



apcss.org/nexus

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.

Security Nexus Perspectives

A BIODEFENSE FUSION CENTER TO IMPROVE DISEASE SURVEILLANCE AND EARLY WARNINGS TO ENHANCE NATIONAL SECURITY

By Michael Baker¹, Jacob Baker², Deon Canyon³, Sebastian Kevany³

ABSTRACT

Intelligence gathering that includes disease surveillance is an important early warning tool that strengthens decision-making capability and national security. U.S. military, medical assets, and intelligence agencies – and those of our allies are crucial for early detection and response in the future fights against emergent disease outbreaks.

It is time to establish a BioDefense Fusion Center. Our intelligence agencies, laboratories, civilian institutions, assets of our allies and partner nations, social media and data mining can be interwoven with technology and leveraged for mutual defense. The basic pillars of an early warning system are already in place and must be better funded and coordinated going forward.

Alliances, partnerships, and interconnectivity need to be improved and coordinated between the U.S. and foreign governments, independent social media data miners, and other assets that can support this mission. These efforts need increased funding and intensive collaboration efforts to weave their information into an international biodefense shield with our allied security partners.

BACKGROUND

Zoonotic transmission, lab accidents, or an intentional biowarfare event can trigger an outbreak, and disease can quickly spread globally - as we have recently seen with the COVID-19 pandemic. The [COVID-19 pandemic has also shown crucial U.S. national security vulnerabilities](#) and shortfalls in our response capability, and our adversaries have likely taken note.

¹ RADM, MC, USN (ret)

² Georgetown University

³ Daniel K. Inouye Asia-Pacific Center for Security Studies, Honolulu HI USA

The views expressed in this article are the author's alone, and do not necessarily reflect the official position of the DKI APCSS or the United States Government.

Military and civilian intelligence agencies that seek foreign source information developed from rapidly ramped-up efforts during World War II. The U.S. Central Intelligence Agency (CIA) was established in 1947 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. The latter evolved into the Armed Forces Medical Intelligence Agency (AFMIC), and later was designated [the National Center for Medical Intelligence \(NCMI\)](#) to reflect the organization's wider constituency which now includes the White House, Department of State, Homeland Security, other agencies, domestic customers, and international partners.

[NCMI also 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.”

Given that diseases are transboundary in nature, it is essential the U.S. has the ability to detect them before they reach American soil. The issue is that many closed nations, [like China, Russia, Iran,](#) and North Korea are not transparent about the medical issues that affect their nation and could affect ours especially a disease outbreak. Information about disease outbreaks such as transmissibility, genome data, and virulence statistics are crucial for combatting disease outbreaks but are characteristically difficult to obtain.

The value of these intelligence tools was evident in [November 2019 when the U.S. intelligence community and NMCI](#) began to warn about a global epidemic, saying that the Corona Virus outbreak in China could develop into a “cataclysmic event,” while policymakers, decision-makers, and the National Security Council at the White House were repeatedly briefed on the issue. In early January 2020, 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, therefore, government intelligence agencies and military medical intelligence gatherers were well ahead of the curve in raising the alarm on this growing threat.

FUTURE THREATS

For some time now, scientific advances have made possible the development of synthetic bioweapons (SBWs), which are weaponized biological vectors modified through synthetic biology for novel effects, mechanisms, or processes. [For example, CRISPR-Cas9](#) is a precise genetic surgery that has successfully cured diseases in human adults, but it can also be used to create SBWs. In addition, SBWs could enable a brand-new capability -- weapons that render threat detection difficult; have no conventional equivalent, and are harder to counter.

[PLA Colonels Qiao and Wang wrote in 1999](#) that China must be prepared to synchronize all government capabilities at all levels of competition, with all tools considered legitimate. Doctrinally, China has also recognized the critical role unconventional weapons might play, and some [Chinese thinkers have already rejected moral limits on SBWs.](#)

FORWARD LOOKING BIODEFENSE ASSETS

The U.S. military, in conjunction with its intelligence resources and a revitalized CDC (along with other global institutions), can provide the initial building blocks for an early warning and rapid response system woven into a national biodefense fusion center. The U.S. DOD has forward deployed bases, forces, labs, hospitals, intelligence assets, and surveillance resources, all of which are backed up by an agency that

has demonstrated success in early warning, testing, and response measures. In 1998, five different organizations within the Department of Defense (DoD) were brought together to create the [Defense Threat Reduction Agency \(DTRA\)](#) to better synchronize plans and actions for nuclear deterrence, weapons of mass destruction, and biothreats. DTRA quickly provided subject matter expertise, mobilized portable lab testing facilities, field vaccines, and treatments for the [Ebola Outbreak in West Africa](#).

The U.S. DOD's network of overseas laboratories perform research on infectious diseases of both public health and military importance. The [Department of Defense Global Emerging Infections Surveillance and Response System includes](#) the following agencies, several of which are World Health Organization (WHO) Collaborating Centers:

- [Armed Forces Research Institute of Medical Science \(AFRIMS\)](#), Thailand
- U.S. Army Medical Research Unit, Kenya
- [U.S. Naval Medical Research Unit \(NAMRU\)-3](#), Egypt (relocated to Italy)
- U.S. Naval Medical Research Unit (NAMRU)-2, Indonesia (relocated to Cambodia)
- Naval Medical Research Center Detachment (NMRCDC), Peru

When it comes to providing early warning of disease threats, these overseas military facilities form the basis for an effective international infectious disease surveillance effort, especially when collaborating with civilian health agencies such as WHO, other partner nations, and non-governmental disease outbreak search platforms.

BIOTHREAT COMMON OPERATING PICTURE

Notwithstanding conventional security threats, investment in military and civilian biodefense is critical. We must enhance threat awareness by developing a global Biothreat Common Operating Picture (BioCOP) in coordination with national and international defense, public health, homeland security, and intelligence agencies. Naturally, allied partners need to be part of the early warning and biodefense response; this will not work as a unilateral effort.

A BioCOP must be able to represent and characterize pandemic threats and possible new SBWs through active bio-surveillance in airports, seaports, and urban hubs. These agencies must be able to communicate, collaborate, and disseminate medical intelligence findings rapidly. Important assets that enable this are in place at this time include Open Source Intelligence Tools (OSINT) – widely used for health surveillance. These must be able to communicate and collaborate rapidly with international partners, agencies, and nations.

INTERNATIONAL OPEN SOURCE INTELLIGENCE TOOLS

The [Epidemic Intelligence from Open Sources](#) (EIOS) program is a collaboration between a wide range of public health stakeholders around the globe for early detection, verification, assessment, and communication of public health threats using publicly available information. EIOS is based on the Early Alerting and Reporting (EAR) project of the Global Health Security Initiative (GHSI), and the Hazard Detection and Risk Assessment System (HDRAS), as well as work with other global initiatives and projects such as [ProMED](#), the Global Public Health Intelligence Network, HealthMap and the Europe Media Monitor (EMM).

The [Global Public Health Intelligence Network](#) (GPHIN) is a web-based program that was set up in the late 1990s and utilizes a network of multinational and multilingual professionals who rapidly detect, identify, assess, 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.” [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 used for 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. Yet 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 announcements by officials or WHO. EIOS picked up the [first report of a cluster-type pneumonia outbreak in Wuhan at 03:14 am \(UTC\) on December 31, 2019](#).

FUTURE STEPS

The [United States National Security Strategy](#) (NSS) provides a framework for protecting the nation and ensuring its freedom, security, and prosperity in a rapidly changing, complex world. Consistently and innovatively translating the NSS blueprint into action remains a core function of government.

It is time for the U.S. to spearhead the development of a BioDefense Fusion Center. This initiative is urgently required to meet growing transboundary infectious threats to international security.

National biodefense must not be exclusively reactive. Further research needs to be undertaken by research organizations, such as the [Defense Advanced Research Projects Agency’s \(DARPA\)](#) biotechnology office. DARPA will need the resources -- more funding and personnel -- to drive the development of advanced biosensors, diagnostics, countermeasures, and other defenses to keep pace with changes in diseases. This has become even more urgent now that designer weapons can be created. Another asset is the [Defense Threat Reduction Agency](#) (DTRA), whose mission “enables DoD and the U.S. Government to prepare for and combat weapons of mass destruction and improvised threats” including those of biological origin.

A comprehensive counter-pandemic and counter-SBW plan would look for and respond to clear and present biological dangers while advancing the operating country’s knowledge about disease potential and emerging threats. The U.S. government must develop flexible, rapid, and effective response plans that include well-maintained stockpiles of specialized sensors, protective equipment, and medications. Defensively, we have also learned the challenges of responding with vaccines, even once the threat is identified, as we see in the current pandemic situation.

BIODEFENSE FUSION CENTER PARTNERS

The U.S. should advance disease surveillance, reporting, and early response with a BioDefense Fusion Center by leveraging its existing security relationships with regional allies and partners in a coordinated approach to improve domain awareness and intercommunication. Intelligence asset reporting, health and lab information, and social media and big data searches from a wide array of sources need to be collated, validated, and rapidly disseminated to provide biodefense.

Partner nations could help build a disease early warning system, as demonstrated by the Asia-Pacific countries that have a major stake in disease surveillance and early warning. These nations are already significantly aligned with the U.S. through organizations such as the [Daniel K. Inouye Asia-Pacific Center for Security Studies \(DKI-APCSS\)](#).

[The pillars of health surveillance and security can be quickly interconnected by leveraging the partner states of the Quadrilateral Security Dialogue \(the Quad\) – Australia, India, Japan, and the United States and the “Five Eyes” – Australia, New Zealand, Canada, Great Britain and the U.S. who currently share information. This can form the basic pillars of a BioDefense Shield as information is directed to the BioDefense Fusion Response Center. Proposals for national and international maritime fusion response centers are being considered to reduce transnational threats in the maritime domain.](#)

Potential partners in a more robust, international Biodefense Fusion Center and Shield alliance could include, Japan, Taiwan, South Korea, and Vietnam. Other partners could be found by bringing in India, Israel, and our NATO-European Union allies into a more global and comprehensive collaborative disease surveillance enterprise. Current events have demonstrated that such alliances are both proactive and successful at mitigating pandemic problems.

The next iteration of U.S. strategy must focus on key collaborative initiatives that collate and fuse data, both from intelligence sources, health assets, and social media web crawlers to tease out new or evolving threats to health and security. Drawing upon the strength and strategic alignment of existing relationships will only be effective with the facilitation of the rapid sharing of intelligence across platforms. Therefore, the U.S. approach needs to be innovative and ensure that critical instruments of alliance power are leveraged quickly to facilitate appropriate responses to health threats with adequate scope and focus.

CONCLUSION

21st Century global health intelligence is an increasingly important part of national security, strengthens national defense, and requires a greater share of the resources currently committed to conventional warfare. It also, through soft power and health security functions, protects national security both directly and indirectly.

Even in extremely challenging operational theaters such as Afghanistan, the use of medical [diplomacy initiatives through military Global Health Engagement](#) has been a highly compelling peacekeeping and nation-building tool. Medical and disease threat intelligence is thus vitally important to the safety and security of this nation and its people. Military, health departments and labs, and civilian intelligence agencies need funding and staffing beyond the level that has been seen in this current national and global pandemic tragedy.

Infectious diseases continue to evolve and disrupt nations around the globe at a faster pace. This process is exacerbated by demographic, political, and climate change pressures on populations that push humanity into habitats that were once wilderness or were considered unfit for living. Thus, our potential exposure to novel agents remains on the rise in line with population growth. The next pandemic may yet strike while we remain exposed due to [rapid, unsustainable urbanization, climate change, destructive food harvesting and producing practices, globalization](#), and reliance on other nations for essential items.

It is time to build a global Biodefense Fusion Center for early detection and early response to disease threats. This will promote U.S. primacy and leadership in global security and will provide the groundwork required for the establishment of a BioDefense shield. Our new 21st Century disease and security threats require us to transition from building tanks, ships, and manned aircraft for the “last war” to deploying better intelligence and surveillance tools; enhancing cutting edge cyber capabilities; and making our labs faster and

more efficient. We need to fund DARPA and DTRA, and link them together with civilian agencies, OSINT tools, and military intelligence assets. Strengthening our ability to defend against the next disease threat requires us to collaborate and [“war” game future threats](#) with allied nations and partners, and where possible, with civilian agencies such as WHO.

The development of truly effective global systems for managing infectious disease surveillance and health intelligence is challenging, but excellent tools and agencies are available, and new tools are constantly emerging. The goal for our future is to establish a global, collaborative surveillance and reporting mechanism, fund it generously, and staff it with our best talent. This is not a project that needs to be started from the ground up, for many of the assets needed and partnerships required to build a collaboration already exist. The United States just needs to be willing to grasp the baton, reframe military and security thinking and resource allocation in the health security context, and lead the next steps in global early warning and biodefense.

*The views expressed in this article are the author's alone, and do not necessarily reflect the official position of the DKI APCSS or the United States Government.
September 2021*