About
The SEI Emerging Technology Center helps the government stay on the edge of technology. The world is innovating software and information technologies very rapidly and the Center assists the government by identifying, demonstrating, extending and applying emerging software technologies to meet critical government mission needs. We focus on promoting government awareness and knowledge of emerging technologies and their application, and shaping and leveraging academic and industrial research.

Contact Us
Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-3612
Phone: 412.268.5800 | 888.201.4479
Web: www.sei.cmu.edu/go/gnta/cyberintelligence
Email: cyber-intelligence@sei.cmu.edu

Cyber Intelligence Conceptual Framework
Comprehensive analysis. Better decisions.

SEI Cyber Intelligence Research Consortium
Analytical Acumen

Analytical Acumen facilitates timely, actionable, and accurate intelligence on a cyber issue. As previously described, this component is the framework’s center of gravity. It conceptualizes an analyst’s interactions with the other components to facilitate the development and dissemination of intelligence that helps decision makers and practitioners make better judgments and quicker decisions. Analytical Acumen interacts with the other components in numerous ways, depending on the cyber issue being analyzed. Sometimes a repeatable process can be introduced or a technology integrated to augment these interactions, but enough flexibility must be built into the process or technology to account for a cyber issue’s propensity to change quickly and often. One of our goals is to account for all these possibilities by visually projecting a nonlinear, interactive approach to performing cyber intelligence.

Environmental Context

Environmental Context provides scope for the analytical effort. Ideally, one of the first steps an analyst will take is to assess the cyber issue as it relates to the operating environment. For example, if the issue involves employees downloading corrupt software from the internet, and the analyst knows the organization’s computer network does not connect to the internet, the analyst can quickly report the limited threat without performing more extensive analysis. If the network does connect to the internet, then the analyst begins to put the cyber issue in context to determine what other information is needed to assess and report the potential threat’s impact on the organization.

An analyst can better understand the state of the operating environment by considering the internal and external factors affecting it. We suggest examining the internal and external factors relating to the network and the organization at large. Examples for the network include topography (infrastructure, access points, system vulnerabilities, identification of critical data) and cyber footprint (physical assets, data storage, web and mobile presence). For the organization at large, factors include business operations (risk management, physical security, and compliance), organizational dynamics (mission, objectives, stakeholders, culture), and external interests (brand reputation, market space, geopolitical issues, and partnerships).

While considering Environmental Context is important at the onset of analysis, it should occur throughout the analytical effort because issues in the cyber domain change quickly and often. This component also highlights the importance of both technical and nontechnical factors in cyber intelligence. Deciphering the functional details of a cyber issue is vital to putting it in context, but so too are many factors that have nothing to do with technical expertise.
Microanalysis represents the assessment of the functional implications of the cyber issue. When performing such analysis, the analyst seeks to evaluate and estimate how the issue impacts the operating environment based on the issue’s technical complexities. Information obtained through Analytical Acumen and Data Gathering should be used to extract relevant data and examine the issue’s nature, ability, and quality. The primary purpose of Microanalysis is to answer “what” and “how” questions: what is happening to the network and how is it being done? The analyst successfully answers these questions using the power of their analytical tradecraft and the continuous interaction with the tools, technology, and people gathering the data.

Knowing how the cyber issue functions, the analyst uses multiple sources, when possible, to validate the credibility of the information and then puts the issue into technical context by applying knowledge to it. The analyst can use what is now intelligence to inform fellow practitioners and decision makers of the cyber issue’s functional implications. We describe this communication and the feedback that follows in the conceptual framework’s Reporting and Feedback component. As a reminder, throughout the entire process, Analytical Acumen facilitates the interactions among these components.

Overall, Microanalysis usually occurs in reaction to an actual cyber issue, not the anticipation of one. This type of analysis is especially useful for network defense, cybersecurity, and incident response purposes. It also informs the individuals in an organization that examine the issue’s strategic implications and make business decisions.

Reporting and Feedback conceptualizes how to offer courses of action to enhance decision making with cyber intelligence. The conceptual framework is arranged so that no matter the component where the intelligence originates, Reporting and Feedback represents the communication of and subsequent responses to the intelligence. An analyst should take into account the audience’s background and technical knowledge and tailor any verbal or written analytical products accordingly. This work usually is distributed to a variety of fellow practitioners, relevant stakeholders, and decision makers at multiple levels of leadership, from first-line supervisors to C-level executives. These individuals then use the intelligence to guide their response to a cyber issue or adjust the overarching direction of the organization.

Regardless of the intelligence being produced, the reporting mechanism is only as effective as its feedback counterpart. Responses in the form of casual observations or official requests for information help to rationalize what the analyst focuses on. Active participation from all audiences not only validates what an analyst does on a daily basis, but also identifies intelligence gaps for the analyst to fill, concepts needing further explanation, and opportunities for collaboration. This spurs continued development of analytical tradecraft, which improves an analyst’s effectiveness and efficiency in using cyber intelligence to help others make better judgments and quicker decisions.
Using the Conceptual Framework

We consider our conceptual framework to be a living framework. It incorporates perspectives from government, industry, and academia to distinguish and organize how we think an analyst should approach cyber intelligence. As these perspectives evolve, so too will the framework. If you have any questions or suggestions, please contact us at cyber-intel@sei.cmu.edu.