INSF Position Paper: Future of the IC Workforce

OVERVIEW

INSA's Intelligence and National Security Foundation (INSF), with support from Avantus Federal, hosted a three-part multimedia series examining the *Future of the IC Workforce.* The series examined key issues facing the intelligence community workforce and provided recommendations to ensure the IC is prepared to meet future challenges and opportunities.

In the three webinars, senior public and private sector leaders shared their expertise on open-source intelligence (OSINT), the credibility of the Intelligence Community, and the state of public-private collaboration.

OPEN SOURCE… NOT THE SAME OLD CONVERSATION

MAY 2, 2022

Speakers:

Hon. Ellen McCarthy
President
Truth in Media Cooperative

Patrice Tibbs
Chief of Community Open Source, CIA

Moderator – Matt Scott
SVP, Avantus

TRUSTING THE IC

JULY 12, 2022

Speakers:

Kelli Arena
Chief of Strategic Communications, NSA

Neil Wiley
Former Principal Executive, ODNI

Moderator – Lindy Kyzer
ClearanceJobs.com

MISSION INTEGRATION

SEPTEMBER 6, 2022

Speakers:

Nic Adams
Professional Staffer, Senate Intelligence Committee

Nitin Natarajan
Deputy Director, CISA

Kristin Wood
CEO, Grist Mill Exchange

Moderator – Lindy Kyzer
ClearanceJobs.com

KEY FINDINGS

OSINT NEEDS TO BE THE INTELLIGENCE COMMUNITY'S "INT" OF FIRST RESORT[1]

The lion's share of information used by the Intelligence Community (IC) today comes from unclassified sources.[2] This is unsurprising, considering that 90% of the world's data was generated in the last two years.[3] Still, cultural and technical barriers prevent open-source material from being used to its fullest potential. While the CIA Director functions as the open-source community manager, each agency has instituted its own practices for integrating OSINT into its collection and analysis.[4] These inconsistencies complicate the establishment of a robust OSINT governance structure and the implementation of common standards for information sharing and tradecraft.

To maximize OSINT's potential, the IC may require a fundamental shift in its business model. If the lion's share of information in an intelligence report is open source and available to anyone, the IC will gain efficiencies with little risk if it expands work in unclassified spaces, relies increasingly on nontraditional sources, and instead focuses security and counterintelligence resources on protecting sensitive sources and methods.[5]

The quick declassification and public release of intelligence regarding Russia's invasion of Ukraine in early 2022, along with the release of unclassified commercially available satellite imagery – is an excellent example of the unique value of open-source intelligence. Such disclosures undermined Russia's disinformation campaign, bolstered U.S. diplomatic efforts to secure European support for Kyiv, and proved the IC's value to the American people.

A STRONG PUBLIC-PRIVATE PARTNERSHIP IS ESSENTIAL IF THE U.S. IS TO MAINTAIN ITS EDGE IN INTELLIGENCE

Speakers throughout the series emphasized that leveraging private sector expertise and tools is vitally important for the United States to maintain its competitive edge in intelligence.[6] The private sector has developed incredible OSINT tools and continues to do so. It outperforms the government in this sector.[7] Because innovative technologies of all types are increasingly being developed by companies with little to no experience working with the federal government, it is imperative that the Intelligence Community figure out how to add such non-traditional government contractors to its roster of industrial partners.

EVOLVING THREATS REQUIRE GREATER COLLABORATION

The importance of solid, well-defined partnerships is essential to address the risks of online connectivity and unprecedented interdependence between critical infrastructure sectors. A cyberattack that causes even a minor disruption in one sector could tremendously impact others.[8] The concept of "national security" has thus broadened to include nontraditional stakeholders in the critical infrastructure and homeland security spheres.[9] Collaboration is hindered, however, by the size of this space and the breadth of actors that operate differently and are affected in different ways by digital threats.[10]

National security stakeholders in the public and private sectors must work to further integrate their approaches to physical and cyber threats.[11] These two worlds need to be brought together in a Whole of Nation approach by strengthening collaboration across all levels of government and with private sector partners.[12]

Moving forward, partnerships between all stakeholders need to be defined, open, and practiced. Collaboration must enhance government and industry actors' ability to collect, analyze, and disseminate accurate information to decision-makers and warfighters quickly enough to be actionable.[13] As more information and data become available, partnerships need to grow stronger to achieve this objective.

THE IC NEEDS A DIVERSE AND DATA-SAVVY WORKFORCE

With more and more applications for data and high-tech resources, the need for a diverse, data-savvy workforce is critical.

The IC needs people capable of using advanced technologies to increase the speed at which new capabilities are developed and delivered – particularly those that make sense of large amounts of information.[14] New technologies to solve the "big data" problem, such as artificial intelligence and machine learning, will not help unless the workforce can adequately apply them.[15]

With digital threats expending, the IC also needs people capable of protecting data[16] and associated technology from cyberattacks. While the up-and-coming generation is tech-savvy, they must also be sufficiently data-savvy to protect personal and sensitive data. Data security is the weakest link, and the entire workforce needs to think about data security as part of everything they do to improve resiliency against online attacks.[17]

New human capital policies may also be needed to improve the effectiveness of IC leadership. Although top officials at executive branch policy agencies change with each Administration, the professional, non-partisan Intelligence Community would benefit from consistent leadership that is insulated to some degree from shifting political winds.[18] Rather than replace leaders every few years, the White House and Congress may want to consider appointing agency leaders for fixed terms that span presidential administrations, such as the ten-year term served by the Director of the FBI.[19]

CHANGES IN THE INFORMATION ENVIRONMENT WILL CONTINUE TO CHALLENGE THE IC

The changes to the information environment, including ease of access and amount available, have challenged the IC, which must now compete with other sources when briefing the public and internal stakeholders.[20] This issue is exacerbated by the tendency for individuals and communities to live in information silos surrounded by only the information they want to hear. Adversaries are also taking advantage of these silos to feed mis-and-disinformation to the American public.[21]

The public's trust in the IC may be undermined by misinformation and by media reports that the relationship between policy and intelligence is contentious. However, high levels of trust exist within the IC and between its key policy customers. Given that the IC exists to enable decision-making, maintaining that trust is vital.[22]

The information environment will only get more complex, saturated, and difficult to navigate. The key is for the IC to remain consistent and apolitical to maintain and expand trust with internal and external stakeholders. The IC must remain above the political debates of the day and perform with integrity and credibility.[23]

AN APPROPRIATE BALANCE BETWEEN TRANSPARENCY AND DISCLOSURE IS NECESSARY TO INCREASE TRUST WITH PUBLIC

Transparency increases trust between the IC and the public, as it allows the public to know what government agencies are doing and spending on their behalf.[24] That said, a balance must be struck between transparency and disclosure: providing the public with sufficient information to understand how the IC operates without disclosing sensitive intelligence sources or methods. The more the public understands about intelligence institutions, the value they produce, and the legal authorities (and guardrails) that guide their efforts, the more comfortable they will be with activities that cannot be discussed publicly.[25]

In many circumstances, it is not appropriate for the IC to have a presence in the public information environment. The IC builds and maintains trust with internal customers and stakeholders through constant engagement; this "back and forth," which highlights the rigor of IC analysis as it helps address policymakers' questions, is inappropriate to reveal in the public arena.[26]

Policymakers must continually evaluate whether the public release of the information they receive – perhaps to advance diplomatic objectives – would help build trust in the Intelligence Community. It is important to understand that the IC itself does not decide what information becomes publicly available; policymakers are charged with deciding what specific information is released and when.[27]

Leaders, especially in Congress, are right to be concerned that the IC's increasing use of open-source data has the potential to infringe upon American citizens' privacy. It is important for IC and other government leaders to communicate the robust legal regime that governs intelligence agencies' activities and explain how the IC uses – and doesn't use – publicly available information on American citizens.

CONCLUSION

With the "Future of the IC Workforce" multimedia campaign, INSF, with support from Avantus, examined some of the most crucial challenges facing the Intelligence Community. The campaign brought together senior leaders from the public and private sectors to discuss harnessing the full potential of open-source intelligence, the importance of trusting the IC and improving mission integration.

The changes to the information environment and threat landscape pose unique and unprecedented challenges to the future of the IC workforce. The widespread availability and richness of publicly available information will increase the IC's open-source advantage and create requirements for skilled personnel who can collect, compile, and analyze information from disparate sources and large unclassified data sets. Strong public outreach is needed to recruit personnel with skills in data analysis, technology applications, and cybersecurity. Similarly, strong collaboration is necessary to ensure that large amounts of available data do not impede timely intelligence analysis.

As threats in the digital realm continue to grow, close interagency and public-private relationships are critical to addressing the risks of cyberattacks. Close relationships and clear communications with the American public will also help the community receive the public support needed for the IC to operate effectively. While the environment the IC works and operates in has, and will continue to, change with the information environment, stronger relationships and collaboration will lead to continued success.

REFERENCES

[1]*Patrice Tibbs: "It (OSINT) is becoming what most of us call the INT of first resort… Every incident, every issue, has been validated or even come to our attention through open source."*

[2]*Patrice Tibbs: "…When you look at the landscape and the demand and how it's increasing and how we now communicate, that (open source) really is the lion's share where information is coming from."*

[3]*Ellen McCarthy: "90% of the world's data today has been generated in the last two years… that number is increasing and at increasing rates."*

[4]*Patrice Tibbs: "The key for me is understanding how to modify and change and adapt to amount of data of data that is available, and because there is*
not a consistency to how each of the 18 organizations is… integrating open source into their workflows, there are inconsistencies in how that is translated and shared."

[5]*Ellen McCarthy: "She (Amy Zegart) assesses that roughly 80% of all information in today's intelligence reports are available through openly available sources… Maybe we need to focus on protecting that other 20% and not the 80% that is already out there."*

[6]*Ellen McCarthy: "We need another Wild Bill Donovan moment… the difference is that it could be a private sector Bill Donovan."*

[7]*Ellen McCarthy: "Are we keeping up on the government side?… I would portend that no, I think the IC has not kept up with the digital age."*

[8]*Kristin Wood: "Now it is all interconnected, so now what each of us do has a tremendous impact on the other… if I introduce something into the supply chain, that is now something government has to deal with."*

[9]*Kristin Wood: "I think there is a conversation around 'what is the national security community'… its not just the traditional spaces, it could really be a tremendous step or two or three or five away from what we've seen as the national security community."*

[10]*Kristin Wood: "The challenge in my perspective is the space is so big… and how conveying the threat is so difficult because how the sectors respond differently and the threats to them would respond differently."*

[11]*Nitin Natarajan: "We look at mission integration in multiple ways. I think kind of at the largest macro-level obviously we are looking at our mission, at the protection of critical infrastructure against cyber and physical threats and that within itself brings together two worlds… mission integration at the largest level is how to bring these two worlds together."*

[12]*Nitin Natarajan: "How do we bring these two worlds together… I do think we look at mission integration on a lot of other levels and layers and a lot of it is our engagement with the private sector and how we can strengthen that… and strengthen our relationship with state, local, and tribal partners?"*

[13]*Nic Adams: "We are collectively making sense of [mass data and threat environment] in terms of how we harness it for national security, so we ensure information and accurate intelligence is getting to both policy makers and warfighters at the speed of relevancy."*

[14]*Nitin Natarajan: "As we look at, how do we speed up this type [information sharing] of capability, how do we continue to maintain a robust capability, it all comes down to the workforce. We are focused on building a great workforce… that we bring in the right talent and we retain that talent."*

[15]*Nic Adams: "You can put all kinds of great technologies into pay but you have to have a trained, talented workforce to execute that, and that has to come from all sectors of American society and one of our strengths is our diversity."*

[16]*Nitin Natarajan: "What I would offer is I'm not sure [the younger generation] is cyber-savvy as much as they are tech-savvy… but have we really trained them to be more cyber-savvy? And this comes with them sharing their personal data and what they're sharing. "*

[17]*Nitin Natarajan: "How do we incorporate a lot of this security into our day-to-day lives… the more we can do across that spectrum because it is the weakest link, and we really need everybody to be doing their part to raise that resilience."*

[18]*Ellen McCarthy: "We need… consistent, focused, very senior leadership on this issue… You just do not get that with the appointment process where people come in for two or three years and then rotate out."*

[19]*Ellen McCarthy: "We need… consistent, focused, very senior leadership on this issue… You just do not get that with the appointment process where people come in for two or three years and then rotate out."*

[20]*Kelli Arena: "There is a lot we do the public just doesn't know. It is harder and harder in this information environment to break through with information especially accurate information and that is where the challenge lies."*

[21]*Kelli Arena: "It is really difficult to get a message that resonates to the general public or stakeholders…Folks are creating information silos so If you are not present in those information venues, you cannot get to those folks."*

[22]*Neil Wiley: "The Intelligence community exists to enable decision-making in the policy and decision-making world, and they have to trust as much or more so than the public does."*

[23]*Kelli Arena: "The IC must move forward in apolitical and consistent way, that engenders trust. You cannot be subject to the whims of the day and the political leanings of the day and move forward with integrity and credibility."*

[24]*Kelli Arena: "There is a happy medium. The public has the absolute right to know authorities we have, the budgets we have, what we are doing with taxpayer dollars."*

[25]*Neil Wiley: "There is a difference between transparency and disclosure. The American public has the full right to know how the intelligence community operates. The more they know about the ethical underpinnings of what we do, the more comfortable they will be."*

[26]*Neil Wiley: "The way we maintain and build trust with internal government stakeholders is through constant interaction and assessment. We expect back and forth, and it is that interaction that highlights the rigor we approach the process. That is where the confidence grows and build. We cannot be as transparent, interactive, or candid with the public sector."*

[27]*Neil Wiley: "The decision for the intelligence community to engage in the public environment is a policy decision, it is not an intelligence community decision… and it has to be done for a very specific reason with a very specific intent."*

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*

Aaron Rosenthal, *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.

Underwritten by Avantus

Avantus Federal, a NewSpring Holdings Company, is a mission-focused digital services and solutions company. We help our Homeland Security, Defense, Intelligence and Federal Civilian clients protect our Nation.

Our core offerings include data & technology, mission services, and consulting & transformation. We have industry-leading capabilities in defensive and offensive cyber, cloud engineering and cloud-native development, and the use of big data and machine learning in operations and analysis. Our clients benefit from our leading-edge capabilities combined with a sense of commitment and responsibility to the mission. And our employees benefit from a values-based culture of continuous investment in their career growth.

www.insaonline.org/foundation