against COVID-19 shots," WebMD, January 29, 2021, accessed April 5, 2021, https://www.webmd.com/vaccines/covid-19-vaccine/news/20210129/anti-vaxxers-mounting-internet-campaigns-against-covid-19-shots.