

ARTEFAKTUM



ARTEFAKTUM REPORT 04/2020

COVID-19 pandemic - an unprecedented
challenge to the intelligence community

March 17, 2020, Russell T. Vought, the acting head of the Office of Management and Budget, has issued a „MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES“, a strict guidance to federal agencies to slow the spread of the coronavirus. Most federal employees are now working from home, including some White House staffers. This report wants to estimate the impact to the U.S. intelligence community

The rapid spread of the coronavirus has sent a large number of federal workers home to telework, in some cases limiting government services, raising concerns that some of the nation's highly sensitive national security work, which can often only be done in secure facilities, could suffer.

With national security agencies having to choose between forcing employees to show up for work — and risk getting infected — or staying home and not working, a number of people working in and around intelligence are raising the prospect that the work of espionage could be hampered.

Uncharted Territory

The acting head of the Office of Management and Budget, Russel Vought, has continued to issue increasingly strict guidance to federal agencies to slow the spread of the coronavirus. Most federal employees are now working from home, including some White House staffers.

But for intelligence officers working on highly classified issues, whether satellite imagery of North Korean missile launches or an Iranian attack, telework often isn't an option.

Government agencies plan for all sorts of crazy contingencies and things that may pop up, from acts of God to inclement weather to acts of terrorism. They've thought about and talked about pandemics. However, it seems that they're definitely in uncharted territory at this point.

Decissions for strategies are needed

Senior officials are now trying to decide on strategies for dealing with the pandemic, and many agencies, including the Office of the Director of National intelligence (ODNI), the FBI and the Defense Intelligence Agency, are implementing shift work and social distancing in the office for essential personnel, according to current and former intelligence and national security officials. They are also authorizing others working on open source intelligence, or other less sensitive areas, to work remotely.

The ODNI "is reducing staff contact through a variety of options including staggered shifts, flexible schedules, and social distancing practices," wrote a spokesperson in an email. Intelligence "agencies are also developing and implementing appropriate response plans consistent with federal guidelines and regulations."

The motivation paradox

Remote work isn't the only problem facing the intelligence community; its employees are also having to analyze and brief on threats, including the coronavirus itself, for a president who initially downplayed the severity of the pandemic. However, intelligence officers are accustomed to risk and working through challenges. Everyone with a security clearance understands the necessity, so they are willingly taking on risk. The mission-critical national security work will go on.

The impact of the pandemic

The impact of the pandemic is spread across the community in different ways. Many employees remain in their offices in Sensitive Compartmented Information Facilities, or SCIFs, enclosed areas that are hardened against eavesdropping. Some work can be done from encrypted cellphones, and a number of top senior officials have rooms in their homes or nearby that are secured for remote work.

The community has even deployed “mobile” SCIFs in certain instances, including for briefing the president at major summits in foreign countries or for the FBI while monitoring major events. However, those options don’t extend to the vast majority of workers. Lesser of ClearanceJobs told Yahoo News that of his conversations with people in the intelligence field, workers fall into two categories: those that understand their jobs are critical and assume they will continue to come into the office, and those who are unsure whether their job duties are vital.

Limitations and road blocks in the „supply chain“

As a result, the machinery of the intelligence community is slimming down, leading to smaller briefing teams and fewer analytic assessments going out to senior policymakers. For analysts who distribute their intelligence reports, it’s unclear whether their work is reaching the government officials who need to see them.

And for case officers and undercover officials with and without diplomatic immunity, the challenges of meeting with and cultivating foreign sources are only made harder. The coronavirus and the limitations it imposes on socializing could make large swaths of the globe almost inaccessible. The “biggest challenge [operations-wise] is meeting with agents worldwide

Contractors need commitments

The coronavirus also threatens the contractors working on intelligence, a large bulk of the workforce. The Intelligence and National Security Alliance (INSA), a nonprofit trade association for current and former national security workers, asked top government officials “to bolster the health of government’s industry partners in the national security sector, which face dire financial straits as a result of the COVID-19 outbreak.”

Lawmakers working on a stimulus package to recharge a wilting economy are considering provisions that would dole out continued payment to contractors, or “equitable adjustments” for delays in completing projects. This authority would be greatly needed to ensure federal agencies maintain access to workers — including highly skilled cleared national security personnel — who can carry out their missions during this crisis and beyond.

Business Continuity for Federal Agencies

All federal agencies are required to have continuity-of-operations plans in case of a national emergency — to include pandemics — most of the preparations involve securing people in a facility rather than having them work remotely.

“They’ve got all sorts of plans for national emergencies,” said Greg Treverton, the former chair of the National Intelligence Council within the ODNI and current professor at University of Southern California. “But there wasn’t much effort at all as to how you might work remotely. ... This is so unique,” he told Yahoo News.

In years past, the focus of preparations for the intelligence community has been on external threats rather than disease.

ARTEFAKTUM

Global pandemics, although identified in worldwide threat assessments as of high priority, have surely never been resourced or funded with the priority of counterterrorism or regional threats like Iran,” said Pfeiffer, the former intelligence officer who served as chief of staff to former NSA and CIA Director Gen. Michael Hayden on CNN.

The risk of working at home

Another unique problem intelligence officials face if they work from home is being a target of foreign attacks or espionage. Employees accessing the internet at home, even for unclassified purposes, create cybersecurity risk.

Bad actors may take advantage of the fact that secure methods of communication can be harder to access or use, and may leverage that difficulty to push users to more insecure methods. A virtual private network being slow or malfunctioning is one such opportunity. In this environment where more people are remote than usual, it's something an adversary might be looking at.

Artefaktum advises Intelligence workers to work NOT from home

More generally, crises like the coronavirus present adversaries with a moment to get away with behavior that would normally elicit a strong response, such as attacks by foreign proxies on military forces overseas, as they think that the intelligence communities are weak in this moment, they will continue to seek to exploit that perceived vulnerability.

We only can urge national security workers to not try and work from home, because it is inherently “not secure.” They should be watching what they talk about on the phone, even a secure phone, because if they live in an apartment or townhouse, they may be sharing walls. Who knows who's listening.”

Why horizon scanning is important

When Artefaktum met with an CEO of a Fortune 100 company in Washington DC. last year in November, he asked the team the question you would ask any risk officer: “What are you most worried about?” Without pausing the team replied, “A highly contagious virus that begins somewhere in China and spreads rapidly. Based on our OSINT knowledge something concerning is going on in China at the moment”. This CEO, a long-term client of Artefaktum, whose company has offices throughout east Asia, adopted the proposed preventive mitigating steps to counter this potential threat.

Since the novel coronavirus has swept the world, the leadership of Artefaktum has often thought about this CEO who thanked us some days ago for our prescient risk calculus. Most leaders lack the discipline to do routine risk-based horizon scanning, and fewer still develop the requisite contingency plans. Even rarer is the leader who has the foresight to correctly identify the top threat far enough in advance to develop and implement those plans.

The Presidents` poor judgment worsening COVID-19 pandemic

Last week, the Washington Post reported on the steady drumbeat of coronavirus warnings that the intelligence community presented to the White House in January and February. These alerts made little impact upon senior administration officials, who were undoubtedly influenced by President Donald Trump's constant derision of the virus, which he began on 22 January: “We have it totally under control. It's one person coming in from China, and we have it under control. It's going to be just fine.”

The same Post report featured the following stunning passage from an anonymous US official: "The president may not have been expecting this, but a lot of other people in the government were – they just couldn't get him to do anything about it. The system was blinking red." That latter passage is an obvious reference to that aforementioned central finding of the 9/11 Commission Report.

The White House detachment and nonchalance during the early stages of the coronavirus outbreak will be among the most costly decisions of any modern presidency. These officials were presented with a clear progression of warnings and crucial decision points by the U.S. intelligence far enough in advance that the country could have been far better prepared.


But the way that they squandered the gifts of foresight and time should never be forgotten, nor should the reason they were squandered: Trump was initially wrong, so his inner circle promoted that wrongness rhetorically and with inadequate policies for far too long, and even today. Americans will now pay the price for decades.

Leaders need to rely on Intelligence - not on their belly feelings

Given that Trump concluded early on that the coronavirus simply could not present a threat to the United States, perhaps there is nothing that the intelligence community, medical experts employing epidemiological models, or public health officials could have told the White House that would have made any difference. Former national security adviser Henry Kissinger is reputed to have said after an intelligence community warning went unrecognized, "You warned me, but you didn't convince me."

Usually, federal agencies are led by those officials whom the White House believes are best able to implement policy. These officials have usually enjoyed some degree of autonomy; not under Trump. Even historically non-partisan national security or intelligence leadership positions have been filled by people who are ideologically aligned with the White House, rather than endowed with the experience or expertise needed to push back or account for the concerns raised by career non-political employees.

Government Intelligence agencies might provide misleading assumptions, but at larger scale of macro events like the actual COVID-19 pandemic, political leaders would be doing good in listening even more carefully, as Intelligence as an early warning mechanism is and will remain the only and first line of defence against any threat and risk for the people and state.



Information contained in our published works have been obtained by Artefaktum from sources believed to be reliable. However, neither Artefaktum nor its authors guarantees the accuracy or completeness of any information published herein and neither Artefaktum nor its authors shall be responsible for any errors, omissions, or claims for damages, including exemplary damages, arising out of use, inability to use, or with regard to the accuracy or sufficiency of the information contained in his publication.

All rights reserved. No part of any Artefaktum published work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from Artefaktum.

ARTEFAKTUM LTD
7 Bell Yard
London, WC2A 2JR
+ 44 20 313 75213
mail@artefaktum.net