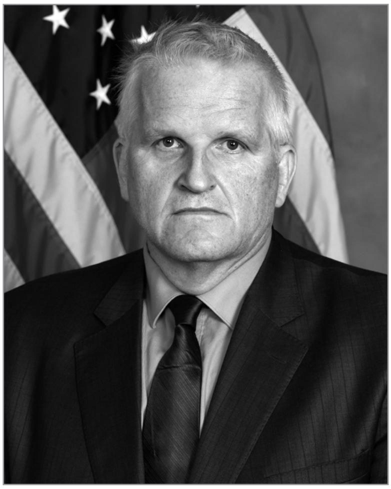
COVID-19: The Information Warfare Paradigm Shift

Jan Kallberg, Ph.D.
Rosemary A. Burk, Ph.D.
Bhavani Thuraisingham, Ph.D.

INTRODUCTION

Thomas Kuhn's *The Structure of Scientific Revolutions* highlights the critical term "paradigm shift," which occurs when it suddenly becomes evident that earlier assumptions are no longer correct. The plurality of the scientific community studying this domain accepts the change. These paradigm-shifting events can be scientific findings or, as in the social sciences, a system shock that creates a punctured equilibrium, triggering a leap forward acquiring new knowledge.

In information warfare, the government lines of effort have been to engage fake news, intercept electoral interference, fight extremist social media as the primary combat theater in the information space, and use the tools to influence a targeted audience to defend against an adversary that seeks to influence our population. The COVID-19 pandemic generates a rebuttal, or at least a challenge, of the information warfare assumption that our government's authority, legitimacy, and control are mainly challenged by tampering with the electoral system, fueling extremist views, and distributing fake political news. The fake news and extremist social media content exploit fault lines in our society and create civil disturbances, tensions between federal and local government, and massive protests that impact only a fraction of the population. We have seen with COVID-19, for example, public health has a far more powerful effect on public sentiment and is more likely to create reactions of larger magnitude within the citizenry, which ripple out. These ripple effects



Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's Degree in Political Science from the University of Texas at Dallas, and a J.D./LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham. Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities, especially offensive cyber operations as an alternative policy option. His personal website is www.cyberdefense.com.

have been hard to predict. The long-term psychological, societal, and health impacts of COVID-19 events have still not yet unfolded. As an example, according to the National Bureau of Economic Research, no other historic pandemic event has affected the stock market as profoundly as COVID-19.[1]

SOCIETAL PRIORITIES

COVID-19 has provided an essential data set for understanding what matters to the population. The environmental aspect of cyber defense, linked to public health, has not drawn attention as a national security matter. As living beings, we react to threats to our living space and the immediate environment. Jeopardizing the environment, intentionally or unintentionally, has historically led to the direct injection of fear and strong reactions in the population. Even unexpected accidents with environmental impact have triggered strong moves in public sentiment towards fear, panic, anger against the government, and challenges to public authority. One example is Chernobyl, which according to former Soviet leader Gorbachev was accredited as the reason for the Soviet collapse five years later as the popular lost faith in their government and their ability to protect their citizens.[2]

An adversary seeks effects that support its agenda and strategy. If an adversary engages in information operations, there is a goal and endgame that it is trying to achieve. From the adversary's perspective, what impact can it have on a US Presidential election, and does it matter whether a Democratic or Republican President is elected? What is the upside? The inference is concerning, and adequate resources are dedicated to addressing the problem.[3] However, if we look at the actual changes to policy outcome, the interference will likely not meet the intended goals of swaying the elections.

Dr. Rosemary Burk is a Senior Biologist with the Department of the Interior, U.S. Fish and Wildlife Service, Head Quarters, Falls Church, Virginia. She earned a Ph.D. in Biology from the University of North Texas with a specialization in aquatic ecology and environmental science. She has co-authored several articles that have linked failed cyber defense and environmental consequences including "Failed Cyberdefense: The Environmental Consequences of Hostile Acts," which was published by the U.S. Army's *Military Review* in 2014.

US defense spending and its grand impact on the world order have been nearly consistent over the decades. Even when presidents and political leaders have made drastic policy decisions, the actual change in the geopolitical landscape has been marginal. As a recent example, President Trump's movement of troops from Germany to Poland, Belgium, and Italy is simply a rearrangement and a new geopolitical position. From a Russian perspective, with an increasingly more military-able Poland and increasing commitment from several NATO countries, the US movement of troops out of Germany does not change the current situation. Until COVID-19, the return on the Russian information warfare investment was not present if the intended goal were to directly impact US policy and general sentiment. Groups and fragments of the population have been impacted, but the general population and large parts of the government and political machinery have been unaffected. We have seen that COVID-19 and information operations have fueled public health concerns and those fears are producing sentiment swings and foreign influence at a higher magnitude.

According to Kenneth Waltz, it is not what you do, but instead what you can do, that gives you the power.[4] A foreign adversary can gain more influence over popular sentiment through threatening to harm the immediate environment and public health, especially as these adversaries do not subscribe to the same ethics, code of conduct, and playbook as the US. COVID-19 has shown that cyber-attacks which create environmental and health threats, even those with a very low probability of occurring, can cause drastic swings in sentiment. Cyber-attacks that threaten public health and the citizens' immediate environment put the government's legitimacy, authority, and control under pressure, and trigger a significant decrease in citizen confidence in the current political leadership. The magnitude of such impacts can hardly be created by tweets and fake news, or rally

Dr. Bhavani Thuraisingham is the Founders Chair Professor of Computer Science and the Executive Director of the Cyber Security Research and Education Institute at The University of Texas at Dallas (UTD). She is also a visiting Senior Research Fellow at Kings College, University of London and an elected Fellow of the ACM, IEEE, the AAAS, and the NAI. Her research interests are on integrating cyber security and artificial intelligence. She has received several awards including the IEEE CS 1997 Technical Achievement Award, ACM SIGSAC 2010 Outstanding Contributions Award, and the IEEE ComSoc Communications and Information Security 2019 Technical Recognition Award. Her 40-year career includes industry (Honeywell), federal research laboratory (MITRE), US government (NSF) and US academia. Her work has resulted in 130+ journal articles, 300+ conference papers, 150+ keynote addresses, six U.S. patents, and fifteen books as well as technology transfer of the research to commercial products and operational systems.

extremists on social media because these events can be proven false and quickly forgotten by the public. Still, plausible threats to health and environment have a lasting impact.

Humans have survived thousands of years by learning and adapting to avoid threats to life and limb. Therefore, cyber-attacks that trigger fears of threats to public health and personal life have a massive initial impact and lasting effects which influence general perception and policy.

One such example is the Three Mile Island accident, which created significant public turbulence and fear and still profoundly impacted how we envision nuclear power. For a covert state actor that seeks to cripple society, embarrass the political leadership, and project to the world that we cannot defend ourselves, environmental damages are inviting.[5] An attack on the environment feels to the general public more close and scary than a dozen servers malfunctioning in a server park. It is tangible and quickly becomes personable and relatable, beyond what politically incendiary memes and social media storms can create.

We are all dependent on clean drinking water and non-toxic air. Cyber-attacks on these fundamentals for life could create panic and desperation in the general public–even if the reacting citizens were not directly affected.[6]

The last decade's study of cyber has left the environmental risk posed by cyber-controlled networks unaddressed.[7] The focus on cybersecurity has included providing for restoration of information systems by incorporating detection, protection, and reactive capabilities. From information security's early inception in the 1980s to today's secured environments, we have become skilled in our ability to secure and harden information systems. The interest in critical infrastructure is to a high degree concerned with accessibility, dependence, and availability, that the systems are working, and restoring their working condition after an attack. However, the long-lasting impact of threats to human health or the immediate environment drives sentiment and affects policy more seriously than a temporary loss of service. Environmental effects such as contamination of drinking water, degradation of ecosystem's functionality, toxic agents released, and flooding with massive soil erosion arising would be dramatic and long-term. Environmental damages and threats to our immediate environment are tangible and highly visible, as problems like flooding, loss of drinkable water, pandemics, biological hazards, mudslides, toxic air, and chemical spills directly affect the population and its surrounding environment. A failed computer server park does not drive media attention, nor can a few hundred tweets create such an impact on the public sentiment as a hundred thousand dead fish floating down a river because of an environmental cyber-attack. The environmental impact is visible, connects with people on a visceral level, and generates a notion that human existence is in jeopardy. Humans put survival first.

Environmental damages trigger radical shifts in the public mind and general sentiment. For a minor state actor, such as an adversarial developing nation, these attacks can be conducted with a limited budget and resources while still creating significant political turbulence and loss of confidence by a targeted major state actor's population. Conflict and potential war, as mentioned, seek to change policy and influence another nation to take steps that it earlier was unwilling to take. The widespread anxiety and stress that can follow environmental damages is a political force worth recognizing, which COVID-19 has evidenced. Systematic cyber-attacks that threaten public health will likely generate influence with enough momentum to change national policy.

LOSS OF LEGITIMACY AND AUTHORITY

Successful covert cyber-attacks that lead to environmental impact are troublesome for the government–the specific damage to systems and the challenge to legitimacy, authority, and confidence in the government and political leadership. The citizens expect the state to protect them. The protection of the citizenry is one of the core elements in the concept of a democratic government. The security of citizens is a part of the unwritten social contract between citizens and their government. The federal government's ability to protect is taken for granted. If the government fails to protect and safeguard its citizens, its legitimacy is challenged. Legitimacy concerns not who can lead, but who can govern. A failure to protect is an inability to govern the nation, and legitimacy is eroded. Institutional stability can be affected, which destabilizes the nation. The political scientist Dwight Waldo believed that we need faith in government; for the government to have strong legitimacy, it has to project, deliver, and promise that life is better for its citizens. In a democracy, the voters need a sense that they are represented, the government works for their best interests, and the government will improve the quality of life for its citizens. In the *Administrative State*, Waldo defined his vision of the "good life" as the best possible life for the population that can be achieved based on time, technology, and resources.[8] Authority is the ability to implement policy.

Environmental hazards that lead to loss of life and a dramatic long-term decrease in quality of life for citizens trigger a demand for the government to act. If the population questions the government's ability to protect and safeguard it, the government's legitimacy and authority will suffer. In the Three Mile Island accident, the event impacted sentiment and risk perception, even decades after the incident, of how citizens perceived the government's nuclear policies and ability to ensure that nuclear power was safe.

President Carter needed to demonstrate the ability to handle the incident and restore the general public's confidence in government policies. Environmental risks tend to appeal to the general public's logic and emotions, especially uncertainty and fear, and a population that fears the future has instantly lost confidence in the government.

The difference between the Three Mile Island accident and cyber-attacks on infrastructure that create environmental damage is that, during the Three Mile Island accident millions of Americans had a real fear for their life and future when faced with the possibility of a nuclear meltdown. Cyber-attacks on our national infrastructure that threaten public health cannot be predicted or potentially contained. These attacks can be massive if they exploit a shared vulnerability. Consequently, the fear generated by Three Mile Island could, in retrospect, have been marginal in comparison to the fear caused by a large-scale cyber-attack on national infrastructure.

ENVIRONMENTAL CYBER DEFENSE

Defending US infrastructure from cyber-attacks is not only protecting information, network availability, and the global information grid. It is also safeguarding public health and the environment, which affect the citizens' lives, their health, and their immediate living environment. The COVID-19 epidemic demonstrated the magnitude of impact attacks on the immediate environment. The citizenry's quality of life directly affects the confidence the population has in the government's ability to govern. From a rogue and unethical adversary's perspective, this represents an "opportunity" that the US needs to address by increasing the environmental cyber defense and clarifying the intersection between public health and cyber.

DISCLAIMER

The views expressed herein are those of the authors and do not reflect the official policy or position of the Army Cyber Institute, the United States Military Academy, the Department of the Army, the Department of Defense, the U.S. Fish and Wildlife Service, or the Department of the Interior.

NOTES

1. Scott R. Baker, Nicholas Bloom, Steven J. Davis, Kyle J. Kost, Marco C. Sammon, and Tasaneeya Viratyosin, "The unprecedented stock market impact of COVID-19," No. w26945, *National Bureau of Economic Research*, 2020.
2. Abbie Llewelyn, "Chernobyl: How Gorbachev claimed disaster was real reason behind the Soviet Union's collapse," *The Express,* June 6, 2019, https://www.express.co.uk/news/world/1137086/chernobyl-hbo-series-sky-atlantic-nuclear-disaster-gorbachev-soviet-union-spt.
3. FBI, 2020, "Safeguarding Your Vote: A Joint Message on Election Security." *FBI*, last modified 8 October 2020, https://www.fbi.gov/video-repository/interagency-election-security-psa-100520.mp4/view.
4. Kenneth N. Waltz, "Nuclear Myths and Political Realities," *American Political Science Review*, (1990), 731-745.
5. Jan Kallberg and Rosemary A. Burk, "Failed Cyberdefense: The Environmental Consequences of Hostile Acts," *Military Review* 94, no. 3 (2014): 22.
6. Jan Kallberg and Rosemary A. Burk (2013), *Cyber Defense as Environmental Protection—The Broader Potential Impact of Failed Defensive Counter Cyber Operations in Conflict and Cooperation in Cyberspace-The Challenge to National Security in Cyberspace*, Edited by P.A. Yannakogeorgos and Adam Lowther, (New York: Taylor & Francis, 2013).
7. Idaho National Laboratory, 2005. US-CERT Control Systems Security Center, Cyber Incidents Involving Control Systems, INL/EXT-05-00671.
8. Dwight Waldo, *The Enterprise of Public Administration*, (Novato, CA: Chandler & Sharp, 1980).