



Spies and the Virus: The COVID-19 Pandemic and Intelligence Communication in the United States

Ana Maria Lankford¹, Derrick Storzieri² and Joseph Fitsanakis^{3*}

¹ The COVID-19 Intelligence Project, Department of Politics, Coastal Carolina University, Conway, SC, United States, ² The Chanticleer Intelligence Brief, Intelligence and National Security Studies Program, Department of Politics, Coastal Carolina University, Conway, SC, United States, ³ Intelligence and National Security Studies Program, Department of Politics, Coastal Carolina University, Conway, SC, United States

OPEN ACCESS

Edited by:

Christian Alexander Vukasovich,
University of Southern Maine,
United States

Reviewed by:

Ganiu Oladega Okunnu,
Crescent University, Nigeria
Desiree Montenegro,
Long Beach City College,
United States

*Correspondence:

Joseph Fitsanakis
jfitsanak@coastal.edu

Specialty section:

This article was submitted to
Political Communication and Society,
a section of the journal
Frontiers in Communication

Received: 11 July 2020

Accepted: 06 November 2020

Published: 03 December 2020

Citation:

Lankford AM, Storzieri D and
Fitsanakis J (2020) Spies and the
Virus: The COVID-19 Pandemic and
Intelligence Communication in the
United States.
Front. Commun. 5:582245.
doi: 10.3389/fcomm.2020.582245

This paper introduces a crucial parameter to the novel coronavirus response in the United States, by shedding light on the early-warning role of intelligence agencies. It argues that the intelligence components of the federal government's Biological Defense Program offered actionable forewarning about an impending pandemic in the years leading to the COVID-19 outbreak. Yet, almost from the opening stages of the pandemic, senior US government officials, including President Donald Trump, have repeatedly claimed that the virus "came out of nowhere" and that "nobody saw it coming." We show that these assertions contradict more than 15 years of pandemic preparedness warnings by intelligence professionals, and disregard the existence of intelligence-led federal pandemic response strategies of every US administration in our time. However, rather than simply placing blame on the White House for discounting these warnings, we advance a conceptual analysis of what many in the US Intelligence Community view as a critical breakdown in strategic communication between intelligence professionals and key government decision-makers. This study agrees with those who suggest that the White House disregarded its own pandemic experts. However, it also posits that the means of strategic communication employed by intelligence experts to alert the White House to the threat were unproductive. These alerts were communicated largely through the President's Daily Brief, an archaic, and ineffectual method of communication that is not designed to facilitate the kind of laser-focused, unequivocal exchange of information needed when potentially catastrophic threats confront the world. This study suggests that the Intelligence Community must implement more direct, immediate and conclusive methods of communicating intelligence to decision-makers, and should seriously consider creating a new line of products that addresses existential challenges to national security. Lastly, we contend it is time to re-evaluate existing rules that prevent intelligence analysts from offering advice on policy. Although we agree that intelligence professionals should refrain from providing policy advice on routine

matters, we question the value of preventing these highly knowledgeable experts from communicating strategic policy advice to decision-makers when it comes to threats of a catastrophic nature, which may prove potentially existential for the US, its allies, and the world.

Keywords: biosecurity, biosurveillance, disease intelligence, warning intelligence, pandemic preparedness, intelligence dissemination, emergency management, crisis communication

INTRODUCTION

From the very onset of SARS-CoV-2 (also known as the novel coronavirus), United States President Donald Trump has led his senior administration officials in a chorus of statements claiming that the pandemic “came out of nowhere” (Trump, 2020a) and that “nobody saw it coming” (Trump, 2020b). The US President has repeatedly described the virus as an “invisible enemy,” which “snuck up on us” and which “nobody could have predicted” (Bump, 2020). Such statements have no basis in fact. A growing body of evidence demonstrates that the US Intelligence Community (IC) has been repeatedly warning policy- and decision-makers for well-over a decade about the potentially catastrophic effects of highly infectious respiratory viruses. In numerous reports, which date to at least 2004, the IC has cautioned US decision-makers of the impending human security threat of a global health pandemic. In these reports, IC analysts use stark language to warn that the United States lacks the capacity to contain a fast-spreading disease and stabilize the economy amidst an impending—not a possible—health pandemic (Miller P., 2020).

The Trump administration’s emphasis on the alleged lack of forewarning is likely part of a political strategy designed to shield the president and other senior officials from mounting criticism over the federal government’s slow response to the novel coronavirus outbreak. The administration did not begin taking moderate steps toward a nationwide response to the virus until 16 March, several weeks after leading epidemiologists began calling for the imposition of aggressive measures to combat the disease. The dramatic impact of the absence of early containment and mitigation in the US can be observed in a comparative data assessment of the US and two other leading industrialized countries, Japan and South Korea. On February 29, 2020, Japan (population 126 million) had recorded five deaths due to COVID-19—the disease caused by the novel coronavirus. On the same day, South Korea (population 51 million) had recorded 17 novel coronavirus-related deaths, while the US (population 328 million) had recorded a single death from the disease. By 5 July, Japan had recorded 977 deaths from COVID-19, which equated to 7.7 deaths per million people. South Korea had recorded 283 deaths, which equated to 5.5 deaths per million people. The United States had reached 132,318 deaths, or 403 deaths per million people (Johns Hopkins University, 2020). Epidemiological models produced in recent months show that “an estimated 90 percent of the cumulative deaths in the United States from COVID-19 [...] might have been prevented by putting social distancing policies into effect 2 weeks earlier, on March 2” (Jewell and Jewell, 2020). As research from Columbia

University shows, even if such measures had been put in place only a week earlier, on 9 March, the US could have seen “~60 percent reduction in deaths” nationwide (Kandula and Shaman, 2020).

In this paper, we review the warnings issued by the US IC in recent years, which challenge the Trump administration’s representation of the novel coronavirus as an unanticipated threat. We show that the administration’s claims contradict over 15 years of pandemic preparedness warnings, as well as federal response strategies implemented by three different US administrations, including President Trump’s own. These claims also contradict numerous IC reports that have guided the current and previous administrations’ pandemic preparedness plans. Yet, we do not place the blame for the substandard US response to the pandemic solely on the White House. Instead, we assess some of the lessons of the novel coronavirus pandemic for established models of strategic communication between the US intelligence and decision-making communities. This study suggests that, aside from flaws in US national preparedness for disease outbreaks, the experience of COVID-19 indicates a disastrous breakdown in strategic communication between the IC and US decision-makers. Additionally, we draw on lessons gained from the novel coronavirus experience to suggest methods of enhancing the efficiency of communication between the IC and US decision-makers.

BIOSURVEILLANCE AND DISEASE INTELLIGENCE FUNCTIONS OF THE US GOVERNMENT

In addition to posing major challenges in the areas of healthcare and public health, disease outbreaks can test the limits of national security doctrines. At the pandemic level, such outbreaks—whether naturally occurring or bioengineered—can quickly and irreversibly degrade complex economic systems by severing their production and distribution functions, and even severing demand for goods and services. In the words of former US Director of National Intelligence Dan Coats, disease outbreaks can lead to “major economic and societal disruptions” (Office of the Director of National Intelligence, 2018a), which, if left unchecked, can deliver mortal blows to the stability of states. It follows that the monitoring of disease outbreaks falls within the operational scope of the US IC, an amalgamation of 17 organizations, whose mission is to gather, analyze and disseminate intelligence to American policy- and decision-makers. Consumers of intelligence products use them

to inform their judgment in the course of pursuing sound and effective governance.

In the US, federal biosurveillance and biodefense tasks are diffused within an extremely wide spectrum, which is known as the US Biological Defense Program. It includes analytical units, such as the Department of Homeland Security's Chemical and Biological Defense Division. It also encompasses protection units, such as the Office of Preparedness and Response of the Department of Health and Human Services (DHHS). Importantly for this paper, it also features units that combine intelligence collection and analysis tasks, such as the Disease Intelligence Program of the Central Intelligence Agency's (CIA) Directorate of Science and Technology. The latter constitutes one of the earliest components of the US Biological Defense Program, with roots that date to the 1966 cerebrospinal meningitis outbreak in Beijing, China (Kawai, 2014). The outbreak prompted the Chinese government to shut down schools and implement a military takeover of the healthcare system. This prompted the CIA's Office of Scientific Intelligence to launch Project IMPACT, an effort to aggregate disease data in order to assess the political fallout of the disease (Carey and Maxfield, 1972). In 1968, when the Hong Kong/A2/68 influenza killed an estimated 4 million people, including around 100,000 Americans (Vuboud et al., 2005), Project IMPACT was merged with a grander effort, codenamed Project BLACKFLAG. Its goal was to “computerize disease information and derive trends, cycles and predictions” (Ferran, 2020) on a global scale. Through BLACKFLAG, the CIA was also able to warn its teams of operatives abroad, instructing them to shield themselves from the flu as it spread in East Asia and, eventually, the world (Ferran, 2020).

The CIA's early disease intelligence efforts showed that data aggregation was critical in helping monitor and forecast outbreaks at a quick pace. They also demonstrated the direct integration of such data with political, military and economic intelligence. Finally, they helped shape the 3-fold mission of disease intelligence, which remains fundamentally unchanged to this day, and is as follows: (a) collect intelligence about the extent and spread of diseases abroad, which may vary widely from data provided by official state sources; (b) forecast the consequences of these trends for American interests in the affected regions; and (c) provide policy- and decision-makers with the information they need to protect American lives and property from the effects of diseases. Since 1966, disease intelligence data have been disseminated to American decision- and policy-makers in a variety of formats and without interruption.

It is important to call attention to the fact that the mandate of the US IC does not include making policy decisions. These are left to elected or appointed decision-makers in the civilian and military realms. Thus, the role of intelligence analysts in the US Biological Defense Program ends once they disseminate the information that has been collected, analyzed and incorporated into finished intelligence products. Dissemination—i.e., the communication of finished intelligence products to the consumer—is a distinct phase of what is known as “the intelligence cycle”—a term that refers to the process that intelligence professionals utilize in order to effectively analyze

and communicate information collected in the field. Conceptual models of the intelligence cycle differ, but most versions consist of five phases: planning and direction; collection; processing; analysis and production; and dissemination [Johnston, 2005]. These steps are interchangeable, allowing for intelligence practitioners to begin at any phase of the intelligence cycle, or to revert to previous phases, in order to create effective intelligence products.

The intelligence cycle typically begins when an intelligence agency assigns tasks to its employees to carry out. This can be an independent action by an agency, or can result once it is tasked by decision-makers—referred to as “customers”—with providing a deliverable, whether that be information, or a physical piece of evidence that could be analyzed to produce effective, actionable intelligence. This process is referred to as Planning and Direction. The completion of this stage leads to the collection of raw data. Collection can be categorized as open-source, clandestine, and covert. Open-source collection utilizes unrestricted networks and officially released documents to obtain information. Clandestine collection involves engagement into secret collection efforts, which is broadly acknowledged by governments—since most governments generally admit to maintaining clandestine collection capabilities. This could involve the use of field agents in the form of diplomats or assets (spies) to collect data. Covert collection involves actions that are tasked by the government, but not sanctioned, so as to avert escalating conflict between nations if collection operations are detected. Consequently, this method of collection must include a high degree of deniability regarding the information collected and the methods used to collect it.

Upon successful collection, raw data enter the processing stage, which is sometimes referred to as “processing and exploitation.” Depending on the type of information collected, analysts may need to translate or decrypt the raw information into a form that helps synthesize analysis. Next, intelligence professionals turn the gathered raw data into actionable intelligence. During the analysis and production stage, analysts are tasked with evaluating the data, in an effort to assess developing trends and forecast future events. This process is time consuming, consisting of multiple possibilities being assessed per event, so as to consider all possible outcomes. Analytical assessments are then evaluated with statements of confidence and likelihood—terminology used by intelligence professionals to communicate the likelihood and credibility of sources and information—to aid in the dissemination of the product to the customer. One of the most important parts of this stage is the absence of bias or influence, since, as explained earlier, the task of intelligence analysts is to provide information, not to determine, or even advise toward, policy options. It follows that the customer, for example a senator, needs to be presented with unbiased information, as any bias, no matter how subtle, could potentially influence the outcome of the customer's overall decision.

Dissemination is arguably the most demanding and critical phase of the intelligence cycle. In the words of one expert, “this step can “make or break” the entire process” (Jensen et al., 2018). In this stage, the compiled and analyzed intelligence

product is communicated to the agencies or professionals that the information was analyzed for. In an effort to hamper espionage efforts by adversaries, in 2008 Director of National Intelligence Mike McConnell reinforced the policy of “responsibility to provide” (Brewin, 2008). This means that intelligence products are communicated only to those that are tasked with receiving the information. Dissemination also poses the risk of adversaries intercepting and exploiting finished intelligence products to further their own aims, making security a major priority at this stage. Finished intelligence products will be briefed to policy- or decision-makers in either a written or oral briefing. The importance or usefulness of the information is ultimately decided by the customer.

PANDEMIC-RELATED WARNINGS IN RECENT INTELLIGENCE PRODUCTS

The earliest known intelligence product that specifically describes a health pandemic similar to SARS-CoV-2 is contained in a 2004 estimative report from the National Intelligence Council (NIC). The NIC operates under the Office of the Director of National Intelligence (ODNI), which is the coordinating body of the US IC (Office of the Director of National Intelligence, 2018b). Its primary mission is to provide American policy- and decision-makers with long-term strategic analysis of existing and emerging threats. The NIC report, entitled *Mapping the Global Future*, offers a descriptive projection of security threats the world could face by 2020. It states that it is “only a matter of time before a new pandemic appears, such as the 1918–1919 influenza virus that killed an estimated 20 million worldwide” (United States National Intelligence Council, 2004a). That assessment was sparked by security concerns raised by the 2002 coronavirus Severe Acute Respiratory Syndrome (SARS) outbreak in China. The NIC reiterated its assessment in 2008, when it issued its *Global Trends 2025* report; it features an entire section discussing the possibility of a global pandemic. Notably, the section describes a now-familiar scenario, centering on “the emergence of a novel, highly transmissible, and virulent human respiratory illness for which there are no adequate countermeasures” (United States National Intelligence Council, 2004b). While the report sees such a pandemic as likely being caused by a pathogen like the Highly Pathogenic Asian Avian Influenza A (H5N1), it warns that “pathogens such as the SARS coronavirus or other influenza strains also have this potential” (United States National Intelligence Council, 2004b). The report also indicates that such an outbreak would likely originate in China, as it is a densely populated country where humans live in close quarters with livestock.

In 2012, amidst the outbreak of the Middle East Respiratory Syndrome (MERS), the NIC published *Global Trends 2035*. The report describes a global pandemic as a “black swan,” and states bleakly that

[a]n easily transmissible novel respiratory pathogen that kills or incapacitates more than one percent of its victims is among the most disruptive events possible. Such an outbreak could result in millions of people suffering and dying in every corner of the

world in less than six months (United States National Intelligence Council, 2012).

Expressed concerns of the threat of a global pandemic are not contained solely in NIC reports. On the contrary, similar warnings were communicated for over a decade via the *Worldwide Threat Assessment*. Known officially as the *Worldwide Threat Assessment of the US Intelligence Community*, this annual intelligence product provides a summary of current and emerging threats to US national security. It is produced annually for use by the US Senate Select Committee on Intelligence, which in turn makes it available to the White House. In its “Human Security” section, the 2013 edition of the report states that

humans will continue to be vulnerable to pandemics, most of which will probably originate in animals. An easily transmissible, novel respiratory pathogen that kills, or incapacitates more than one percent of its victims is among the most disruptive events possible. Such an outbreak would result in a global pandemic that causes suffering and death in every corner of the world, probably in fewer than six months (Office of the Director of National Intelligence, 2013).

This statement appears to forecast with remarkable accuracy the place of origin and mode of global transmission of SARS-CoV-2. Further on, the report employs stark language to caution policy-makers, stating that “[t]his is not a hypothetical threat. History is replete with examples of pathogens sweeping populations that lack immunity, causing political and economic upheaval, and influencing the outcomes of wars” (Office of the Director of National Intelligence, 2013). Similar threats were discussed in the 2015 edition of the *Worldwide Threat Assessment*, which states that “infectious diseases are among the foremost health security threats. A more crowded and interconnected world is increasing the opportunities for human and animal diseases to emerge and spread globally” (Office of the Director of National Intelligence, 2015). It is notable that the mounting concerns of the IC about a global pandemic were largely driven by the unparalleled growth of a globalized transportation infrastructure.

The annual *Worldwide Threat Assessment* reports have not only elaborated on the potential of a highly damaging health pandemic, but have also cautioned that the international community is not adequately prepared for such an event. This was noted in the 2016 assessment, which suggests that “the international community remains ill prepared to collectively coordinate and respond to disease threats” (Office of the Director of National Intelligence, 2016). Similar concerns were projected again in 2018, where we read about the possibility that a global health pandemic could lead to “a strain on governmental and international resources, and increase calls on the United States for support” (Office of the Director of National Intelligence, 2018a). The most recent *Worldwide Threat Assessment*, produced in 2019, specifically notes that current global health security regimes may not be sufficiently effective in the event of a global pandemic. The assessment includes the statement: “[a]lthough the international community has made tenuous improvements to global health security, these gains may be inadequate” (Office of the Director of National Intelligence, 2019).

In addition to the above strategic-intelligence products, which were made available to presidential administrations dating back to 2004, other elements of the US government have discussed repeatedly in recent years the potentially catastrophic effects of a global pandemic. In 2017, a Department of Defense pandemic and influenza response plan, which was drafted following the MERS coronavirus, stated that “the most likely significant pathogen threat is a novel respiratory disease, particularly a novel influenza disease” (United States Northern Command, 2017a). More recently, press reports have suggested that both the CIA and the Defense Intelligence Agency briefed senior officials in the Trump administration about the SARS-CoV-2 (Arciga, 2020). These briefings are believed to have taken place in early February, before the virus made its way into the US in a major way—though the question of whether the White House was briefed before COVID-19 arrived on American soil remains unanswered for the time being, given that the precise timing that the virus’ entry into the US is itself under debate (Arciga, 2020).

The intelligence products discussed above demonstrate a clearly discernible evolution in the language used by their authors to alert their customers. One can observe the terminology change from estimative and speculative in feel at first, to gradually formulating direct warnings about the catastrophic consequences of a pandemic. Overall, it is clear that these concerns grew substantially in the 15 years following 2004 and the publication of *Mapping the Global Future*. Furthermore, the evolution of the language in these reports provides strong evidence of a growing trajectory of apprehension among disease-intelligence experts. By 2018, these experts were openly sounding the alarm about the threat of a global pandemic caused by a respiratory virus.

Intelligence products disseminated in the early stages of that period tend to discuss the broader context of pandemic threats, such as their effects on globalization. For instance, in a section titled “The Contradiction of Globalization,” the National Intelligence Council’s 2004 report, *Mapping the Global Future*, highlights the rapid expansion of globalization due to Chinese and Indian economic liberalization, the collapse of the USSR, and the technological revolution of the information era. It argues that the rapid advancements in globalization could simultaneously hinder, and even reverse, the process if certain events, such as a pandemic, were to unfold. The report characteristically states that: “experts believe it is only a matter of time before a new pandemic appears, such as the 1918–1919 influenza virus that killed an estimated 20 million worldwide” (United States National Intelligence Council, 2004b). The analysts plainly articulate their greatest concerns regarding a pandemic, namely the human death toll and the adverse impact on the world economy. They also note that globalization would be threatened “if the death toll rose into the millions in several major countries and the spread of the disease put a halt to global travel and trade during an extended period” (United States National Intelligence Council, 2004b).

The context discussed in these earlier reports lays the foundation that successive *Worldwide Threat Assessment* releases stand on from 2008 onward. In sections titled “PLA Modernization,” and “Infectious Disease and US Security,” the 2008 report points to concerns about China’s “high incidence of chronic and infectious disease” (McConnell, 2008), and even

raises alarms about the United States’ insufficient response to prior disease outbreaks, such as the avian H5N1 (“swine flu”) virus. The 2009 edition of the *Worldwide Threat Assessment* expands upon the threat of a pandemic, by including a section titled “Global Health.” As late as 2014, a full decade following the initial warnings issued by the NIC, Director of National Intelligence James R. Clapper continued to insist that, if a novel respiratory pathogen that had the ability to kill or incapacitate more than 1 percent of its victims were to become easily transmissible, “the outcome would be among the most disruptive events possible” (Clapper, 2015).

In another notable instance, the ODNI’s 2017 *Worldwide Threat Assessment* explicitly notes that “a novel or reemerging microbe that is easily transmissible between humans remains a major threat because such an organism has the potential to spread rapidly and kill millions.” The 2018 edition of the report includes a similar statement about the next health pandemic, which can be described as a direct warning, rather than a precautionary comment. The warning explicitly mentions a strain of coronaviruses as potentially being responsible for causing the next health pandemic (Office of the Director of National Intelligence, 2018a). Shortly after that report was issued, the NSC’s director of medical and biodefense preparedness warned that the threat of a pandemic flu was the world’s foremost health security concern, something that the US was not prepared for (Sun, 2018).

Also in 2017, the Department of Defense’s US Northern Command Branch *Plan 3560: Pandemic Influence and Infectious Disease Response* was published, based on an earlier plan drafted in 2006. The document is in essence a policy draft that details the US military’s response to the causes of disease in humans. It describes in stark language how “a catastrophic biological incident could threaten the Nation’s human, animal, plant, environmental, and economic health, as well as America’s national security” (United States Northern Command, 2017b). The report goes into acute detail, discussing the strategic capabilities of the US military, a classification system for sorting the types of diseases and their methods of transmission, as well as the agencies responsible for the various stages of plans, establishing a chain of command in the event of an outbreak of “unique or novel pathogens” (United States Northern Command, 2017b).

In January of 2019, the ODNI’s *Worldwide Threat Assessment* again included a warning about the next global health pandemic, this time explicitly stating that the US remained extremely vulnerable to the next pandemic. In September of 2019, the President’s Council of Economic Advisors warned that the next pandemic would cause great economic damage and loss of life (Council of Economic Advisors, 2019). The following month, the DHHS concluded that the US biodefense infrastructure was underfunded, underprepared, undercoordinated, and generally incapable of combatting a flu-like pandemic as determined by a precautionary exercise (Sanger, 2019). Finally, between late November and early December of 2019, the Department of Defense’s National Center for Medical Intelligence warned of a rapidly spreading and novel virus in Wuhan, China (Margolin and Meek, 2020).

DISMISSAL AND INACTION BY THE TRUMP WHITE HOUSE

In 2018, on the day after the NSC's director of medical and biodefense preparedness warned about the threat of a pandemic flu and the US' lack of preparedness, he was removed from his position and was never replaced. In the same breath, the NSC disbanded its Global Health Security Team overnight. Only days following that development, two members of the House Committee on Foreign Affairs wrote a letter to the President's National Security Advisor, expressing concern that the recent actions of the NSC "downgraded the importance of health security in the US" (Connolly and Bera, 2018). These moves signaled major departures from the pandemic-related preparedness planning of prior administrations, including that of George W. Bush Jr., which was the first to develop a nationwide global health pandemic response plan (The White House, 2007). That plan was put in motion shortly after the NIC released its *Mapping the Global Future* report mentioned earlier, which explicitly discussed the threat of a global health pandemic. In November of 2005, President Bush delivered a speech on his plan, entitled "National Strategy for Pandemic Influenza Preparedness and Response" (The White House, 2007), in which he highlighted three key elements of that plan, which his administration saw as the most critical. The first element was the importance of bio-surveillance, which would ensure the early detection of viruses occurring anywhere in the world. The second element was the need to develop a national stockpile of critical virus-fighting vaccines and antiviral drugs, and to increase the nation's capability of developing new vaccines at faster rates. The third key element centered on the importance of pandemic preparedness at all levels of government, to include federal, state, and local (The White House, 2007).

To achieve these goals, in May of 2006 the Bush administration officially released its *National Strategy for Pandemic Influenza Implementation Plan*—a national security plan to combat the threat of a global health pandemic. In addition to that step, the Bush administration continued to fund the World Health Organization (WHO) Global Outbreak Alert and Response Network. It also invested in state and local government outbreak preparedness plans and developed a plan for dispersing critical medical resources in the event that they became scarce (The White House, 2007). In its reports, the Bush White House noted there were areas in pandemic preparedness that would continue to be in need in the coming years. Some of these areas included: strengthening US capabilities in clinical bio-surveillance, so as to better-detect outbreaks within the United States; strengthening medical capacity in order to properly care for and treat patients in the event of a pandemic; and continuing to work with international agencies like the WHO so as to properly prepare on a global scale for a health pandemic (The White House, 2007). These efforts by the Bush administration closely mirrored the critical developments proposed in relevant intelligence reports made available to the White House.

The major elements of the pandemic preparedness planning by the administration of President Barack Obama are highlighted in a cumulative report entitled *Playbook for Early Response to High-Consequence Emerging Infectious Disease Threats and Biological Incidents* (United States National Security Council, 2015). This report, better known as "The Pandemic Playbook," was produced by the National Security Council toward the end of the Obama administration, with the expressed purpose of passing on strategic pandemic preparedness knowledge to the incoming Trump administration (Knight, 2020). This publicly available document describes at length various pandemic preparedness procedures and includes a guide on how to assess public health threats, descriptions of how various pathogens originate and spread, and numerous charts to guide in risk assessments. It also highlights and describes the threat of a "novel coronavirus" similar to the current COVID-19 pandemic (Knight, 2020). The most pronounced distinction between the Bush and Obama administration's plans on pandemic preparedness is that the Obama administration's "Pandemic Playbook" focuses heavily on tracking a pathogen with pandemic potential before it poses an imminent threat to the United States—something that represents a clear enhancement of the previously available planning model. This appears to have been implemented in direct response to preparedness and containment shortcomings that the IC's *Worldwide Threat Assessment* indicated.

In 2017, just days after the inauguration of Donald Trump as the 45th president of the United States, officials from the Trump and Obama administrations participated in a pandemic preparedness exercise. The goal of the exercise was for the departing officials to inform their incoming counterparts of existing policies in the "Pandemic Playbook," which were designed to respond to a national health crisis. Most Trump administration officials who attended that exercise were no longer in office by the time of the outbreak of SARS-CoV-2 (Sun, 2018). Later that year, the Trump administration decided not to adopt the "Pandemic Playbook" created by Obama administration officials. Instead, it created its own pandemic preparedness plan, which is called the *Pandemic Influenza Plan* and is a product of the DHHS.

Shortly after developing its *Pandemic Influenza Plan*, the White House proposed a total of \$277 million in budget cuts affecting the government's pandemic preparedness program. The plan included cutting \$136 million from the Office of Public Health Preparedness and Response, \$65 million from the National Center for Emerging and Zoonotic Infectious Diseases, and \$76 million from the Centers of Disease Control and Prevention's (CDC) Center for Global Health (Baumgaertner, 2017). These cuts were rejected by Congress in May of 2017, but on February of next year the Trump administration did manage to withdraw \$1.25 billion in funding from the CDC's Public Health Fund (Sun, 2018). On April 10, 2018, President' Trump's newly hired National Security Advisor, John Bolton, dismissed the White House's Homeland Security Advisor, days after he had called for "a comprehensive biodefense strategy against biological attacks and pandemics" (Toosi et al., 2020). Budget cuts

continued in the coming year, with the White House proposing once again a budget cut of \$252 billion for global health. In May 2018, these efforts prompted a letter to the president from Senator Sherrod Brown, who expressed concern that cutting federal and global health and pandemic preparedness budgets could “cost American lives” (Goodman and Schulkin, 2020). In September of that year, on orders from the president, the DHHS diverted \$266 million from the CDC to the Unaccompanied Alien Children program, which provides housing for detained immigrant children (Goodman and Schulkin, 2020). That same month, the president announced the launch of a new “National Biodefense Strategy” and the creation of a Biodefense Coordination to “ensure a comprehensive and coordinate approach to biological incidents” (The White House, 2018). That strategy closely models the response plan implemented by the 2004 Bush administration, by highlighting the need for a well-stocked national stockpile of critical medical equipment, accelerating vaccine production capabilities, and increasing pathogen detection capabilities, specifically for influenza viruses (The White House, 2018). However, as we have seen, this plan failed to materialize in the critical early stages of the SARS-CoV-2 pandemic.

DISCUSSION: SARS-CoV-2 AND INTELLIGENCE COMMUNICATION

The actions of the Trump administration in the years leading to the novel coronavirus outbreak reveal a systematic demotion of pandemic preparedness at the level of national strategy. They also provide a telling context for the administration’s inaction in the early stages of the outbreak. It is therefore difficult—indeed impossible—to propose a forensic evaluation of America’s response to COVID-19 without placing a significant portion of the responsibility on the door of the White House. The question, however, remains, and is at the heart of the issue: why were the warnings of the IC not heeded by the president and his administration? We believe that this query can be addressed on multiple levels, including political, economic, and even cultural. At least one of them, however involves the role of the IC in protecting American national security, specifically through the dissemination of intelligence, which, as explained earlier, is arguably the most critical step of the intelligence cycle. Addressing this issue is vital for the future of American national security, because it points to the desperate need for efficient communication between the IC and the highest levels of government, especially on matters of critical importance to the safety of the nation.

It has become apparent to intelligence agencies that the communications revolution in our century has multiplied the channels of readily available information that are available to consumers of intelligence (Liaropoulos, 2006). As a result, US intelligence finds itself operating today in “an extraordinarily competitive environment,” in which it is “competing for business, and consumers” (Degaut, 2016). The latter are now increasingly questioning the value of intelligence products given to them, and constantly compare these products to a host of open-source channels of information, such as 24-h television news, as well as

Internet sites. This tendency has arguably seen its culmination with President Trump. According to insiders like Susan Gordon, until recently Principal Deputy Director of National Intelligence, the president is known to consistently confront his intelligence briefers with comments such as: “I don’t think that’s true” or “I’m not sure I believe that,” even when presented with conclusive evidence on a topic of concern (Gordon, 2019). This potentially points to a breakdown in communication between the IC and the president, during meetings that are often combative and cut short due to the president’s other obligations.

This growing problem is compounded by what former senior CIA Directorate of Intelligence officer Martin Petersen describes as “the most precious commodity in Washington”—not information, of which there is an abundance, “but time” (Petersen, 2011). Decision-makers understand the importance of being informed. However, their scarcity of time forces them to prioritize sources of information that offer easily digestible analyses with immediacy and certainty. This poses major challenges for authors of finished intelligence products, who tend to prioritize quality over speed. Unlike the raw information collected by intelligence agencies, finished intelligence products are meticulously analyzed so as to lessen the degree of uncertainty of a particular issue. Consequently, they rarely—if ever—present the reader with absolute answers to questions, which makes them appear inconclusive. It is therefore imperative that the IC places emphasis on the speed of communication between it and key consumers as a matter of policy. A major way of facilitating increased immediacy is by focusing less on “the incremental addition of new intelligence from human sources or technical sensors” (Hulnick, 2006) and more on already available data to answer questions. According to former CIA intelligence analyst Hulnick, such a methodology is realistic, given that existing data “is already so large that a competent analyst could write about most events without any more than open sources to spur the process” (Hulnick, 2006).

The time-constraint factor in intelligence communication is especially prevalent in interactions between the IC and the president. Since 1946, American presidents have been the main recipients of what has been described as “the finest intelligence publication in the world” (Wilder, 2011), namely the President’s Daily Brief (PDB). The PDB provides the president, and a small number of senior officials selected by the president, with snippets of current intelligence on pressing global developments. It is produced by the ODNI in coordination with the President’s Analytic Support Staff of the CIA Directorate of Analysis, and contains descriptive and estimative reports based on information provided by practically every agency in the IC. Reports in the press have stated that President Trump received information about the novel coronavirus through the PDB. According to these reports, successive PDBs “raised the prospect of dire political and economic consequences” with a frequency that “reflected a level of attention comparable to periods when analysts have been tracking active terrorism threats, overseas conflicts or other rapidly developing security issues” (Miller, G., 2020). However, the degree to which the PDB can be expected to deliver warning intelligence to the president is questionable. According to CIA analysts, the PDB is typically viewed by intelligence managers

and decision-makers alike as “educational in nature,” and “not [...] the kind of intelligence product used for warning” (Hulnick, 2006). Moreover, decision-makers often find it difficult to focus on the details contained in PDBs, due to their highly specific and technical nature. The latter contrasts with the abstract and strategic mode of thinking that presidents and other senior officials are accustomed to engage in. Consequently, it is often the case that the consumer of the PDB leaves the meeting without having retained the information that the briefer, as well as the authoring analysts, view as paramount (Wolfberg, 2014).

The unpredictability and arbitrariness of PDB encounters only increases when the consumer is someone like President Trump, who has admittedly limited experience in statecraft or intelligence matters. Trump’s background in these fields lacks in comparison to most prior presidents, including, for instance, George Bush Sr., a former ambassador, who also served as director of the CIA before entering the Oval Office. Even in the best of times, PDB meetings are awkward and involve “both briefer and policymaker [sitting] down in the same room, physically near each other, while the policymaker reads the written material” (Wolfberg, 2014). The consumer peruses the material “under the gaze of the briefer,” who is often reduced to “carefully [watching] the policymakers’ gestures, body language, and facial expressions,” following “the policymaker’s eyes, attempting to detect which sections the policymaker [is] spending the most amount of time on reading” and even paying “attention to the pattern the policymaker’s finger [makes] as he or she [views] each page of the briefing book” (Wolfberg, 2014). The awkwardness of this mostly silent exchange is compounded by the pressing schedule the consumer is under, which inevitably leads to “difficulty in absorbing all the material in the briefing book” during the relatively short PDB meeting. Inevitably, therefore, policymakers filter the information, “paying attention to some things, ignoring other things” (Wolfberg, 2014).

It should also be noted that, even though the PDB is delivered to the consumer in a written format, many presidents expect to be guided through the document orally by the briefer. President Trump has been repeatedly criticized in the press for allegedly having a “style of learning” that does not involve reading. The president is alleged to have eventually made it clear to his briefer that “he was not interested in reviewing a personal copy of the written intelligence report known as the PDB.” Instead, he has relied on exclusively “oral sessions,” according to administration officials (Leonnig, 2018). This has been seen as a radical—even alarming—departure from established practice, and must have been looked down upon by the IC, where the prevailing notion has always been that “policymakers who do not devote time on a regular basis to read intelligence reports [...] are clearly not doing their jobs” (Degaut, 2016). It is equally true, however, that “[t]he history of the PDB is one of flexibility and remarkable adaptation of support to fit each president’s needs and information acquisition styles” (Wilder, 2011). This statement, made by an IC insider, implies that it is the IC’s briefing conventions that must adapt to the consumer’s style of retaining and digesting the information, rather than the other way around. It also points to further communication breakdown between President Trump and his IC briefers—an unfortunate

state of affairs that may be at least partially responsible for the administration’s slow response to the novel coronavirus pandemic. We can thus infer that, as has been reported in the press, PDBs in November and December of 2019 made repeated mentions of COVID-19. By that time, however, the president was viewing the product as, in the words of former CIA analyst Martin Petersen, “optional equipment” (Petersen, 2011).

How can this problem be corrected? We believe that the PDB continues to be an efficient method for communicating current intelligence to the highest levels of government. However, as the COVID-19 experience shows, this mode of intelligence communication cannot serve as an effective warning mechanism. The same can be stated for the myriad of in-depth intelligence reports produced annually by the analytic components of the IC, such as *Global Trends* and the *Worldwide Threat Assessment*. As Hulnick has remarked, these intelligence products are “meant more for policy officials at working levels rather than senior decision makers, who rarely have the time to read them” (Hulnick, 2006). Like the PDB, these annual reports cannot be seen as replacing what the IC refers to as “deep dives,” namely in-depth presentations on pressing matters of concern that bring together decision-makers with the IC’s domain experts, rather than just trained briefers (Wolfberg, 2014). Such deep dives—30-min to an hour-long interactive sessions on specific topics of concern—must become more prevalent as a form of strategic communication between the IC and key customers. Moreover, we believe that the IC must give serious thought to the possibility of producing a separate version of the PDB that will focus strictly on warning intelligence—that is, critical information on topics that are not on the radar of decision-makers. This version of the PDB—let us call it the President’s Critical Brief, or PCB—does not need to be produced daily, though it should be disseminated at least weekly. Additionally, it should concentrate heavily on catastrophic and existential threats to national security, including threats by new and unfamiliar actors, large-scale biosecurity concerns, weapons of mass destruction, climate change indicators, and other similar topics.

Lastly, we propose a thorough reconsideration of the principle of preventing IC analysts from proposing policy options to decision-makers. As explained earlier, the line that divides the relaying of information from proposing policy options is engrained in the very operational modality of the US IC—though interestingly it is not a feature of intelligence work in other Western countries. However, the case of the novel coronavirus may point to the need to reconsider this division when it comes to topics that pose existential or otherwise catastrophic challenges to national security. As NSC analyst Dennis Wilder has astutely observed

increasingly today, policymakers and legislators find that the intelligence analysts’ adherence to this article of faith robs the policymaker of the ideas and suggestions for policy that a highly informed analyst can provide (Wilder, 2011).

The reasoning that informs this “article of faith,” as Wilder calls it, is a sound one—namely the need to preserve the intelligence analyst’s political objectivity and professional integrity, by

keeping them at arm's length from the policy domain. However, as Wilder notes, preventing an analytical expert from advising on policy—especially on threats of an existential nature—denies the policymaker “some of the most useful byproducts of analytic depth and sophistication” that the IC is known for Wilder (2011).

CONCLUSION: TOWARD AN EFFECTIVE MODEL OF INTELLIGENCE COMMUNICATION

The Trump administration is being untruthful when it portrays the novel coronavirus pandemic as a strategic surprise. Its assertions that COVID-19 “came out of nowhere” fly in the face of over 15 years of pandemic preparedness warnings by the IC. Moreover, such claims insult the intelligence professionals whose work has consistently informed the pandemic preparedness strategies of three presidential administrations, including President Trump's. Consequently, we believe that it is impossible to forensically evaluate the slow US response to the pandemic without placing much of the responsibility for it on the White House. It is equally impossible, however, to assess the inaction of the Trump administration without examining the deeper breakdown in strategic communication between key decision-makers and the IC. Indeed, the breakdown in communication between these two actors points to the urgent need to re-evaluate the standard methods of intelligence dissemination to the highest levels of government.

It is clear that, in the decade leading to 2020, the IC drew on over 70 years of experience in disease intelligence to warn policy- and decision-makers about the impending threat of a respiratory virus. These warnings became increasingly stark between 2014 and 2018, by which time IC experts were openly and directly sounding the alarm about what they correctly saw as an imminent threat. That the Trump administration downplayed pandemic preparedness as a matter of national policy is unquestionable. It is equally unquestionable, however, that the means of strategic communication employed by the IC to alert the White House to

the threat were unproductive. These alerts were communicated largely through the PDB, an archaic and ineffectual method of communication, which is not typically seen as an instrument of warning. The awkwardness, unpredictability, and randomness of PDB exchanges do not facilitate the kind of laser-focused, unequivocal exchange of information that is needed when potentially catastrophic threats are upon the nation. Instead, the IC must implement communication methods that favor more direct, immediate and conclusive intelligence dissemination, and should seriously consider the creation of a new line of products that address existential and potentially catastrophic challenges to national security. Lastly, we believe it is high time to reconsider the division between intelligence reporting and policy advising. We agree with the view that intelligence analysts should stay clear of providing policy advice during routine reporting to customers. However, we do not see the value of preventing highly knowledgeable and capable intelligence professionals from offering policy advice to decision-makers when it comes to threats that are considered catastrophic or potentially existential for the US and its people.

AUTHOR CONTRIBUTIONS

AL and DS assembled and compiled the data used in this article from a variety of declassified United States Government sources. AL provided the information regarding the responses of various administrations to the pandemic response documents produced by the United States Intelligence Community. DS authored the description of the intelligence cycle. JF provided the institutional context of the analysis and wrote the discussion of the findings, as well as the recommendations and conclusion. All authors contributed to the article and approved the submitted version.

ACKNOWLEDGMENTS

The authors would like to thank intelligence practitioners Rachel Panichella and Maeve Stewart for their advice on this paper.

REFERENCES

- Arciga, J. (2020). “US intelligence sounded coronavirus alarm in january: WaPo,” in *The Daily Beast*. Available online at: <https://www.thedailybeast.com/us-intelligence-agencies-reportedly-sounded-coronavirus-alarm-in-january> (accessed March 12, 2020).
- Baumgaertner, E. (2017). *Trump's Proposed Budget Cuts Trouble Bioterrorism Experts*. The New York Times. Available online at: <https://www.nytimes.com/2017/05/28/us/politics/biosecurity-trump-budget-defense.html> (accessed May 28, 2017).
- Brewin, B. (2008) *New Intelligence Sharing Strategy Shifts From 'Need to Share' to 'Responsibility to Provide'*. Government Executive. Available online at: <https://www.govexec.com/defense/2008/04/new-intelligence-sharing-strategy-shifts-from-need-to-share-to-responsibility-to-provide/26642/> (accessed April 04, 2020).
- Bump, P. (2020). “How trump's rhetoric on testing in the US compared with what was—or wasn't—being done”, in *The Washington Post*. Available online at: <https://www.washingtonpost.com/politics/2020/03/31/how-trumps-rhetoric-testing-us-compared-with-what-was-or-wasnt-being-done/> (accessed March 31, 2020).
- Carey, W. F., and Maxfield, M. (1972). Intelligence implications of disease. *Stud. Intell.* 16, 71–78.
- Clapper, J. (2015). *Worldwide Threat Assessment of the US Intelligence Community*. Washington, DC: Office of the Director of National Intelligence. Available online at: https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (accessed February 15, 2020).
- Connolly, G. E., and Bera, A. (2018). *Letter to National Security Advisor*. Available online at: https://connolly.house.gov/uploadedfiles/connolly_bera_letter_to_nsa_john_bolton_on_global_health_security.pdf (accessed May 15, 2018).
- Council of Economic Advisors (2019). “Mitigating the impact of pandemic influenza through vaccine innovation,” in *The White House* (United States Government). Available online at: <https://www.whitehouse.gov/wp-content/uploads/2019/09/Mitigating-the-Impact-of-Pandemic-Influenza-through-Vaccine-Innovation.pdf>
- Degaut, M. (2016). Spies and policymakers: intelligence in the information age. *Intell. Natl. Security* 31, 509–531. doi: 10.1080/02684527.2015.1017931
- Ferran, L. (2020). Project impact: disease intelligence and how the cia traced epidemics out of Cold War Asia. *ABC News*. Available online at: <https://>

- abcnews.go.com/Politics/project-impact-disease-intelligence-cia-traced-epidemics-cold/story?id=71299224 (accessed June 20, 2020).
- Goodman, R., and Schulkin, D. (2020). *Timeline of the Coronavirus Pandemic and US Response*. Available online at: <https://www.justsecurity.org/69650/timeline-of-the-coronavirus-pandemic-and-u-s-response/> (accessed May 07, 2020).
- Gordon, S. (2019). *Former Trump Administration Officials on National Security*. Washington, DC: Women's Foreign Policy Group. Available online at: <https://www.c-span.org/video/?466944-3/trump-administration-officials-national-security> (accessed December 3, 2019).
- Hulnick, A. S. (2006). What's wrong with the intelligence cycle. *Intell. Natl. Security* 21, 959–979. doi: 10.1080/02684520601046291
- Jensen, C., III, McElreath, D., and Graves, M. (2018) *Introduction to Intelligence Studies*. New York, NY: Routledge.
- Jewell, B. L., and Jewell, N. P. (2020). *The Huge Cost of Waiting to Contain the Pandemic*. The New York Times. Available online at: <https://www.nytimes.com/2020/04/14/opinion/covid-social-distancing.html> (accessed April 14, 2020).
- Johns Hopkins University (2020). *COVID-19 Global Map, Center for Systems Science and Engineering*. Baltimore, MD: Johns Hopkins University. Available online at: <https://coronavirus.jhu.edu/map.html>
- Johnston, R. (2005). *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*. Washington, NY: Central Intelligence Agency.
- Kandula, S., and Shaman, J. (2020). Differential effects of intervention timing on COVID-19 spread in the United States. *medRxiv*. doi: 10.1101/2020.05.15.20103655
- Kawai, F. (2014). Epidemic cerebrospinal meningitis during the cultural revolution. *Extrême-Orient Extrême-Occident*. 37. Available online at: <http://journals.openedition.org/extremeorient/341>
- Knight, V. (2020). *Evidence Shows Obama Team Left A Pandemic 'Game Plan' For Trump Administration*. Kaiser Health News. Available online at: <https://khn.org/news/evidence-shows-obama-team-left-a-pandemic-game-plan-for-trump-administration/> (accessed May 15, 2020).
- Leonnig, C. D. (2018). *Breaking With Tradition, Trump Skips President's Written Intelligence Report and Relies on Oral Briefings*. The Washington Post. Available online at: https://www.washingtonpost.com/politics/breaking-with-tradition-trump-skips-presidents-written-intelligence-report-for-oral-briefings/2018/02/09/b7ba569e-0c52-11e8-95a5-c396801049ef_story.html (accessed February 9, 2020).
- Liaropoulos, A. N. (2006). *A (R)evolution in Intelligence Affairs? In Search of a New Paradigm*. Research Paper No. 100. Athens: Research Institute for European and American Studies.
- Margolin, J., and Meek, J. G. (2020). *Intelligence Report Warned of Coronavirus Crisis as Early as November: Sources*. ABC News. Available online at: <https://abcnews.go.com/Politics/intelligence-report-warned-coronavirus-crisis-early-november-sources/story?id=70031273> (accessed April 08, 2020).
- McConnell, M. J. (2008). *Annual Threat Assessment of the Intelligence Community*. Washington, DC: Office of the Director of National Intelligence. Available online at: https://www.dni.gov/files/documents/Newsroom/Testimonies/20080227_testimony.pdf (accessed February 27, 2008).
- Miller, G. (2020). *President's Intelligence Briefing Book Repeatedly Cited Virus Threat*. Washington Post. Available online at: https://www.washingtonpost.com/national-security/presidents-intelligence-briefing-book-repeatedly-cited-virus-threat/2020/04/27/ca66949a-8885-11ea-ac8a-fe9b8088e101_story.html (accessed April 27, 2020).
- Miller, P. (2020). "How the intelligence community predicted COVID-19," in *The Dispatch*. Available online at: <https://thedispatch.com/p/how-the-intelligence-community-predicted>
- Office of the Director of National Intelligence (2013). *Worldwide Threat Assessment of the US Intelligence Community 2013*. Washington, DC: Office of the Director of National Intelligence. Available online at: <https://www.dni.gov/index.php/nctc-newsroom/nctc-speeches-testimonies-and-interviews/item/1707-2013-worldwide-threat-assessment-of-the-us-intelligence-community> (accessed March 12, 2013).
- Office of the Director of National Intelligence (2015). *Worldwide Threat Assessment of the US Intelligence Community 2015*. Washington, DC: Office of the Director of National Intelligence. Available online at: https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (accessed February 26, 2015).
- Office of the Director of National Intelligence (2016). *Worldwide Threat Assessment of the US Intelligence Community 2016*. Washington, DC: Office of the Director of National Intelligence. Available online at: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf (accessed February 09, 2016).
- Office of the Director of National Intelligence (2018a). *Worldwide Threat Assessment of the US Intelligence Community 2018, United States Office of the Director of National Intelligence*. Office of the Director of National Intelligence. Available online at: <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>
- Office of the Director of National Intelligence (2018b). *Worldwide Threat Assessment of the US Intelligence Community 2018*. Washington, DC: Office of the Director of National Intelligence. Available online at: <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf> (accessed February 13, 2018).
- Office of the Director of National Intelligence (2019). *Worldwide Threat Assessment of the US Intelligence Community 2019*. Washington, DC: Office of the Director of National Intelligence. Available online at: <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf> (accessed January 29, 2019).
- Petersen, M. (2011). What I learned in 40 years of doing intelligence analysis for US foreign policymakers. *Stud. Intelligence*. 55, 13–20.
- Sanger, D. (2019). *Before Virus Outbreak, a Cascade of Warnings Went Unheeded*. The New York Times. Available online at: <https://www.nytimes.com/2020/03/19/us/politics/trump-coronavirus-outbreak.html>
- Sun, L. H. (2018). "Top white house official in charge of pandemic response exits abruptly," in *The Washington Post*. Available online at: <https://www.washingtonpost.com/news/to-your-health/wp/2018/05/10/top-white-house-official-in-charge-of-pandemic-response-exits-abruptly/> (accessed May 10, 2020).
- The White House (2007). *Pandemic Flu: Preparing and Protecting against Avian Influenza, United States Government*. Available online at: <https://georgewbush-whitehouse.archives.gov/infocus/pandemicflu/> (accessed July 17, 2007).
- The White House (2018). *National Biodefense Strategy, United States Government*. Available online at: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf>
- Toosi, N., Lippman, D., and Diamond, D. (2020). *Before Trump's Inauguration, a Warning: 'The Worst Influenza Pandemic Since 1918'*. Politico. Available online at: <https://www.politico.com/news/2020/03/16/trump-inauguration-warning-scenario-pandemic-132797> (accessed March 03, 2020).
- Trump, D. (2020a). "Remarks at signing of the coronavirus preparedness and response supplemental appropriations act, 2020," in *The White House* (Washington: DC). Available online at: <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-signing-coronavirus-preparedness-response-supplemental-appropriations-act-2020/> (accessed March 06, 2020).
- Trump, D. (2020b). "Remarks in roundtable on border security," in *The White House* (Washington, DC). Available online at: <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-roundtable-border-security-yuma-az/> (accessed June 23, 2020).
- United States National Intelligence Council (2004a). *Mapping the Global Future*. Washington, DC: Office of the Director of National Intelligence. Available online at: https://www.dni.gov/files/documents/Global%20Trends_Mapping%20the%20Global%20Future%202020%20Project.pdf
- United States National Intelligence Council (2004b). *Global Trends 2025, Office of the Director of National Intelligence*. Washington, DC: United States National Intelligence Council. Available online at: https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf
- United States National Intelligence Council (2012). *Global Trends 2030, Office of the Director of National Intelligence*. Washington, DC: United States National Intelligence Council. Available online at: https://www.dni.gov/files/documents/GlobalTrends_2030.pdf
- United States National Security Council (2015) *Playbook for Early Response to High-Consequence Emerging Infectious Disease Threats and Biological Incidents*. Washington, DC: Office of the Director of National Intelligence.
- United States Northern Command (2017a). *Department of Defense Influenza/Pandemic Response Plan*. Colorado Springs, CO: Department

- of Defense, Peterson Air Force Base. Available online at: <https://www.scribd.com/document/454422848/Pentagon-Influenza-Response> (accessed January 06, 2017).
- United States Northern Command (2017b). *USNORTHCOM Branch Plan 3560: Pandemic Influenza and Infectious Disease Response*. Colorado Springs, CO: Department of Defense, Peterson Air Force Base. Available online at: <https://www.cenae.org/uploads/8/2/7/0/82706952/pentagon-influenza-response.pdf> (accessed January 06, 2017).
- Vuboud, C., Grais, R. F., Lafont, B. A. P., Miller, M. A., and Simonsen, L. (2005). Multinational impact of the 1968 Hong Kong influenza pandemic: evidence for a smoldering pandemic. *J. Infect. Dis.* 192, 233–248. doi: 10.1086/431150
- Wilder, D. C. (2011). An educated consumer is our best customer. *Stud. Intell.* 55, 23–31. doi: 10.1037/e741172011-003
- Wolfberg, A. (2014). Communication patterns between the briefer and the policymaker. *Int. J. Intell. Counterintell.* 27, 509–528. doi: 10.1080/08850607.2014.872534

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright © 2020 Lankford, Storzieri and Fitsanakis. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.