The Future of the IC Workforce: *The Promise and Limits of Remote Work Technology*

OVERVIEW

The onset of the COVID-19 pandemic presented significant challenges to the U.S. intelligence and national security community (IC). Quarantine regulations, maximum occupancy rules, and social distancing guidelines forced the IC to embrace remote work. This initially proved challenging to a culture that primarily deals with classified information within sensitive compartmented information facilities (SCIFs) and has been resistant to change. The impact on teamwork, workplace relationships, and general wellbeing also raised concerns. As months passed and agencies were able to pivot their operations, the shift to remote work prompted deeper discussions about risks and benefits, impact on recruitment and retention efforts, and appropriate use of emerging technologies that facilitate secure remote work environments.

In pursuit of its mission to deepen understanding of the IC, The Intelligence and National Security Foundation (INSF), in partnership with Avantus Federal and ClearanceJobs.com, launched "The Future of the IC Workforce" videocast series in spring of 2021 to explore these questions. This three-part program examined these issues from the people, processes, and technological perspectives by eliciting key insights from top public and private sector leaders. The three discussions underscored key challenges and lessons learned from the shift to remote work.

Moderated by ClearanceJobs' Lindy Kyzer, "Episode One: Risks and Benefits of Remote Work" featured retired NSA Executive Director Harry Coker and Avantus Federal CEO Andy Maner; Acting Assistant Secretary of State in the Bureau of Intelligence and Research (INR) Kin Moy and Assistant Director of National Intelligence and the IC's CFO Trey Treadwell participated in "Episode Two: Adapting the IC Workforce: Recruiting, Retaining, Training, and Re-Skilling;" and Marie Falkowski, Chief of Digital Innovation, Weapons and Counterproliferation Mission Center, CIA, and Dr. Eliahu Niewood, Vice President of Intelligence & Cross-Cutting Capabilities, MITRE closed out the series in "Episode Three: Enabling a Secure Hybrid Work Environment."

KEY FINDINGS

REMOTE WORK IN THE IC IS HERE TO STAY

Top government and industry leaders acknowledge that remote work will persist in some form after the pandemic ends. A home and office work hybrid model will maximize the potential of the workforce. In-person work is still 'Plan A', but the pandemic has proven that not all work needs to be done in the office.[1] Workers should have the ability to work in a hybrid setting if they have demonstrated that they can be productive from home; the last year and half has repeatedly proven this.[2] Organizations stayed on track—despite the disruptive effects of the pandemic—due in large part to a successful transition to hybrid models.[3]

Work can be done outside of SCIFs, although a permanent shift to remote work presents significant questions about classification. Although the IC works with classified information, not every piece of information meets that standard, and the entire supply chain that is needed to get the job done is not always classified either. The IC has a propensity to over-classify information, and this process needs to be re-evaluated to ensure that materials are appropriately labeled to introduce greater flexibility.[4] Accurate classification will identify unclassified tasks that can be performed outside of secure workspaces and aid efforts to pivot to hybrid work models.[5]

GOVERNMENT AND INDUSTRY NEED TO EMBRACE OSINT

In a similar vein, leveraging open source intelligence (OSINT) to a greater degree further enables virtual work. Commercial success stories pertaining to OSINT demonstrate the incredible work that can be done; Bellingcat's meticulous investigation and findings regarding the FSB plot to assassinate Russian activist Alexei Navalny is a prominent example.[6] The IC must make better use of open source information to fully understand the threat landscape and protect the country.

A recent study published by Visual Capitalist provided a compelling snapshot of the staggering amount of available information. The report studied how much information is contained within an 'internet minute.' In this timeframe, 400,000 hours of videos are streamed on Netflix, 500 hours of video are uploaded on YouTube, 42 million messages are sent on WhatsApp, 6,500 Amazon packages are delivered, and over 200,000 people participate in Zoom meetings. These figures are potential sources of intelligence that could be used across the IC to study patterns of life for different groups and regions. By assigning attributes to this data, analysts can develop warning indicators. However, our adversaries also possess some of these same capabilities, and may even be more advanced if they do not have to adhere to civil liberties. IC leaders must ponder the risks and rewards of open source, understanding that our adversaries might be learning more about us than we are learning about them.

[1]*Kin Moy: "The workforce overwhelmingly supports more flexibility in telework...Plan A is still going to be being in the office and being present there where we can be the most productive...We are going to be looking at allowing workers...to use that telework flexibility...If you can show that you are quite productive still working remotely, there's no reason why you shouldn't be able to take advantage of that."*

[2]*Kin Moy: "When people drop out of the workplace...that really is a hit to not just our economy, but it is a hit to our society as well. We have invested so much in the next generation of employees in the IC. We've invested too much not to consider different kinds of flexibility."*

[3]*Harry Coker: "A former colleague told me that they have not dropped the ball on...no-fail, short term missions...those missions are going unabatedly."*

[4]*Harry Coker: "Even our classified work we had to and need to take a look at. Everything doesn't need to be in a top secret facility...There is a lot more space for us to be creative and still accomplish all of our missions."*

[5]*Trey Treadwell: "Necessity is the mother of invention...We started identifying what was it that we could do that was unclassified work [remotely]. You can do a lot of business processing reengineering without having to be in a SCIF...We started pushing onto our teams, what do you think you can do? What else is out there? What policies, what technologies do you need?"*

[6]*See Bellingcat, "Hunting the Hunters: How We Identified Navalny's FSB Stalkers," December 14, 2020. At https://www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology.*

GOVERNMENT AND INDUSTRY LEADERS MUST RETHINK HOW THEY LEAD

The disruptive effects of the pandemic have not been confined to the workforce. Shifting dynamics require leaders across the national security enterprise to analyze their leadership styles and adopt new practices. Breaking through traditional organizational boundaries and developing a bias towards action are critical steps that IC leaders must take during these challenging times. Now and in the future, leadership teams must improve their outreach to employees. Despite its merits, more remote work can be isolating and can induce stress. Leaders must make a more concerted effort to stay connected, offer timely feedback, and advocate for employees' wellness. An agile workforce must be joined by agile leadership to meet the mission.

REMOTE WORK PRESENTS NEW OPPORTUNITIES TO ATTRACT, UTILIZE AND RETAIN A SKILLED WORKFORCE

Government and industry leaders were unanimous in their optimism for remote work due in large part to recruitment and retention opportunities. Although the IC has never been restricted to recruiting solely in the beltway area, the pandemic, which temporarily limited traditional workforce functions, created an environment in which candidates from across the country attained greater visibility. The reduced need for candidates within the beltway or other national security hubs to travel into work, onboard in person, and work with classified material presented newfound flexibility for recruiters.[7]

The CIA and the State Department's Bureau of Intelligence and Research (INR) are two such organizations that took advantage. The CIA expanded its recruitment efforts outside the DC area and is "finding the talent where it sits."[8] Expanded remote work, coding and research training are just some of the ways the Agency has evolved over the course of the pandemic.

The CIA continues to leverage its technology to conduct virtual interviews and maintain better communication with applicants throughout the hiring process. In a time of isolation, these practices reintroduce a personal touch and reaffirm the agency's commitment to its people. The CIA is also using virtual reality to conduct virtual orientations, provide language courses, and present training scenarios for officers.[9]

Similarly, INR has also conducted virtual interviews and offered remote training for its applicants and workforce. INR strives to broaden its message to a more diverse audience by virtually inviting notable guest speakers to record personal messages to potential candidates. Soliciting input from the INR workforce has also informed the organization's retention efforts. An INR survey found that employees overwhelmingly supported remote work and would like the option of working in a flexible hybrid model in the future.

Government and industry leaders agreed that the pandemic reinforced the imperative to take care of the workforce. Agile leadership requires identifying what is working and what is not. The scenario of moving to the National Capital Region and working in a room with no 'comms' or windows every week has its drawbacks. Today's exceptionally talented workforce has compelling career options in both the public and private sector. Applicants and those who are already hired are often confronted with three questions: am I content with my lifestyle, do I like my boss, and where am I ultimately headed? Whether in government or industry, leaders must give greater consideration to these questions and make appropriate changes. For some situations, implementing a hybrid work model will convince parts of the workforce to stay.

[7]*Dr. Eliahu Niewood: "We need to grow that workforce. And I think we grow that workforce by having challenging problems that they can start with on the unclassified side, where they can build the technology unclassified, and we can tell them what they are working on. And then over time we can get them cleared and exposed to sponsors and have them understand the IC more."*

[8]*Marie Falkowski: "I'm a huge, huge proponent of taking advantage of the talent where it sits...In my opinion, not everyone needs to have a clearance to do great work for the IC, and particularly for those who are writing code, labeling data, delivering technologies."*

[9]*Marie Falkowski: "Virtual reality and augmented reality...will give us a lot of new options, everything from conducting virtual orientations of foreign locations. You can model the tactics for advanced weapons and technology use cases, and then language training as well as even enabling wellness and capabilities for officers who are working in high stress environments."*

Additionally, the emerging workforce has distinct philosophical differences than the 'traditional' workforce. Decades ago, it was commonplace for employees to spend their entire careers at a given agency or organization. Nowadays, many younger employees, who have a desire to work in many different spaces, do not see their career path as linear. The government needs to be more open to folks leaving government service and encourage them to come back in the future.[10] Gaining a diversity of experiences, learning new lessons, and understanding how to apply them will only help the IC. The government must allow the younger generations to find their path and welcome them back with open arms should they return.

CHALLENGES TO REMOTE WORK

Certain challenges to remote work can be mitigated through agile leadership. Leaders in the government and private sector must adapt to changing conditions to support the mission and their people. Now more than ever, strong leadership is required and maintaining communication with the workforce is paramount. Employees can feel isolated and detached from the mission when working from home. Leaders should promote the wellness of the workforce by taking a genuine interest in their situation. Indeed, strong workplace relationships are a necessary ingredient to mission success. Similarly, this issue can manifest itself in attracting and retaining a skilled workforce. A Zoom call can never replicate a firm handshake or an in-person networking session. The IC is still grappling with how to make its outreach more interpersonal.[11] Following the CIA's examples, other IC agencies should leverage virtual technology to a greater extent to mitigate this problem.

Moreover, cybersecurity concerns must be immediately addressed.[12] The shift to remote work and altered classification levels create new vulnerabilities that the workforce must be aware of. Counterintelligence and insider threats top the list. Home networks may be easy targets for malign actors, especially if employees do not practice safe cyber hygiene. Securing home and office web communications, informing the workforce of these risks, and maintaining relationships to alleviate stress can mitigate the risks of foreign actors targeting employees.

Widespread contractual requirements that companies perform all work for classified projects in a secure workspace (often at a government facility) made it difficult for companies to carve out unclassified tasks that could be undertaken remotely. Future contracts could be written with more flexible language that permits classified work to be performed at both government- and industry-operated secure facilities and that authorizes unclassified contract tasks to be performed remotely.

BUDGET ISSUES

The onset of the pandemic served as the impetus for the CARES Act. Section 3610 of this statute played an essential role in supporting government contractors by ensuring they would be paid even if they could not work in a SCIF due to social distancing requirements or other health and safety precautions. Despite 3610's huge impact, the implementation process could be improved. The government did not implement the legislation consistently across defense and intelligence agencies, and agency-specific rules and regulations complicated the process.

[10]*Harry Coker: "There is something very positive about diversity of experiences, going elsewhere, and taking lessons somewhere else, and then bringing lessons back. Diversity is an important word and it does not only rely on race, ethnicity, and gender...It applies to ways of thinking as well."*

[11]*Kin Moy: "When we are doing training at a site...there are certain aspects of that training that you get that can't be replicated, such as networking...And so we're still learning how to do that...We have to face the reality that a Zoom meeting is not the same as an in-person session...Zoom can't replicate a firm handshake and it can't replicate eye contact...Those are the things we have to make sure we're developing, a kind of personal contact with people."*

[12]*Trey Treadwell: "Technology is one of the biggest risks. The insider threat, frankly, is the most significant risk. Foreign intelligence services do try to continuously collect and target our people as potential assets...We almost always have to have in mind and the expectation that we are being monitored by somebody else...It's an awareness that we want to keep on everybody's mind."*

> We can do a lot more innovation in an unclassified space than we can in the classified spaces. We can try different things, we can just be faster, we can use the latest and greatest... I think that there are a lot of opportunities.

Organizations across the IC asked themselves what they needed to do to keep their people safe.[13] Many agencies made HVAC updates, installed cubicle and plexiglass improvements, implemented temperature monitoring, and invested in more hand towels, masks, and more frequent office cleanings. Some organizations also opened up their offices on the weekends or during early and late hours to give their workers more flexibility and reduce population density in offices. All of these measures raised costs, but the INSF speakers were adamant that these expenses were well worth it to avoid losing the workforce.

THE IC EMPLOYED TECHNOLOGY AT THE UNCLASSIFIED LEVEL

The IC leveraged emerging technologies to enable shifts to remote work and empower the workforce to do more unclassified work. Leadership continues to explore how to make these platforms more secure; implementing zero-trust architecture is certainly part of the puzzle. The Air Force piloted secure remote technologies that allowed workers to access classified information up to Secret from their homes and other remote locations away from a secure workspace.

Emerging technologies continue to be leveraged to analyze digital exhaust and commercial sensing data. AI/ML, object and image recognition, neural networks, and language translation and transcription platforms are other areas under development.[14] These technologies will be especially important to store and sort through massive volumes of open source material. Open source is the fastest growing commodity that can disrupt societies and shape public opinion, and there is no way for the IC to bring all of this into its security fabric.

[13]Trey Treadwell: "What are the things we need to do to keep people safe? In the grand scheme of things, we can replace buildings, we can replace satellites, we can replace other sorts of tangible assets. But the people of the IC really are the most critical element to making it succeed."

[14]Marie Falkowski: ""Leveraging artificial intelligence and machine learning will be game changing. It's going to help us do everything from automating collection and our reporting processes as well as making sense of large volumes of data...The use of tools like object and image recognition...neural networks and machine learning for on-demand language translation and transcription [will enhance mission effectiveness]."

Using technologies to conduct more research at the unclassified level should also engender more innovation and collaboration. Without referencing how they might be used on the high side, these projects can be marketed to attract a highly technically skilled workforce. As these folks wait for their clearances, they can work on these technologies until they are developed enough to transfer to the high side.[15] Moreover, doing this work at the unclassified level is faster and opens more space for experimentation.[16]

This approach comes with risks. Everyone must be cognizant about the classified-unclassified divide. Leaders need to understand when the questions they and their colleagues ask about unclassified data crosses a line into the classified space.[17] Moreover, it is important to protect the integrity of the data through zero-trust architecture and other mechanisms. Organizations should consider red teaming themselves to see what they are exposing at the unclassified level and how secure their systems truly are.

Instituting the appropriate policies is also critical; technology is only as good as its end user. The technology exists, but the obstacles lie in the people, processes, and culture. The IC continues to consider how it might reform certain policies to bring in more technology in a safe and rapid fashion. Incorporating more technology will always introduce more risk, but the IC agencies tend to be risk-orientated organizations. IC leaders must cultivate a workplace culture that is agile enough to adapt to new technologies and to increased risk.

CONCLUSION

Cybersecurity concerns, insider threats, and an isolated workforce are all risks associated with remote work. But risk is to be mitigated, not avoided in pursuit of the IC's mission. The benefits of remote work outweigh the drawbacks and that strong and agile leadership can greatly reduce the risks. Remote work enables IC recruiters to look beyond the beltway, find the talent where it sits, and assign unclassified projects to new hires as they wait for their clearances. Moreover, flexible schedules improve the quality of life of the workforce, particularly for parents and employees who care for other family members. For these reasons, remote work will outlive the pandemic.[18]

Referencing a McKinsey & Company report on how Fortune 500 CEOs must adapt to COVID-19, Avantus Federal CEO Andy Maner put it best. "… [we must] move even faster, break through traditional organizational boundaries, be even more intentional with a bias towards action, and set the tone from the top...We've done that... We've practiced some really good things during COVID. Let's institutionalize them. Virtual work is one that we have to work on. It's happening. It's not going away, and we are more effective with it."

[15]*Dr. Eliahu Niewood: "We need to grow that workforce. And I think we grow that workforce by having challenging problems that they can start with on the unclassified side, where they can build the technology unclassified, and we can tell them what they are working on. And then over time we can get them cleared and exposed to sponsors and have them understand the IC more."*

[16]*Dr. Eliahu Niewood: "We can do a lot more innovation in an unclassified space than we can in the classified spaces. We can try different things, we can just be faster, we can use the latest and greatest...I think that there are a lot of opportunities."*

[17]*Dr. Eliahu Niewood: "Where does risk cross the line? When do the questions I'm asking about unclassified data...make what I'm doing classified? We need to do more to help people understand where that line is, meaning at what point do the questions or compilation of data move across the security boundary, and how do we deal with that?"*

[18]*Andy Maner: "We have to embrace this as a change that was coming. This had to be done and the pandemic made it so...I think [virtual work] is inherently doable, but we have to see it as a workforce challenge, not just this 'COVID thing.'"*

ACKNOWLEDGEMENTS

INSF expresses its appreciation to the speakers and staff who contributed their time, expertise, and resources to this paper.

PROGRAM MODERATOR

Lindy Kyzer, Director of Content and PR, ClearanceJobs

SPEAKERS

Harry Coker, *Former Executive Director, NSA*

Marie Falkowski, *Chief of Digital Innovation, Weapons and Counterproliferation Mission Center, CIA*

Andy Maner, *CEO, Avantus Federal*

Kin Moy, *Acting Assistant Secretary of State in the Bureau of Intelligence and Research, State Department*

Dr. Eliahu Niewood, *Vice President of Intelligence & Cross-Cutting Capabilities, MITRE*

Trey Treadwell, *Assistant Director of National Intelligence and the IC's CFO*

INSA STAFF

Suzanne Wilson Heckenberg, *President, INSA and INSF*

John Doyon, *Executive Vice President, INSA*

Larry Hanauer, *Vice President for Policy, INSA*

Peggy O'Connor, *Director of Communications and Policy, INSA*

Britany Dowd, *Marketing and Communications Assistant, INSA*

Nicholas Damianos, *Intern, INSA*

ABOUT INSF

The Intelligence and National Security Foundation (INSF) is a 501(c)3 nonprofit organization dedicated to addressing contemporary intelligence and national security challenges, facilitating public discourse on the role and value of intelligence for our nation's security, and advancing the intelligence field as a career choice.

www.insaonline.org/foundation