The Merits of Adopting a Common Approach to Describing and Measuring Cyber Threat

This paper is intended to stimulate discussion of the merits of adopting a standardized approach to measuring and recording malicious cyber threat activity and to describe potential next steps an organization – or nation – might take to harmonize its approach towards recording and analyzing cyber threat activity. It builds on the U.S. experience developing and beginning to implement a common cyber threat framework across government. In the process, it was discovered that a common model or approach can facilitate both the accurate and timely sharing of cyber threat information between policymakers and cyber experts, as well as trend or gap analysis that can yield metrics for use in evaluating threat activity or the efficacy of cyber security measures.

This common cyber threat framework (hereafter, framework) was developed in response to a recognition that the diversity and growing number of cyber threat models underpinning information used by or shared with government made it difficult to share cyber threat data and to communicate effectively with policymakers, across government missions such as military, law enforcement, and cyber security operations, and with victims of malicious cyber activity in the private sector. The resultant common cyber threat framework and an accompanying lexicon of terms for malicious cyber activity has helped create standard definitions and a shared methodology within government for characterizing and describing cyber threat activity.

The resultant framework began as effort to enhance data-sharing throughout government to facilitate situational analysis based on objective (typically, sensor-derived) data and to provide a simple yet flexible common environment and world view of cyber threats. It was intended to provide a common backbone (a 'cyber Esperanto') to facilitate interoperability, mapping multiple models to a common standard rather than directly to each other, and to help avoid cyber experts and senior policymakers talking past each using common terms that each interpreted differently. The goal was to have a repeatable and scalable model that was flexible and could be configured to provide the optimal focus, view, and supporting content for audiences ranging from policymakers to cyber experts.

The framework is intended to capture the data of more complicated and diverse models and to be broad enough to cope with a wide variety of threat vectors (e.g., Internet-based, supply chain, insider-enabled) and victims (e.g., government, industry, academia, and international partners). To accomplish that, the Framework uses a hierarchical or nested approach to describe the potential *Stages* in the lifecycle of an adversarial cyber activity, the *Objectives* that a threat actor might hope to achieve in these Stages, the *Actions* through which Objectives are met, and measurable *Indicators* of action or activity. The layering of data within the framework provides a general, high level overview of activity at the Stages level for senior policy makers, and by 'drilling down' into increasing specificity in the underlying detail in the lower layers supports a more technical and tactical view for the cyber expert. This structure and layering provides a repeatable and scalable tool where data can be aggregated or disaggregated to support the desired focus and content of audiences ranging from non-technical executives to cyber subject matter experts. The US government is using this model in some of its published cyber threat reporting and is exploring its use to help dynamically allocate cyber resources and as a common language for victim notification. This common cyber threat framework is also being implemented in a variety of foreign government, industry, and academic settings.

Lessons Learned/Points to Consider

1. An open framework approach enables consistent characterization and categorization of cyber threat activity regardless of the mission (e.g., defense, cyber security, intelligence, law enforcement) of the organization that detects it. The construct allows adopters to map disparate threat models to a common backbone, which promotes consistent categorization of cyber threat events and provides a foundation from which to identify trends or changes in threat activity and to gauge the effectiveness of cyber security measures.

2. A common cyber threat framework supports but does not replace human-driven analysis. Beyond describing current threat activity, the data captured in the framework can readily support trend, predictive, environmental, and vulnerability analysis, since the uniform categorization and characterization of the underlying data allows analysts to identify changes in threat activity over time or changes in the behavior of various threat actors towards specific targets, and to anticipate future developments, note gaps in the available information, and conduct risk analysis.

3. The value of the framework in fostering interoperability and situational awareness across organizations is not affected by the source of the data, regardless of whether it comes from open sources, sensitive/classified sources or whether it is internally-derived or externally-provided. Its value lies in the compilation of threat data in common terms and categories, and the presentation of content in a consistent and repeatable manner.

4. Key to successful application of a common cyber threat framework is explicit documentation and transparency. Using terminology in the framework that is mission-neutral and not specific to any one operational discipline (e.g., intelligence, military operations, or law enforcement) or line of business facilitates broader dialogue within government and with the private sector that owns and operates many of the networks and systems affected by cyber threat activity.

Specific recommendations

1. *Adopt a model that follows a structured and hierarchical approach to describing threat activity.* This allows the model to work for multiple audiences ranging from private sector executive management or government policymakers to cybersecurity and information technology experts, and to capture threat activity regardless of source (e.g., malicious external actors, insider threats, or from compromises in the supply chain). This enables the user to tailor their view of the collected data, expanding or collapsing the information displayed in the model to suit specific needs without losing accuracy in the process.

2. *Ensure the model, its constituent parts, and the associated terms and concepts are explicitly documented and freely shared.* Even if the model one adopts differs from the common cyber threat framework or some other standard, as long as it is explicitly documented and its content and concepts can be mapped back to a common ontology and standard, the collected data can be readily shared with others. Some or all of the translation between models can be automated to increase and to speed shared situational awareness of threat activity.