A White Paper on the Key Challenges in Cyber Threat Intelligence:
Explaining the *"See it, Sense it, Share it, Use it"* approach to thinking about Cyber Intelligence

We spend considerable time and effort producing cyber threat intelligence. Once a monopoly of government, the private sector as well is now actively producing and consuming 'actionable' cyber threat intelligence. The National Intelligence Manager for Cyber is charged with integrating this activity within the US Intelligence Community and of looking strategically for ways to improve the quantity, quality, and impact of cyber intelligence. As part of this dialogue within Government, we created this graphic and model as a simple way to describe the cyber threat intelligence process and think about ways to improve our performance.

1. **See it:** collecting intelligence/data on foreign cyber threat activity is a significant challenge. Government sees and collects only a fraction of foreign-based malicious cyber activity that occurs. Its resources are limited and must be allocated judiciously; collection management informed by historical activity or predictive analysis is used to focus effort on the vectors or targets most likely to pose significant threats. At the same time, malicious cyber activity will grow in scale and scope and the potential 'attack surface' will also grow as a function of technology (e.g., the Internet of Things, 5G wireless) and digital innovation. In short, no government or private sector organization has the bandwidth or resources to be omniscient in seeing malicious cyber activity. Improvement in collection is more likely to result from partnerships--pooling data to create shared situational awareness—than from any organization successfully collecting against <u>all</u> relevant external threat activity on its own.

2. **Sense it**: making sense out of data (processing it), turning raw data into intelligence, and turning intelligence into insight.

Processing it: means turning raw data into 'dots' that can be connected. We typically see, collect, and analyze threat activity in stovepipes based on the modality and organization by which it was collected. However, data collected by different means and organizations is not necessarily additive or intrinsically comparable; for example Internet vs. human-sourced vs. imagery data differ in form and focus and may not be directly comparable. In addition it is worth considering the following questions:

- How much of the data that we collect or have access to do we *actively* process (attempt to normalize or make readily comparable) for use in analysis?
- How much of the data is available for *passive* use (e.g., as background, reference, or as research data)?
- How can technology (e.g., Artificial Intelligence, machine learning, automation, secure collaboration) increase the volume and efficiency of data exploitation?

'Connect the dots': There are significant conceptual challenges even after data has been rendered interoperable.

- Malware signatures, information on hacker intentions or activity, and firewall log data can be all potential indicators of activity pertaining to the same threat operation, but this data may not be readily compared or connected without a process or framework to normalize it via a common ontology or lexicon so that disparate data can be efficiently and effectively compared and understood.
- Determining threat actor intent is an important facet of analysis, since malicious cyber activity is a means to an end. How do we blend technical, regional (understanding of the actors and their motivation), and functional (e.g., cybersecurity or counterintelligence) expertise on motive and intent in performing cyber threat analysis?

Understanding threat in context. Threat intent and activity need to be mapped against target vulnerability and the consequence or impact of success by the actor in order to provide a holistic picture of threat (i.e., what we see *and* what it means). This can be especially challenging for Government when the bulk of the potential targets and first-hand information about vulnerability and consequence of malicious threat activity belongs to the private sector. Data owners often struggle to comprehensively identify their assets and to understand their vulnerability and the potential consequence of threat activity; this lack of internal insight compounds the challenge of effective two-way communication with providers of threat information.

Making our understanding of threat actionable. What is 'actionable' for a senior decision maker, a network defender, or someone conducting cyber operations are distinct and different, and this argues against adopting a one size fits all solution. What you want the recipient or consumer of a threat report to do with it should shape its focus and content.

3. **Share it:** providing actionable threat information to decision makers, network defenders, and those who need to be informed in order to operate and work on the network. These consumers of threat reporting can be located:

- *within the community* that produces it (e.g., an Intelligence, Law Enforcement, or Cybersecurity community)
- *within related communities* such as across Government or a private sector consortium.
- *external* to the originating group or community.

Sharing can be done either directly by the reporting organization or indirectly through other elements. In the case of information shared indirectly, it is worth separately tracking whether

the intermediary organization actually passed the threat information to its intended recipient and how long this process took. If the information was not passed, why not (e.g., resource constraints, policy constraints, a judgment that the information would not be helpful to the recipient)? Was feedback provided to the originator by these intermediaries?

4. **Use it**. This is the primary purpose underlying the production of cyber threat intelligence! If threat reporting was not used, was it because of a shortcoming related to the product? For example, was the intelligence not actionable? Not timely? Did it lack contextual information to allow the recipient to evaluate it and prioritize whether and how to act? Alternatively, was the report not used for factors beyond the threat intelligence provider's control, such as human error or resource constraints on the part of the recipient? The latter is probably the most frequent outcome since few if any organizations have enough cybersecurity resources to deal with *all* threat activity!

5. **Was feedback provided?** While threat intelligence is not a panacea and it would be problematic to require that a recipient act on a report, documenting its passage and giving the recipient the opportunity to provide feedback both provides a means of tracking progress (are we sharing more over time?) or problems in information sharing and also creates an opportunity to drive improvement in the quality of reporting. This affords private sector targets, in particular, with the opportunity to sensitize government threat producers-- those struggling in the 'Sense it' part of the intelligence cycle with a lack of first-hand insight into target vulnerability and impact—with insight and potentially with specific information that would be useful in shaping future analysis.

There are a number of tools or levers that can be used to drive change at various points in this cyber threat intelligence cycle. These tools include:

- **Organizational structure** such as the merger or co-location of business units to facilitate fusion of expertise and data (e.g., to tackle the challenges in 'Sense it')
- **Technology** such as AI and Machine learning, automation, collaboration tools, anonymization of sensitive data, etc.
- **Processes** (directives and standard operating procedures)
- **Legislation** (creating requirements, authorities or organizations)
- **Additional Resources** (“throwing people or money at the problem”)
- **Oversight** or focused senior management attention

Some of these tools are more useful (i.e., readily applied or have more impact) at certain points in the cycle than at others.