SECURITY NEXUS
A free, open access, international, peer-reviewed, online publication for the Daniel K. Inouye Asia-Pacific Center for Security Studies faculty and alumni.
apcss.org/nexus

Security Nexus Perspectives

THE INTERSECTION OF GLOBAL HEALTH, MILITARY MEDICAL INTELLIGENCE, AND NATIONAL SECURITY IN THE MANAGEMENT OF TRANSBOUNDARY HAZARDS AND OUTBREAKS

By Michael S. Baker, M.D. - Rear Admiral, USN (ret)

Dr. Sebastian Kevany[1]

Dr. Deon Canyon[2]

Jacob Baker[3]

Introduction

The COVID-19 pandemic-induced, shocking collapse of national and international trade, air travel, and tourism have rocked the world, and brought into stark relief the need for better health and disease surveillance. We have witnessed the global economy brought to its knees by the rapid spread of infection, resulting in widespread illness and many deaths. The rise in nationalism and isolationism, political use of the blame game, along with locked-down peoples chafing against shelter-in-place, work, or travel restrictions, have caused further divisiveness.

U.S. national security disasters, like Pearl Harbor and 9/11, led to significant overhauls of U.S. intelligence in an effort to prevent future surprises. Hopefully, governments with the resources and capacity will now make a greater commitment to funding and staffing their health systems, develop new medical intelligence tools to pursue enhanced disease intelligence efforts, and enhance vigilance to ensure they are never again caught by surprise by a major epidemic or pandemic crisis.

Health and disease intelligence are a central part of U.S. national security, along with other specialties, such as counterterrorism, counterespionage, and cybersecurity, and may often overlap with them. These security areas of expertise intersect, and those involved must work collaboratively. This is particularly true in the case of a future national security catastrophe deriving from either spontaneous or deliberate spread

[1] University of California, San Francisco
[2] Daniel K. Inouye Asia-Pacific Center for Security Studies, Honolulu
[3] Georgetown University

of hazardous or infectious agents. As health and politics become increasingly and inexorably intertwined, the risk of "cross-contamination" across previously-distinct professional and disciplinary areas increases exponentially. Associations between world politics, global health initiatives, and clandestine organizations such as the Central Intelligence Agency (CIA) have never before been so much in the public eye. State and non-state actors have simultaneously taken advantage of the geopolitical fallout and institutional weaknesses caused by the current viral pandemic to conduct terrorism, spy probes, disinformation campaigns, and cyberattacks. Even the likelihood of them using human delivery agents to spread vectors in target areas is a possibility.

In a future hypothetical situation where there is little or no functioning diplomacy or supranational collaborative effort amongst nations, the links between infectious disease control and containment strategies are inevitably strained. Much like investors in global markets, nation-states seek information to mitigate risk and reduce threats. Politics and strategies play out on domestic and international audiences as sovereign countries decide what they are able and willing to share, particularly regarding pandemic and epidemic information.

National security requires that we continue to enhance our medical intelligence work and add new tools to mitigate emerging threats. The intersection of global health assessment, military and civilian intelligence gathering, and national security needs is currently pushing the envelope of privacy and already imposing limits on personal liberties. New electronic hardware and software tools are being brought to bear in surveillance and tracking. While there has been some comment on how this is intruding on personal privacy, many nations see the benefits of information outweighing the social costs and are moving ahead in this area.

Disease surveillance and early warning

There are several approaches to hazard or outbreak surveillance and early warning. Traditional civilian multinational monitoring of cases, as well as government-sponsored and military intelligence agencies, need to lead ever more strongly and decisively in this area. First, we need scientific and medically astute eyes and ears around the world in areas subject to zoonotic diseases. We should also rapidly and broadly deploy the latest electronic tools to enhance our early detection and warning systems. Third, all collaborating countries need to be onboard by adopting a standard framework for transparent data sharing to facilitate early reporting.

Classical data sources for health intelligence include clinical reports, notifiable disease reporting, lab reports, pathology results, registries, and death records. Health intelligence originates at the local level, usually as clinical information. Clinical cases are identified and samples from patients are tested in the laboratory to identify the hazard or pathogen. Once a red flag has been triggered, epidemiologic investigation to determine source of infection and additional exposures, is carried out in parallel and, together with further laboratory investigations.

"Syndromic surveillance" is the use of clinical symptoms as criteria for reporting. This means the inclusion of non-clinical data collected from automated non-diagnostic systems such as pharmacy records,

ambulance call categories, personnel absences, or emergency department (ED) chief complaints. While individual symptoms may not be indicative of a particular disease, the detection of a cluster of symptoms, or syndrome, can be used to trigger early warning systems.

In this context, it is widely agreed that the key to recognizing and managing an effective response to a pandemic is early detection and early response. The infection rate and mode of transmission are crucially important since they can render a pandemic uncontrollable regardless of early warning. In the current pandemic crisis, the existing early warning apparatus worked as planned to some extent, but was inhibited by the current state of surveillance tools, a lack of transparency, a lack of international cooperation, delays in reporting and lab confirmation, disinformation campaigns, and counterfeit equipment and drugs.

We are in an era with more potential resources and useful tools than ever before including rapid global communication, electronic monitoring of health data, advanced tracking systems, and rapid molecular diagnostics. The increasing number of COVID-19 infections, and their rapid global spread emphasize the importance of early detection, but also reveal, in some countries and states, humanity's complacency or even outright reluctance in responding to clear signals of danger.

In recent years we have seen outbreaks of SARS, Ebola, and H5N1, which have been instructive in preparing for the present crisis. Yet many nations did not adequately prepare for this fight or proactively respond with their full capability as quickly as needed to mitigate public harm. We need to deploy the newest high-tech tools, along with additional resources in conjunction with the enhancement of our intelligence-gathering agencies, to provide a better early warning and response system and apparatus. We need to supplement that with educating national leaders, state governors and other decision-makers about what these warnings mean and what possible consequences might require an urgent response.

The history and current role of U.S. military medical intelligence gathering

The intersection of medicine, intelligence, and national security dates to the lead up of World War II. Alarmed by the rise of militarism and expansionism in Europe and Japan in the late 1930s, intelligence elements in the Federal Bureau of Investigation and the Departments of State, War, and Navy, stepped up collection of information.

In 1947, after World War II, the Central Intelligence Agency was established and began producing medical intelligence reports focused on Communist Bloc capabilities and trends, while the U.S. Army Medical Intelligence and Information Agency (USAMIIA) handled the related military medical intelligence program. In 1982, USAMIIA was renamed the "Armed Forces Medical Intelligence Center" (AFMIC), and was mandated to prepare intelligence assessments and forecasts on foreign military and civilian medical systems, infectious disease and environmental health risks, and biomedical research. These reports informed military planners and national security policymakers on both health risks and foreign health-care capabilities before deploying U.S. forces overseas.

In 2006, AFMIC expanded its support to homeland security by providing intelligence assessments in areas of biological terrorism, biological warfare, counterterrorism, and counterproliferation. Two years later,

AFMIC was designated the "National Center for Medical Intelligence" (NCMI) to reflect the organization's wider audience in which now included the White House, Department of State, Homeland Security, other domestic customers, and foreign partners. Today, NCMI serves as the lead U.S. Department of Defense (DOD) agency for the production of medical intelligence, responsible for coordinating and preparing "integrated, all-source intelligence" for the DOD and other government and international organizations on "foreign health threats and other medical issues to protect U.S. interests worldwide." NCMI provides: a) timely warning and projection of significant infectious disease and environmental health risks to U.S. personnel abroad and within the United States; b) analysis of foreign developments in life science technology and countermeasure development; c) analysis on health trends, foreign health diplomacy, military and civilian health system capabilities; d) biosafety and biosecurity policies; and e) biomedical and environmental related assessments "that are critical to military force and homeland health security protection."

As demonstrated during the 2003 SARS outbreak, the 2009 influenza pandemic, the outbreaks of multi-drug resistant tuberculosis, and now COVID-19, infectious diseases are not constrained by international borders. Outbreaks, whether linked to lab accidents, bioterrorism or from zoonotic causes, can spread rapidly across the globe, with significant adverse impact on economic and social stability. The value of NCMI in this context has been demonstrated repeatedly. In April 2009, two months before the World Health Organization (WHO) and the U.S. Centers for Disease Control and Prevention (CDC) officially declared the global outbreak of H1N1 influenza to be a pandemic, the NCMI published an intelligence product for senior U.S. policymakers that predicted H1N1 would be a transboundary global issue.

China experienced an outbreak of severe acute respiratory syndrome (SARS) caused by a coronavirus in November 2002 (if not earlier), but did not begin reporting it until February 2003, by which time the government listed 305 cases. Even as the virus spread, Chinese officials continued to undercount cases and delay reporting to WHO. Their attempt to conceal and downplay the outbreak highlighted the importance of having our own medical intelligence surveillance and analysis. Alas, the lesson learned was not acted upon.

The U.S. intelligence community and NMCI began to warn about a global epidemic in November 2019, saying that the Corona Virus outbreak in China could develop into a "cataclysmic event," and policymakers, decision-makers, and the National Security Council at the White House were repeatedly briefed on the issue. In early January, mention of the novel coronavirus outbreak first appeared in the President's Daily Brief (PDB) of intelligence matters that is placed on the president's desk every morning.

In this current pandemic, government intelligence agencies and military medical intelligence gatherers were well ahead of the curve in raising the alarm of this growing threat. But early response was sorely lacking, but neither adequate resources were gathered, nor modern tracking tools brought to bear by U.S. government and agencies.

Evolving tools for health threat surveillance and early warning

THE INTERSECTION OF GLOBAL HEALTH, MILITARY MEDICAL INTELLIGENCE, AND NATIONAL SECURITY IN THE MANAGEMENT OF TRANSBOUNDARY HAZARDS AND OUTBREAKS

A wide array of intelligence sources are engaged to identify and prevent the spread of infection as part of the U.S. surveillance and monitoring of disease. These include information and reports gathered by intelligence agencies, ally nations, and international health groups. It is necessary for intelligence and medical fields to be open, transparent, and collaborative on important developments in international disease outbreaks. While some of the data is available to the public, the bulk of it requires professionals in analytics and research to search the many data sources for specific points of interest. Classic intelligence tools for this include human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signatures intelligence (MASINT), social media intelligence (SOCMINT), and open source intelligence (OSINT).

Open Source Intelligence (OSINT) is defined by the DOD National Defense Authorization Act for Fiscal Year 2006 as 'produced from publicly available information'. This is a broad definition of any openly available source, and includes media sources that can be accessed instantly, with potential use in outbreak alerts. OSINT is currently in use globally and forms the foundation of many public intelligence capabilities. The public health community has begun to recognize the scope of these services, and many projects explore how OSINT can help identify and monitor emerging disease threats that may constitute a Public Health Emergency of International Concern (PHEIC).

Government of Canada (Health Canada), in collaboration with the WHO, operate the Global Public Health Intelligence Network (GPHIN), a program set up in the late 1990's that assists in the collection and assessment of OSINT in disease intelligence via a network of professionals who rapidly detect, identify, assess, prevent and mitigate threats to human health. GPHIN is a crucial part of a larger platform developed by the WHO, the Hazard Detection and Risk Assessment System (HDRAS), which uses web-based epidemic intelligence tools and collects information from Healthmap and the Program for Monitoring Emerging Diseases (ProMED), amongst others. Healthmap uses informal online sources for disease outbreak monitoring and real-time surveillance of emerging public health threats, including the mobile app "Outbreaks Near Me." Relatedly, the ProMED is a program of the International Society for Infectious Diseases (ISID) that was launched in 1994 as an Internet service to identify unusual health events related to emerging and re-emerging infectious diseases and toxins affecting humans, animals, and plants.

OSINT tools applied to health surveillance, such as GPHIN, automatically collect and collate data, thereby evaluating much larger quantities of information with algorithms and producing relevant reports. GPHIN, ProMED, and HealthMap have provided alerts on some of the most serious outbreaks since the turn of the century. For example, despite its earlier experiences with SARS, China did not report a November 2003 human H5N1 influenza case until 2006. By evaluating content from Chinese media and low-level chatter, ProMED provided the first English language alert of SARS and even 'prompted' subsequent confirmation by the Chinese government. Similarly, some indicators of the recent Ebola outbreak were detected by HealthMap before any official announcement because of its ability to scan news stories in the local language.

Social Media Intelligence (SOCMINT) is a subsector of OSINT that uses social media and web forums to provide contemporaneous information on a specified topic or theme. The geographic availability of

SOCMINT is limited, but this is improving as mobile data coverage in all regions is growing exponentially, especially among younger generations. The most popular services accessed through mobile data are sites, such as Facebook, has the potential to deliver more raw health information directly to the public than traditional publishing sources.

Signals Intelligence (SIGINT) is an intelligence technique that is less commonly used in infectious disease surveillance, but it may provide the best early warning system. It involves the collection of communication data through interception of telephone conversations and emails and can survey internet metadata and location data. Due to the sensitive legal nature of SIGINT, data collection is often only undertaken by national intelligence agencies and law enforcement, who may either target specific individuals or analyze big data. Programs such as the U.S. National Security Agency's PRISM and X-Keyscore, or the British Government Communications Headquarters (GCHQ) Tempora, can collect communications data on a mass scale through the interception of data through internet servers, satellites, fiber-optic cables, telephone systems and personal computers.

Digital Disease Detection (DDD), also known as digital disease surveillance, is used extensively in epidemiology. It is particularly useful in time series analysis for the investigation of the period preceding the outbreak, for assessing public sentiment regarding the perceived impact of a disease, and for determining the proportionality of government or health service response.

Other initiatives have attempted to demonstrate the potential of search-term surveillance. This technique exploits data on searches made by members of the public to compile trend data based on keywords. Most significantly, in 2008 Google launched Google Flu Trends (GFT), an attempt to aggregate data, based on the volume of public searches for keywords related to influenza, and use it to predict when an outbreak might occur. The principle behind this was that when people are ill with an influenza-like illness (ILI), they search for keywords relating to treatment and symptoms. Unfortunately, while GFT results corresponded well for some time with ILINet (CDC's surveillance program for ILI), it deviated spectacularly and completely missed the flu season in 2013 by 140%.

Another option fortunately exists. Cell phone data provided by technology companies can show how people move in their communities and throughout the world. When this data is paired with other metrics, such as the number of new infections or death rates, it can guide policymakers on when and where to implement measures, such as social distancing. This data can be used to trace the movements of people infected with the virus, and those with whom they come in to contact. Singapore has kept the rate of COVID-19 low at least in part through cell phone contact tracing.

Designed specifically for high-volume, high-velocity location data, Tectonix mapped cell phones from workers in meatpacking plants, known to harbor high infection rates. By visualizing billions of data points in near real-time, they tracked workers from a COVID-19-affected meat packing plant and were able to show phones traveling from the pandemic hot zone to 48 states over a 30-day period. This information facilitated rapid situational analysis, evaluation, and prompt response.

In this context, the Republic of Korea's strategy of targeted testing and aggressive contact tracing has been referenced as a successful example of how to contain the virus even as other countries have been slow to adopt it. The tools deployed by Korean authorities are readily available in other technologically advanced countries. But what sets Korea apart, is the political willingness to use these tools to their full potential in supporting a public health response.

Resistance to early detection and surveillance systems

While some agencies know that military and intelligence agencies conduct disease surveillance and have information to share, most are unaware of this and how to access the data. Some agencies, particularly those with a history of not working with the military, dismiss or deride these data sources because they constitute a form of 'Big Brother' surveillance. To many, the loss of personal freedom and discretion is, not just in libertarian eyes, a means of social control equitable to authoritarianism politics or command economies. It is perhaps only with the specific targeting of health or epidemic issues in emergency contexts, much as the 2001 Patriot Act transcended many related issues, that such systems can be more beneficial than oppressive.

The opposite is a completely libertarian and laissez-faire society in which personal surveillance is non-existent, and in which disease, infections and epidemics can spread in much the same way the Black Death or other plagues of the European middle ages raged. Nonetheless, the balance between respecting personal privacy and collecting actionable surveillance is an extremely hard one to get right, even in public health emergencies. One solution is to ensure that all data acquired by surveillance is immediately anonymized and made available to the public, thereby better informing local understanding of disease presence, control and response at the community level.

Two important ethical issues arise in the above regard. Firstly, concerns of individual infringements of privacy through surveillance can only be overcome if the information is immediately made public. Data is harvested from the individual and then returned, in benign fashion, to the community in the form of detailed geographical and demographic data related to disease transmission. SIGINT can be used in contact tracing and is now a reality.32-34 Expanding existing data collection programs to include targeted global health priorities would thus provide alerts for human operators to analyze and validate, which adds to vital early warning and response capability. Second, clear legal boundaries are required for any mandate to expand personal surveillance efforts to ensure that non-health communications and associated freedom of speech are not compromised.

Intelligence services also have an expanded role in fighting emergent outbreaks by uncovering state secrets. U.S. intelligence likely provides Washington policymakers with unique information, unavailable from any other source, about foreign state secrets concerning the virus, including whether official government infection rates are accurate. Given that diseases are transboundary in nature, these secrets are particularly important to discover in nontransparent, closed regimes like China, Russia, Iran, and North Korea. China concealed the extent of its initial viral outbreak, according to U.S. intelligence assessments. Russia had suspiciously low official levels of COVID-19 infections during the first wave of global outbreak,

but has now imposed draconian lockdowns. Clearly a better view of real events can be had by having one's own intelligence resources evaluating the target.

The crucial importance of medical intelligence gathering in national defense

Pandemic response requires early detection and early response, which is not possible without collaborative efforts with worldwide agencies such as the WHO, the cooperation of numerous countries and professionals, and special relationships, even with countries traditionally adversarial. Health Intelligence and disease surveillance are important early warning tools that strengthen decision-making capability and national security. But to accomplish this, our intelligence agencies need funding and staffing at a level that matches the demands of this national and global tragedy. 21st Century Global Health Intelligence is an increasingly important part of national intelligence gathering and national security, and requires a greater share of the resources committed to conventional warfare. Put simply, these new 21st Century threats require us to transition from building tanks and manned aircraft to deploying soft-power approaches, developing cutting edge cyber capabilities, and fast and efficient laboratories.

The development of truly effective global systems for managing infectious disease surveillance and health intelligence is challenging, but new tools are emerging. The goal for the immediate future is to have a vision that incorporates what we know has worked. We know, for example, that if they are well-resourced and supported, the Centers for Disease Control and Prevention and the National Center for Medical Intelligence are effective lead agencies.

Lead disaster-health agencies must collaborate, to the extent possible, with technologically astute intelligence-gathering agencies, using new tools that emerge in our high tech society, such as those following cell phone data for isolation and contact tracing. Our traditional tools of OSINT, SOCMINT, and SIGINT need to have at least part of their efforts focused on population health, disease surveillance, and the early detection of new threats. These techniques dominate today's news, but also open a door on new surveillance techniques that we urgently need as we fight successive waves of re-emerging and novel future pandemics. This is essentially a move from static to active data and mapping. The former techniques have been used by the military since leaders could draw map overlay updates, or push representative carved pieces across maps, but the latter, derived from active open source intelligence, allows for a real-time representation, that can be used in operational evaluation, response planning and decision-making.

Security and international relations at this time are evolving, yet one point does seem clear: it is only through the timely and detailed collection and sharing of disease outbreak and surveillance information between countries that pandemics can be contained or prevented. Building a wall or limiting travel is only going to delay the spread of disease. The earlier and more quickly surveillance notes a problem, the sooner alerts can be transmitted, the better the public health outcomes, and thus, the better the prospects for regional and international security and cooperation.

THE INTERSECTION OF GLOBAL HEALTH, MILITARY MEDICAL INTELLIGENCE, AND NATIONAL SECURITY IN THE MANAGEMENT OF TRANSBOUNDARY HAZARDS AND OUTBREAKS

The views expressed in these articles are those of the author and do not reflect the official policy or position of DKI APCSS, the U.S. Indo-Pacific Command, the U.S. Department of Defense, or the U.S. government.

June 2020