Empowering Food and Agriculture to Respond as Critical Infrastructures to COVID-19 and Future Pandemics

Part 4: Gray Zones, Black Swans and Gray Rhinos – Preparing for Disruption

February 2021

This publication is part of a partnership between Auburn University's McCrary Institute and Air University pursuant to which challenges related to cyber and critical infrastructure security are examined for the purpose of advancing U.S. national security.

ABOUT US

McCrary Institute

The McCrary Institute, based in Auburn with additional centers in Washington DC and Huntsville, seeks practical solutions to pressing challenges in the areas of cyber and critical infrastructure security. Through its three hubs, the institute offers end-to-end capability – policy, technology, research and education – on all things cyber.

Air University, based at Maxwell Air Force Base, Alabama, is the intellectual and leadership center of the U.S. Air Force, providing full-spectrum education, research and outreach, through professional military education, professional continuing education and academic degree granting.

AUTHORS

R. A. Norton, Ph.D.

Professor, Veterinary Infectious Diseases, Biosecurity and Public Health, Department of Poultry Science, Auburn University
Faculty Fellow, McCrary Institute, Auburn University

S. P. Rodning, DVM

Associate Professor and Extension Veterinarian, Department of Animal Sciences and the Alabama Cooperative Extension System, Auburn University

D.J. Collier

Senior Intelligence Officer, LeMay Center for Doctrine Development and Education, Air University Intelligence Directorate

P.H. Nelson, M.D., Col, USAF, MC, CFS

Department of International Security Studies, Air War College, Former Surgeon General's Chair to Air University

N. Simmons

National Security and Disaster Planning and Response Researcher

E. Monu, Ph.D.

Assistant Professor, Food Safety, Department of Poultry Science, Auburn University

D.V. Bourassa, Ph.D.

Assistant Professor and Extension Specialist, Department of Poultry Science, Auburn University

J.T. Sawyer, Ph.D.

Associate Professor, Meat Science, Department of Animal Sciences, Auburn University

PART FOUR

The pandemic caused by the coronavirus called SARS-CoV-2, known as COVID-19, has dramatically damaged the world economy and changed global commerce. This series of manuscripts has analyzed the threats that were manifested to agriculture. The authors believe that agriculture and food can be used as a model for other Critical Infrastructures (CIs) that will experience disruptions in the future. Even as the U.S. struggles with COVID-19 as a persistent problem (public health; economic), the other national security related struggles have not abated. China continues to pursue its circumvention of U.S. intellectual property and patent rights. It continues to erode national sovereignty in places like Hong Kong, and escalates challenges to the norms and rules of international diplomacy and free navigation in the South China Sea.

COVID-19 is, in a very real sense, the proverbial canary in the coal mine. Things are not right in the world, or more precisely the world is made more aware that things are not right. COVID-19 continues to erode our economic power, necessary for finding solutions. Perception has on a scale never before seen become reality on the global stage of social media. Insight is possible, but made less likely because of ever circulating disinformation and misinformation, whether COVID-19 or some spin-off political intrigue. If not righted soon, the lack of fact will continue to cause profoundly negative social and economic effects, as decision makers and the public alike are misled into error. We as a nation must learn from both our triumphs and mistakes. By doing so, we can better plan, but more importantly better act toward the next challenge that is sure to come our way.

One Last Look at China

China in many ways remains largely uncooperative as the world tries to determine how this pandemic happened. If internal investigations have determined the specifics on the index case, China has not shared the level of detail required for a thorough and independent analysis. Although, there were rumors that the SARS-CoV-2 virus might have been a biological weapon released either intentionally or unintentionally, publicly available data does not support that hypothesis at this time. Other rumors have circulated alleging that release of a naturally occurring virus might have resulted from an accident in a high-security microbiological laboratory in Wuhan, China. Although the hypothesis is plausible, given documented biosecurity problems with the facility in the past, the rumor remains unproven in either direction – yes or no - largely again because the Chinese Communist Party (CCP) has not allowed a rigorous external scientific enquiry from the Global Public Health Community (GPHC).

Given the paucity of data, the authors of this work remain undecided on the events surrounding the index case(s). The lack of validated information is more than a serious gap in the epidemiology. Getting this information therefore remains as the highest global priority

requirement. If left undetermined, this lack of knowledge may well impede the world's response to the next pandemic. We see this gap as an Intelligence problem that must be remedied. Medical intelligence was both lacking and stovepiped. It may or may not have been available to the highest levels of the federal government, but was certainly not available to decision makers at the state or local level or in business. As we have witnessed decision makers at these level also need validated information. Collection and right interpretation of global health data is critical, but so also is dissemination of that information. Public health is an important national security element for right decision making and therefore must be made available to all that need it.

Future Challenges to National Security

While America possesses the most powerful (and expensive) military on earth, the SARS-CoV-2 outbreak demonstrated that it is not equipped to fully respond to a truly disruptive agent. We live in a hyperlinked and connected world, which as it expands and evolves necessitates the redefinition of America's security perimeter. In one sense the SARS-CoV-2 was the natural world's equivalent to the 9-11 hijackers, which also did not respect sovereign constraint and arrived unexpectedly (in that case intentionally) through more primitive global connections. Both disruptors (manmade and non-manmade) arrived via air transportation. Future disruptors and future adversaries will not necessarily be confined to that physical constraint. Pandemics will still be confined to the physical world (people, places, objects, etc.), since that is their nature, but other types of thinking adversaries (nation state, non-nation state) are capable of causing disruption at the speed of electrons.

Adversaries have certainly observed the vulnerabilities seen currently and can be expected to leverage them in any future asymmetric challenge to America, either in limited operations less than total war (i.e. gray zone), or total (whole of society) fusion warfare. Protecting the American population and infrastructures in a "Survive to Operate" (STO) model will be an exceedingly difficult series of tasks, but could serve as one of several potential effective deterrence strategies. This approach could also help frame both expected and unexpected changes across this nation's critical infrastructures.

Critical Infrastructures

Critical Infrastructures (CIs) are not isolated systems, but instead complex Systems of Systems (SOS), which interconnect not just to each other internally, but also externally as one CI touches the next. The food supply is inextricably reliant on agriculture –each a gigantic and highly complex SOS in its own right. As CIs, each is interconnected to the chemical, commercial facilities, communications, dams, energy, financial services, transportation and water and wastewater sectors, etc. This interconnectivity makes possible our modern society and robust economy, but it also provides potential attack vectors, whereby a targeted CI can experience a rapid series of failures due to failures which started elsewhere. In time of war, it should be expected that an attack on one CI domain will rapidly become an attack on all.

Future War

War does not have to be inevitable, but history proves that it often comes when we are least prepared. How we prepare to fight the wars of the future will define us and future generations of Americans. Those choices may also determine whether our nation remains sovereign. In two world wars, the U.S. has proven our nation's military is very good and will ultimately prevail when we are able to define and execute the type of war that we prefer to fight. In the past, the security perimeter provided by the Atlantic and Pacific Oceans allowed us to trade distance for time, which allowed us to prepare, pick and choose the nature of the conflict in which we successfully engaged. We no longer have this luxury.

These kinds of global conflicts are now our nation's ancient history. The world does not fight these same kinds of all-encompassing wars any more, as illustrated by subsequent conflicts, including the Korean War, Vietnam, Iraq, and Afghanistan and a host of smaller conflicts. Now, our nation prefers to not even use the term "war," although this semantic distinction must seem irrelevant to those in the throes of conflict.

The enemy now has an equal say in initiating conflict, but also the timing and schedule of battle. Even the least equipped adversary now has connectivity with our nation and the globe, enabling them to choose the cyber realm as the most effective attack vector. The U.S. prefers to go into wars with technological supremacy, and have for centuries. Those days are also rapidly disappearing as Near-Peer-Nations (NPNs) inch closer to our technological capabilities, both on the battlefield and off. Some new way of fighting the enemy is badly needed.

At the start of many wars, the U.S. has initially assumed that each fight would be much like the last, where technological advantage, mass and speed assures victory. And yet, history frequently proves otherwise. The march to Baghdad during Desert Storm and the accompanying air campaign were brilliant and magnificent examples of technological superiority dominating the military of a weakened nation state (Iraq). Then something happened. The enemy chose to continue to fight in a very different way, causing the advantages of technology, mass and speed to be lost. The same problems emerged after the U.S. invaded Afghanistan. In these conflicts, early and overwhelming victories did not annihilate the enemy, who instead chose the long fight of economic, political and social attrition.

Our enemies now know we will no longer fight their conflicts in the same way we fought the two world wars. Annihilation is no longer a strategy or tactic. There will be no strategic bombings, and no breaking the will of the enemy to fight by wholesale destruction of military and civilian infrastructure or cities. Our war today is a very different war, and our military has very different Rules of Engagement (ROE) than it did, even early on in Iraq and Afghanistan. War now is constrained. We do not comment here on the appropriateness of these changes; that is left to the civilian and military decision makers and strategists. We only make note of

these changes to point out that during a future war, if (when) we will face an adversary or adversaries (working in concert), who may not impose those same constraints upon themselves. Future war – the time, the place, the strategies and tactics of attack will next time be chosen by the enemy. How we plan and how fast and in what way we respond will largely determine whether we will prevail, and at what cost to our society and economy.

Collective Survive to Operate (STO): A Mindset to Move Forward

As a nation we can learn from applying the military Joint Operational and Force Protection concepts of "Survive to Operate" to critical infrastructures. Current military doctrine emphasizes "joint" operations, with six critical interlinked domains being Air, Land, Sea, Sub-Sea, Space and Cyber. Interestingly, one senior military leader recently proposed that infectious pathogens could represent an emerging seventh domain based upon the recent experiences with COVID-19.

Each of these domains is interrelated, and a total failure in one domain would negatively impact all of the other domains as well as their mission of not only surviving but operating together. For example, a degraded military Space or Cyber environment could wreak havoc on Air, Army, Navy or Marine forces. Since much of our military supply chain depends on easy transport in uncontested global commons, total loss of Air or Sea power would negatively impact the other domains. Our military systems are built with resiliency and redundancy to prevent total failure of any domain, and those portions of the system that are truly single point failures are hardened to prevent critical failures.

Because many of our critical infrastructures are privately held and built for profit, they may lack the redundancy that can prevent critical failures. For example, early in the pandemic we saw intensive care hospitals, normally operating at or near capacity with normal patient through-put, in failure mode when a majority of their intensive care capacity was shifted to care for COVID patients. This lack of redundancy makes the CIs fundamentally different than a military system, where significant attrition is expected and planned for. Addressing this lack of redundancy is a limitation of our ability to "Survive to Operate."

The other challenge we face in adopting this mindset is the resistance of the American public, especially the general public, to assume risk to accomplish a job or mission. Military units and their commanders (in both wartime and peacetime) assume a certain level of risk to their personnel and units to achieve operational (or training) objectives. This risk is mitigated through intelligence-based defensive systems and actions, but some level of risk to personnel and unit is unavoidable and acceptable as part of being in the military. Military members are trained on the unit systems and operations, personal equipment, and individual actions that will mitigate this risk and give them confidence to operate in dangerous and complex environments, and "Survive to Operate."

On the other hand, our civilian workers who populate the CIs represent a significant vulnerability if not assuming this mindset. With a few acknowledged exceptions (for example,

the Emergency Services CI, including first responders such as police and fire) most civilians do not go to work thinking that they face a risk to their lives or the lives of their loved ones at home. This pandemic has changed the perception, starting certainly with our medical workers, but expanding into all workers who are deemed "critical."

Front line workers, whether transit operators, sales clerks or meat processers, now justifiably feel vulnerable in ways that few Americans have felt in a sustained way in recent memory. The lack of PPE for health care workers early in the pandemic was a clear reminder to all about how unprepared we were, and how individuals were assuming significant personal risk to keep our society functioning. Ensuring the organizational commitment to protect these workers, and ensuring that they are properly trained and equipped, will be critical to sustaining the CIs. Only then do workers have confidence to return to work, and allow the infrastructures to "Survive to Operate."

Decision Making Based on Faulty Information Increases Risk

Government and business in the best of times experience information overload. During COVID-19, the information tide became a tsunami, filled with the debris of correct and vetted information, but also wrong and un-vetted rumor and opinion. "Fact" and "data" were often touted in the mainstream media, when both were either missing all together or, at best, incomplete. Critical analysis often lags behind the 24/7 news cycle, so health officials and decision makers alike often chose expediency rather than waiting for proven facts. Decision makers were also often influenced in a variety of ways by connectivity to the media. Although the goal of "flattening the curve" was noble, the medical operational realities on the ground versus the varied and sometimes hyperbolic opinions from subject matter experts (SMEs) caused confusion and led in part to wrong decision making (e.g. sick elderly sent back to nursing homes). Opinion presented as fact fed into a proclivity toward groupthink.

Wrong decision-making also spread the medical effects into the realm of the economy and larger society, making clear that the effects of a pandemic were and continue to be greater than the sum of the parts. Total lockdown ("stay at home") made sense in the early days, but then the realities of the economic collapse and surge in psycho-social effects started to take hold. Drug and alcohol abuse soared, as did depression and other psychological effects. Spousal abuse also soared. Children's educational progress was disrupted. Businesses failed. Social disruption was massive. In the midst of this chaos, some intrepid decision-makers began to ask questions about how this evolving disruption could be better managed, and local solutions began to emerge. If one preeminent lesson emerged, it was one many already knew - local solutions are often best solutions. Local solutions that worked best, were those based on facts and validated data.

Intelligence Needs

This group considers accurate (scientifically based facts) and consistent messaging (bereft of politics) as essential to the public health in the midst of this and future pandemics. Public health is a national security issue. Put differently, properly aggregated, vetted and analyzed public health information (or what is called in the national security realm "Intelligence") is sorely needed. Inconsistency in messaging, or messaging based on inaccurate information, both seem to this group as very dangerous in the midst of any crisis likely to emerge in the future.

The Office of the Director of National Intelligence[1] defines "Intelligence" as,

> "…information gathered within or outside the U.S. that involves **threats to our nation**, its people, property, or interests; development, proliferation, or use of weapons of mass destruction; **and any other matter bearing on the U.S. national or homeland security.** Intelligence can provide insights not available elsewhere that warn of potential threats and opportunities, assess probable outcomes of proposed policy options, provide leadership profiles on foreign officials, and inform official travelers of counterintelligence and security threats."[2] (emphasis added)

The very broad brush used in refining the meaning of "information" and "…threats to our nation…"should be noted. In essence, what the U.S. refers to as Intelligence is anything that would be used for producing insight. Information related to public health is sometimes referred to as "Medical Intelligence," but doesn't have to be limited solely to that specific tradecraft. Other types of intelligence may also be useful to provide insight that has public health applications. There is an overarching process used by the Intelligence Community (IC): "The intelligence cycle is a process of collecting information and developing it into intelligence for use by IC customers. The steps in the process are direction, collection, processing, exploitation, and dissemination."[3] The result of these products are "products." These go to decision makers.

Factual information is critical to decision makers, whether in government or business. To be of value, it has to be free of political spin or hidden agendas. Agenda-driven information makes very poor-quality Intelligence. Wrong information or wrongly nuanced information makes more likely poor decision-making. Ambiguity is a constant reality, even in the best of circumstances. To an Intelligence professional, there is always a desire for more information. To a decision-maker, the information is needed now. A delicate balance between the two needs must be struck. "Timely

[1] Website: https://www.dni.gov/index.php.
[2] Office of the Director of National Intelligence (ODNI). "What is Intelligence?" Link: https://www.dni.gov/index.php/what-we-do/what-is-intelligence.
[3] IBID.

information," called by some "actionable information," is always the goal. In times of major disruption, timely information can mean the difference of success, perhaps even survival, versus disaster and defeat.

As has been mentioned in previous articles in this series, many CIs have established Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs). These are supposed to act as the bridge between government and business. Also, as noted, agriculture and the food industry lack such an organization, but instead uses a structure called the Food and Agriculture Sector Committee, which is sponsored by the U.S Department of Agriculture and the Food and Drug Administration. This somewhat informal organization holds biannual meetings (including a classified session for those business officials with clearances), relays information to companies via emails and provides access to some "For Official Use Only" (FOUO) documents, otherwise not available to business. Although helpful in providing some background, the information falls short of the "Intelligence Standard" (IS), meaning vetted and analyzed information that gives value (insight) to decision makers, which can then develop a "Course of Action" (COA) or "Courses of Action" (COAs), meaning a variety of decision options.

There are many necessary legal impediments that preclude government officials from sharing information with business. Foremost is the need to protect "sources and methods," The U.S. gathers Intelligence using a variety of methods, and these methods must be protected so that the adversary cannot develop strategies making gathering that information more difficult for the U.S. Exposing "sources and methods" might also reveal the identity of individuals within adversarial governments or organizations who have cooperated with the U.S. in gathering information. That can and often does cost lives.

Beyond this, Intelligence sharing between government and business is made more difficult by the very nature of business today. Business is increasingly multinational. Although a given CI might be based solely in the U.S., the corporations involved might touch suppliers or other partners that are not. Many nations like China invest wherever possible in corporations based in the United States. Any company associated with China, wittingly or unwittingly, touches the Chinese government and military. What China cannot buy to serve their Intelligence needs, China steals by a variety of means, including espionage. China is not alone in their goal of increasing connectivity to multinational corporations. A safe assumption with any multinational corporation is to expect that nations involved in those enterprises are gathering Intelligence.

Since timely or actionable Intelligence remains a priority for many corporations, and given the problems with government sharing, the most expedient solution is to duplicate the same processes of information gathering, vetting and analysis, but apply it solely internal to the company. This is Business Intelligence (BI). Many companies

already do it, but far more do not. BI can and should bolster resiliency. If it isn't, then the BI needs to be quickly modified.

How does BI work? Done right, it facilitates development of COAs, giving options to decision makers and providing warnings on those things deleterious to the business that may be encountered in the future. BI is a highly sensitive process, the tradecraft of which may be as important as that carried out by the government.

Remember what was said about multinational corporations. Many touch foreign nations, which in a high percentage of cases means foreign governments, which means foreign Intelligence. Many foreign countries are largely benign and only competitive in the economic sense, while others are potential adversaries. Any company in a consortium of companies has to remain aware of the ramifications of sharing information. Work-around strategies and TTPs can be developed, but every company should first guard carefully any information about itself that could potentially be exploited by others, whether governments or business competitors.

Recommended Actions

The following list is a starting point to enhance America's ability to "Survive to Operate."

1) This group of authors strongly advocates a thorough and non-partisan review of the federal, state, local and business responses to COVID-19 through the formation of a bipartisan blue-ribbon commission of experts, drawing from federal, state and local agencies, business, academia and medicine, as well as representatives from faith and civic organizations.
2) Develop and execute at scale through a "Whole of Society" "Survive to Operate" strategy, that bridges research, implementation, and funding across all sectors of society, including government, defense, civil society, academia, business, faith and civic organizations.
3) Prioritize and incentivize investments in public-private partnerships, given that most of our infrastructure sectors are dual use (military and civil society).
4) Develop a robust Medical Intelligence Infrastructure (MII) at the agency level within the Department of Homeland Security, using a model similar to that of the Cybersecurity and Infrastructure Security Agency (CISA). This new sub-agency will develop and prioritize requirements, coordinate medical and public-health-related intelligence across the IC and U.S. public health sectors and disseminate findings on a timely basis to state and local public health agencies and business.
    a. This new agency should further be charged with coordinating all civilian and military public health intelligence functions with CISA in order to prioritize protection of U.S. Critical Infrastructures.
    b. Special attention should be paid to the rapid lateral communication of critical findings across the whole of society (government, business and general citizenry).

c. Most importantly, this agency should serve an integrative function that crosses all societal boundaries and leverages, not replace work being conducted by international, federal, state and local partners.
d. The agency also should provide appropriate interagency coordination with the Department of Defense.
e. To expedite the stand-up and integration of this new capability, we recommend that this capability be embedded within DHS state fusion centers to facilitate appropriate information dissemination at the state and local government levels. The authors do not advocate a model whereby a new stand-alone IC agency is created.

5) Engage in a robust policy debate with constitutional scholars and civil society to pre-determine appropriate responses and decision trigger formulas, collectively necessary for better protecting the citizenry and U.S. economy in the next pandemic.