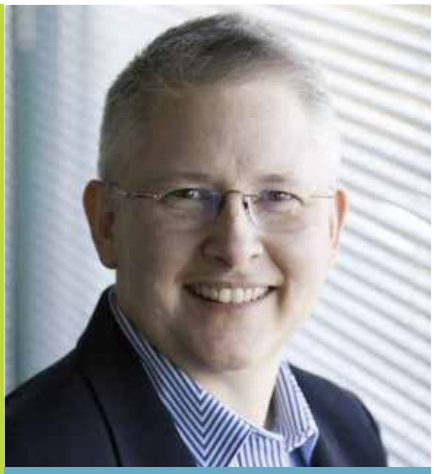
Welcome to the inaugural Innovations column. We are in the most expansive period of contracting innovation since the mid-1990s and NCMA wants to help you navigate it. In this monthly column, I will present examples of innovation in and around the contract management community—all with the goal of bringing you ideas, approaches, methods, and tools to inspire, inform, educate, delight, and challenge you to think, explore, and, attempt new things.

This month's column is by Mike Pansky, Vice-President for Innovation at U.Group, who writes about a brand new tool he and his team have created to identify COVID-19 risks to the Defense Industrial/Innovation Base (DIB). I'll leave it to him to explain the tool, but I challenge you to think of all the different ways it could be put to use for contracting and more well beyond the DIB.

Mike is a peripatetic data analyst and creator with many years' experience delving into and making sense of U.S. federal contracting and contractor data. He is especially adroit in identifying emerging companies with capabilities that are or soon will become in demand by defense and other federal agencies. I am happy to be able to share his smart, applicable, and, in this case, vital creation with you.



Anne Laurent
NCMA Director of Professional Practice and Innovation

Clearing COVID-19 from the Defense Supply Chain

How one firm is leveraging its analytical expertise to help track and assess COVID-19 risk within the Defense Industrial/Innovation Base.

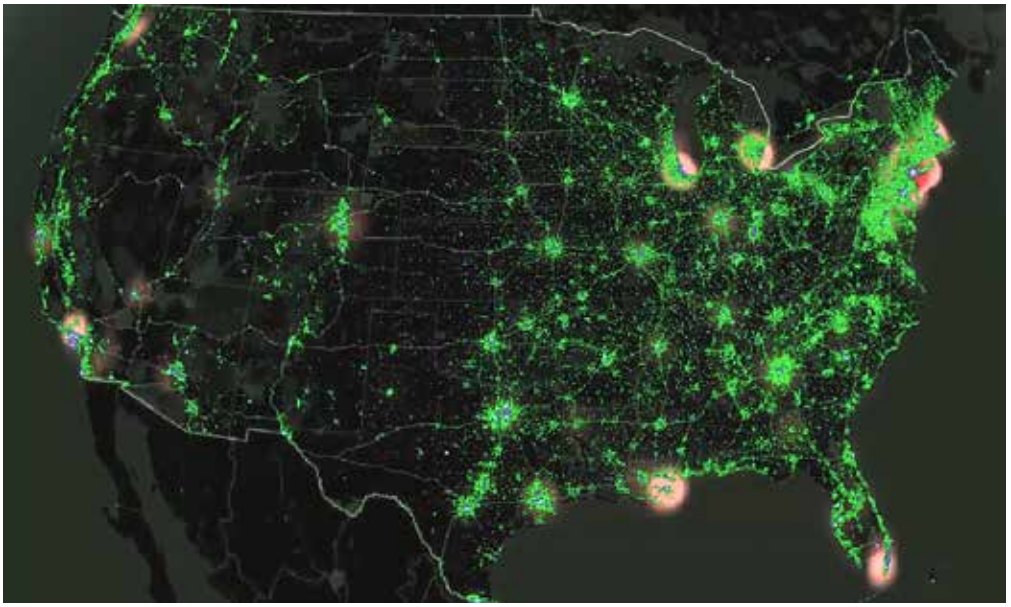
BY MICHAEL PANSKY

How do you fight an invisible threat? This is the question experts across fields, industries, and nations are scrambling to answer as the world attempts to tackle the COVID-19 pandemic head-on. The U.S. national security supply chain is far from immune to these health risks, though it has received less attention.

But unless the COVID-19 threat is curtailed quickly, lapses in supply will inevitably diminish our capacity for dealing with traditional security threats – exposing the United States to the will of malign actors. As businesses and factories shut or slow down, the Defense Industrial/Innovation Base (DIB) will increasingly face difficulties in providing critical inputs to national security. This will in turn affect research, development, and production of defense systems and other infrastructure necessary to the safety and security of our country.

To address the challenges the DIB faces during this pandemic, we've been working with colleagues to develop a first-ever, proprietary data platform we are calling CASSE.ai.[1] The platform is designed to track COVID-19 risk, overlaying DIB suppliers, so organizations and the U.S. government can anticipate where – and when – lapses in the supply network might arise.

COVID-19 strikes rapidly and can be transmitted by asymptomatic carriers, making it difficult to track. Without accurate tracking, it's nearly impossible to fully understand the virus' severity and impacts. Even with advanced modeling, we're always one



CASSE.ai's heatmap of DIB suppliers to the U.S. federal government. (Screen capture from VIMEO.)

(or two) steps behind. Community practices like disinfection, quarantines, and social distancing help combat the spread, but these measures alone are not enough. They're difficult to enforce, especially in areas with higher concentrations of essential workers and acute resource shortages—and in areas where residents are particularly susceptible to disinformation campaigns.

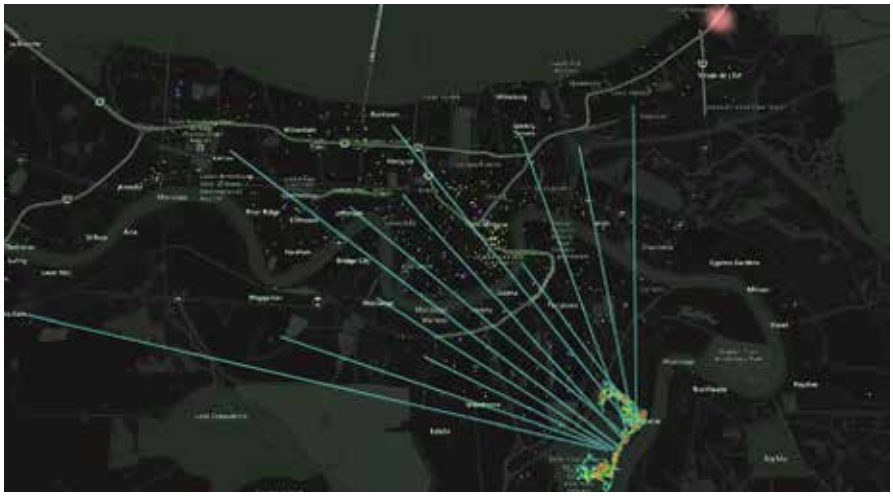
Given these challenges, it's clear we need to do more to trace and manage COVID-19's spread. We must find a way to turn an invisible enemy into a visible, trackable entity. We are developing CASSE.ai to do exactly that.

Since the initial outbreak of the pandemic, we've been exploring new ways to leverage our data science capabilities, open-source intelligence (OSINT), and proprietary sources to analyze COVID-19 spread patterns and their effects on the DIB. By tapping into social media insights, CDC reports, and nontraditional, open-source data, we correlate this critical infrastructure information—like hospital bed numbers and exposed DIB supplier facilities—to help users understand vulnerabilities under a variety of scenarios.

Open-source data fused with context about contact-traced COVID-19 confirmed cases and individuals experiencing symptoms enables analysts to work back in time to understand aggregated patterns of life, while enabling machine learning models to predict future spreads. Mapping this information to defense and civilian agency suppliers allows for precise calculation, visualization, and analysis of movement patterns in and out of suppliers' facilities. Geolocating these movement patterns to counties, towns, and cities known to have high COVID-19 risks can help federal buyers and the companies themselves better understand where pandemic-related slowdowns or closures have a higher likelihood of occurring. This intelligence, in turn, can help program and contract managers prepare for possible supply interruption, shift workload, and gauge sub-supplier risk. The information could also provide a critical data point in assessing the viability of bidders during source evaluations, as well as that of nontraditional providers new to the federal market.

We are acutely aware of the privacy risks associated with this data. We treat it with the highest level of caution, deliberation, and security. Among our precautions, we use a novel differential privacy approach to add noise and to aggregate data prior to sharing information or visuals about movement patterns derived from any of our datasets. Minimizing the risk of exposing personally identifiable information, even by inference, is one of our highest priorities—especially since we track nearly 12 billion data rows each week.

To build the supply chain information layers of CASSE.ai, we collected data from our U.Data Platform (UDP), which cleans and corrects information about U.S. federal contractors from the System for Award Management (SAM) and Federal Procure-



An example of CASSE.ai tracking COVID-19 risk factors along the supply chain. (Screen capture from VIMEO.)

ment Data System (FPDS). The result is geocoded information on more than 600,000 companies. Outside of the traditional federal contracting databases, we also bring in and entity-resolve data on more than 500,000 nontraditional suppliers and startups (along with their venture capital information). This information is vital at a time when defense programs have opened hundreds of innovation hubs to attract new firms with novel capabilities into the federal market.

Federal contractors in aggregate have vast supply chains – numbering perhaps in the millions of second- and third-tier suppliers – that are distributed globally. While we do not have movement pattern and COVID-19 infection risk data on them all, we can extrapolate from our data their intersections and thereby the U.S. defense supply chain risk of exposure due to interactions between U.S. contractors and suppliers or subsidiaries abroad. Leveraging our understanding of Major Defense Acquisition Programs and supplier contract relationships, we have created risk-scoring models that can make a big difference in keeping supplies, communications, health, and other vital systems functioning during the global pandemic and helping them ramp back up after the threat subsides.

Platforms like CASSE.ai can support more than defense program and contract managers. For example, the platform could be focused on hospitals or on emergency and health agencies charged with managing supplies of medical equipment across the country. Insights derived from the patterns of movement of patients, staff, and other emergency medical personnel among hospitals could help identify those in most immediate need of resupply and capacity expansion. Focusing the platform on COVID-19 testing stations could show how those seeking and receiving testing disperse among surrounding communities, for example, to identify locations where outbreaks might be brewing.

It's useful to view the COVID-19 threat through the lens of cybersecurity. We've already learned that the Department of Defense and civilian agencies are only as safe from cyber-attack as are the least protected of their contractors' suppliers. We've heard the stories of cyberattacks on contractors exposing plans for the F-35 fighter plane in 2016, private information on 30,000 federal employees, sensitive undersea warfare data in 2018, and more. Just as poor cyber hygiene in the supply network can cripple Pentagon programs, so can poor protection against a pandemic by leaving vital defense programs adrift without essential suppliers. Just as every program and company must redouble their efforts to monitor networks and be proactive in cyberspace, we must build up our protections against viral incursions through the use of data, analyst tools, and visualization platforms.

We're not the only ones applying our analytical expertise to the COVID-19 crisis, but we are laser-focused on the DIB and supporting the small business backbone of America. We are one of the few groups keying in on the contractors and supply network that undergird our national security to provide new, privacy-protected tools to program and contract professionals seeking to understand, ameliorate, and manage COVID-19 risk. Our choice is borne of our understanding that America's protection and its health rest on robust industrial and innovation bases providing warfighters, first responders, and health and medical staff the best equipment, supplies, and services we can muster. CM

Michael Pansky
- Vice-president for innovation, U.Group—a technology and human-centered consulting company serving the Department of Defense, federal agencies, and the private sector.

ENDNOTES

1 Editor's Note: For a demonstration of the CASSE.ai platform, visit https://vimeo.com/406924808.