COVID-19 and Cyber – Foreshadowing Future Non-Kinetic Hybrid Warfare

Rob Schrier

ABSTRACT

2020 was a year like no other in our lifetime. The COVID-19 Pandemic had a broadly evident and devastating impact on our health, our society, and our economy. Less evident have been adversaries' attempts to employ cyber-attacks[1] to exacerbate the pandemic through cyber-based disruption, exploitation and cyber-driven disinformation. The focus of this essay is on the nexus between cyber security and our future biological threat security (biothreat security). This article begins with a few key questions. What have we learned from observing adversary cyber tradecraft this year? What can we surmise our adversaries have learned from trying to take advantage of the current pandemic that they will use against the US in the future? More importantly, what can we extrapolate from these observations for the future of cyber-attack as the key element of strategic hybrid non-kinetic warfare?

My worst-case version of the future envisions adversaries creating or taking advantage of biothreat security events (or natural disasters) and using cyber-attacks and disinformation in multiple ways to aggravate the situation in a new form of hybrid non-kinetic warfare. We must predict the adversary's potential strategies for the future cyber-driven hybrid non-kinetic warfare and we must determine what we must do to prevent, preempt, or counter that future with our own disruptive campaigns. As a nation we need a level of resolve we do not have today to defend ourselves against cyber-attacks and their effects. While biothreat security is the sole focus of this essay, many of these ideas can be applied to climate events and other disruptions that impact key areas of the critical infrastructure, and our security more generally.

Rob Schrier is the Chief of Staff of Asymmetric Operations Sector of Johns Hopkins Applied Physics Laboratory. He leads research on military cyber and information operations (IO). He moved to the Laboratory after retiring from the DoD Senior Executive Service after a thirty-six year career. He served as the Deputy to the Commander, Cyber National Mission Force (CNMF), U.S. Cyber Command. Mr. Schrier was a plank holder on the team who established U.S. Cyber Command and served as the initial Deputy Director for Current Operations. Throughout his career, he held a variety of DoD leadership positions after beginning his career as an analyst. Mr. Schrier has more than ten years' experience as a leader in cyber operations. Mr. Schrier earned a Bachelor of Arts Degree from the University of Maryland, a Master of Science Degree in Applied Behavioral Science from Johns Hopkins University and attended the Chairman, Joint Chiefs of Staff CAPSTONE Course.

2020 OBSERVATIONS

The 2020 pandemic with its societal impacts provided a rich environment for cyber adversaries. While COVID-19 has had global impact, so have the increases in 2020 cyber-attacks, and this confluence has prompted several pundits to characterize 2020 as the year of "the Cyber Pandemic".[2] The 2020 cyber-attack landscape was quite widespread. We witnessed direct cyber-attacks on health organizations including the World Health Organization, pharmaceutical companies, medical research organizations and individuals through health-focused phishing emails. There were undoubtedly cyber-attack attempts to impact the outcome of the 2020 US federal election. We witnessed a surge in ransomware attacks against a range of targets including hospitals, schools, and local governments, some of which seemed motivated to exacerbate both the health and societal impacts of the pandemic. We witnessed perhaps the deepest, broadest supply-chain attack ever observed against the US government, and private industry.[3] Growing cyber-enabled disinformation attacks were a major feature of the 2020 cyber landscape. While it is hard to measure their long-term impact yet, there undoubtedly was some significant impact. As the American workforce largely transformed overnight from an office workforce to a remote workforce, we collectively became far more vulnerable to cyber-attack. In October 2020, 58% of the American workforce worked remotely either all or some of the time. The number was even higher in April 2020.[4] There is the prospect that a significant increase in remote work is here to stay. Also, much as the aftermath of 9/11 saw an increased focus on security against terror threats, an increased focus on biothreat security will hopefully be here to stay.

How Adversaries Can Employ Cyber-Attack

The focus for the rest of this article is about how our adversaries will use cyber-attacks to achieve strategic non-kinetic hybrid warfare objectives in the future and what we should do to keep them from being successful. Too many of us regard cyber-attacks as being for "cyber sake" and do not focus attention on cyber as a means to a strategic end. While none of this is new, our experiences with the 2020 pandemic have raised the likelihood of cyber-attack being the critical ingredient of future strategic hybrid non-kinetic warfare, especially events involving biothreat security.

2020 has clearly shown how vulnerable our security against biothreats is, whether against natural biological events, manmade biological attacks or adversary-driven natural biological attacks. The impacts of the COVID-19 pandemic, beyond the pure health aspects, are indisputable and they have exposed cyber vulnerabilities in every facet of our health ecosystem. They have also exposed vulnerabilities in our broader supply chain and redefined how we view the supply chain. For example, early in the pandemic, normally routine daily items like toilet paper, paper towels, cleaning and disinfecting products were in short supply and therefore a huge focus of the population and a potentially exploitable vulnerability. There was also a variety of domestic and global food supplies that had trouble reaching the shelves of grocery stores, creating a sense of a food shortage, even though there never actually was a food shortage in the US.[5] Finally, cyber-driven disinformation has clearly exacerbated the impact of the pandemic, our processes to measure and quantify their specific impacts are immature and still evolving.

Health Ecosystem Cyber Threat Landscape

So, I would like to offer my incomplete layperson's view of the health ecosystem cyber threat landscape as an adversary might see it. This is by no means a comprehensive examination by a biothreat security expert, so it is bound to be incomplete.

There are key vulnerabilities in every facet of the health ecosystem, including data security and health privacy information, health infrastructure and process security which also include research, clinical health practices, communications and public health, and public and government perceptions of the validity of the science and data. As adversaries look to employ cyber to achieve outcomes against this ecosystem, the following are exemplars of both public and private vulnerable areas they may target, though again this is by no means a comprehensive list:

- Medical equipment and medically relevant cyber systems used for research, medical storage, testing and treatment, to include remote care, in both the private, non-profit and public domains
- Medical equipment and their cyber systems used in creating or distributing pharmaceuticals and active pharmaceutical ingredients (APIs)
- Cyber systems associated with medical databases, health surveillance data, patient information and health records
- Cyber systems associated with government organizations overseeing healthcare and managing research, such as the CDC, NIH, FDA and others

- Medical communications systems that convey medical appointments, test results and other information through cyber driven communications systems (generating emails, text messages, etc. to patients or staff)
- The underlying supply chain driving the entire health ecosystem
- The private and professional emails of doctors, researchers, nurses, local, state, tribal, and federal government officials associated with the health ecosystem
- Disinformation against the general population and personnel in the health ecosystem.

While each of these cyber vulnerable areas is threatened individually, an even more serious strategic threat comes from an adversary mounting a campaign with attacks in several of these areas, planned in a way to achieve a specific strategic goal. Our adversaries have gained a tremendous amount of open-source intelligence by observing the pandemic this year through the lens of categories such as those listed above.

Cyber Driven Hybrid Non-Kinetic Warfare Scenarios

This leads us to the future of cyber-driven hybrid non-kinetic warfare and the central role that cyber may play in every facet of non-kinetic conflict. So, let's walk through a few representative, realistic future scenarios.

These scenarios could begin with either a natural biological event or with a manmade biological attack. For purposes of these scenarios, we focus on a natural biological event. An adversary will employ cyber-attacks in a number of ways to transform the biological event into a far more strategically consequential attack. The adversary will consider the primary outcomes it wishes to bring about. Does it want to focus on increasing loss of life or number of ill/casualties, overwhelming our healthcare system? Sow confusion to impact our economy, create societal friction, or undermine confidence in the government? Sow mistrust among US Allies? Degrade some industry or service to increase its own international market share or international political standing? While we may never know the precise motivation behind an adversary's cyber actions, it is important to regard the adversary in terms of the strategic motivations that may drive its coordinated actions.

To realize these goals, an adversary may want to cause failures (either recognized or not recognized) in medical equipment or databases, which will result in degrading healthcare delivery. It can corrupt health surveillance data that will impact decision making, testing and treatment. The adversary may attack actual medical equipment or accompanying infrastructure and communications to disrupt our response, such as within testing or manufacturing equipment. For example, if an adversary blocks or deletes a database that contains the list of patients eligible and prioritized for a vaccine or treatment, then long lines waiting for that vaccine or treatment will grind to a halt and healthcare will be delayed for a large number of people. A similar scenario involves an adversary interdicting an automated process to notify patients via text message or email of their medical appointment times for tests, vaccines, or treatment, that then send a large number of patients to healthcare locations to overwhelm and confuse the healthcare system.

The adversary may take steps to disrupt the medical research process. It can achieve this through compromising research equipment or the integrity of the research data, or by using disinformation through the introductions of false reports (variants of concern, vaccine efficacy, vaccine resistance, greater disease transmission, higher lethality, false alternative treatments, etc.) and combining this disinformation with the cyber compromises.

There are even more insidious or nefarious potential scenarios. An adversary can interfere with or corrupt the manufacture and distribution of pharmaceuticals, APIs, vaccine, or testing. The adversary can conduct cyber exploitation of the entire health ecosystem to gain intelligence advantage and targeting data. As part of this scenario, undoubtedly a part of any adversary cyber-attack campaign will include the attack and exploitation of email accounts associated with public or private healthcare officials through phishing attacks and other means. The adversary will then use disinformation as a weapon to exacerbate the strategic impact of any of the above scenarios. The disinformation will be critical to getting our general population to lose confidence in vaccines, testing, treatments, and overall effectiveness of the public and private health care system. Almost all information paths are cyber-based (or at least cyber-influenced); therefore, the cyber and cognitive elements of disinformation are intertwined.

The most troubling aspect of the scenarios above is that a determined adversary will weave together several of its cyber-attack capabilities into a focused campaign. That is why the above scenarios are representative and not meant to be comprehensive. The key point is that an adversary's campaign approach poses a very serious strategic danger to the US and our Allies. In a sense the US was lucky in the current pandemic, as it seems no adversary had a multi-faceted campaign already in place and could not take full advantage of cyber vulnerabilities across our entire biosecurity ecosystem. However, some were opportunists with capabilities ready to employ and we should assume they have observed and learned from 2020 actions—theirs and ours.

Accepting the Premise of Cyber-Attack Driven Hybrid Non-Kinetic Warfare, What Steps Can the US Government Take?

I have painted some dire scenarios for the future. We must not passively accept these scenarios as inevitable. First, we must face the brutal facts regarding both our level of vulnerability and our adversaries' will and intentions. Second, we must be resolute, even through all the challenges, to gain and maintain an upper hand. We need to be willing both to have a sense of urgency and to regard this as a long game and demand that government, industry, non-profits, and academia put tremendous energy into solving these problems as if our national safety and security depend on it—as it does.

The best way the US can ensure that adversaries can never actualize the above scenarios or other cyber threats to our biothreat security, both in pandemic events but also in broader biothreat events, is to create a whole-of-nation campaign to disrupt our adversaries and keep the cyber risk to our biothreat security very low. The following are the key elements of that campaign.

- The government must continue to prioritize and significantly expand "persistent engagement" as the cornerstone of our overall cyber defense.[6] We must continuously contest our cyber adversaries outside of US networks to keep them off balance. We will never successfully defend our health ecosystem from cyberattack just by trying to close down vulnerabilities within our own networks. This tracks with a recommendation from the Solarium Commission's Recommendation Pillar 6 (Preserve and Employ the Military Instrument of National Power).[7]

- The US must develop a comprehensive biothreat security strategy that includes a focused effort to assess and improve cybersecurity and cyber defense across the entire public and private health ecosystem. This will be a major undertaking that will require public, private, non-profit and academic collaboration.

- Immediately implement the Solarium Commission's Recommendation Pillar 1 (Reform the U.S. Government's Structure and Organization for Cyberspace). The government must create a National Cyber Director as outlined in the report to kickstart a whole-of-government approach to national Cyber Defense and accelerate building the public-private partnership.
    - I urge moving beyond one of the Commission's recommendations and opting for my more aggressive recommendation to create an effective national level 24/7 cyber defense operational capability.[8]

- Implement the Commission's Recommendation Pillar 5 (Operationalize Cybersecurity Collaboration with the Private Sector). Building an operationally credible private-non-profit-international-US government partnership will produce a critical layer of cyber defense which today may be our weakest area. We need to find innovative ways to harness the enormous cyber power of the private sector, who will be critical in securing our health ecosystem including key medical equipment.

- Finally, we need to develop and implement a national strategy to prevent, counter and mitigate the impacts of disinformation against US and Allied interests. This strategy should be developed with a focus largely on cyber-attack since cyberspace is a key factor in virtually all facets of disinformation and should be developed as part of the broader cyber recommendations and not apart from them. Preempting and countering disinformation must become a key part of our defending forward strategy.

The key will be for the US to execute these recommendations as a continuous campaign, since the strategic biothreat security threats to our nation are here to stay. Our strength will be in coordinating efforts to carry out the above recommendations and combining their effects. While there will be those who disagree with my specific recommendations, my hope and expectation is that my depiction of the threat landscape and representative scenarios will spark further dialogue and debate, so as a nation we can put our tremendous energy into solutions for these problems that our national safety and security can depend on over the long term.

NOTES

1. The term cyber-attack will be used throughout this paper in a broad non-doctrinal definition to represent offensive cyber operations, cyber exploitation and cyber-driven disinformation.
2. Don Lohrmann, Government Technology Magazine, December 12, 2020, "2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic."
3. Kai Paul, The Guardian, "What you need to know about the biggest hack of the US government in years", 15 December 2020 and Ellen Nakashima, The Washington Post, February 23, 2021, "Biden administration preparing to sanction Russia for Solar Winds hacks and the poisoning of an opposition leader."
4. Megan Benan, Gallup News, October 13, 2020, "COVID-19 and Remote Work: An Update."
5. USDA Report, "Will COVID-19 Threaten Availability and Affordability of our Food?,"posted by Robert Johansson, USDA, Chief Economist in Food and Nutrition Magazine, April 16, 2020; Amy Gunia, Time Magazine, May 8, 2020, "How Coronavirus is Exposing the World's Fragile Food Supply Chain – and Could Leave Millions Hungry."
6. Foreign Affairs Opinion, "How to Compete in Cyberspace – Cyber Command's New Approach," Authors Paul Nakasone and Michael Sulmeyer, August 25, 2020. In this opinion, the authors write, "Cyber Command implements this defend forward strategy through the doctrine of persistent engagement. The idea behind persistent engagement is that so much of the corrosive effects of cyber-attacks against the United States occur below the threshold of traditional armed conflict. Yet much of Cyber Command's combat power had been devoted toward preparations in the event of future contingencies. We realized that U.S. Cyber Command needs to do more than prepare for a crisis in the future; it must compete with adversaries today. This doctrine of persistent engagement reflects the fact that one-off cyber operations are unlikely to defeat adversaries. Instead, US forces must compete with adversaries on a recurring basis, making it far more difficult for them to advance their goals over time."
7. Cyberspace Solarium Commission Report, Cyberspace Solarium Commission - Report, March 2020.
8. Rob Schrier, *The Cyber Defense Review*, Fall 2019, Volume 4, Number 2, 23-26.