Carnegie Mellon University
Software Engineering Institute

Cyber Intelligence Tradecraft Report

Executive Summary

IN 2018, THE SOFTWARE ENGINEERING INSTITUTE (SEI) AT CARNEGIE MELLON UNIVERSITY conducted a study to understand how organizations in the United States do the work of cyber intelligence. In our Cyber Intelligence Tradecraft Report: *The State of Cyber Intelligence Practices in the United States*, we provide a detailed look at the best practices and common challenges we discovered during our study of organizations and their cyber intelligence teams. We identified the top ten areas of opportunity and concern:

Top Ten Things You Need to Know Now About Cyber Intelligence Practices

1. **Cybersecurity is not cyber intelligence.** Definitions for cybersecurity and cyber intelligence vary widely and are often misunderstood as one and the same. This misunderstanding leads to confusion of effort and organizational vulnerability. A common lexicon on terms is needed to build trust.
2. **Organizations should adopt a defined and repeatable cyber intelligence workflow.** The analytic framework defined in the 2013 Cyber Intelligence Tradecraft Project report still holds true today. A workflow should consist of an organization's understanding of its environment, data collection, threat and strategic analysis, and reporting and feedback to decision makers.
3. Organizations have trouble identifying the location of confidential and intellectual property data due to information silos within the organization. These silos also affect an organization's ability to understand how data moves across the organization and when and how individuals interact with the data. **Crown-jewel identification exercises can help.**
4. Organizations lack people, time, and funding to build a cyber intelligence team. **Organizations should leverage NIST NICE SP 800-181 as a starting point to create a cyber intelligence team.** While most organizations agree technical skills can be taught, non-technical skills such as critical thinking, a passion to learn, and emotional intelligence are equally important.
5. **Fusion centers,** generally found in larger organizations, help break down information silos and enable timely action **regarding threats, risks, and opportunities.**
6. Many organizations lack consistent intelligence requirements and data validation processes. **Create collection management teams to assist with intelligence requirements, data validation, and third-party intelligence provider relationships.**
7. **For threat analysis and cybersecurity tasks, SOAR technologies can be a force multiplier** for organizations with limited time and people drowning in repetitive manual tasks.
8. **Strategic analysis is not only comprehensive, it is also anticipatory.** Organizations should perform strategic analysis to holistically assess threats, emerging technologies, and geopolitics that may impact the organization and/or provide opportunities for the organization today and in the future.
9. **Consumers of cyber intelligence reports,** especially leadership, **should provide active feedback to the cyber intelligence team** on content, format and new requirements.
10. **The amount of data generated is increasing exponentially, so humans and machines need to team together to manage it.** Organizations will not only need more compute power, they will need more machine learning engineers, data scientists, and cyber intelligence analysts proactively working together to extract intelligence out of data.

INTELLIGENCE DATES TO ANCIENT TIMES when early civilizations used it to protect their assets and gain an advantage over their adversaries. Although the ways we perform the work of intelligence have changed, it remains as critical as ever. And this can be no truer than in the cyber domain. In performing cyber intelligence, we collect, compare, analyze, and disseminate information about threats and threat actors seeking to disrupt the cyber ecosystem,[1] one of our most critical assets. Through cyber intelligence, we know ourselves and our adversaries better. And with that knowledge, we can proactively take steps to better understand risks, protect against threats, and seize opportunities.

In 2013, the Software Engineering Institute (SEI) at Carnegie Mellon University conducted a study on behalf of the U.S. Office of the Director of National Intelligence to understand the state of cyber intelligence practices at organizations throughout the country. We conducted a similar study in 2018, and this report details our findings.

We built on outcomes from the 2013 study to develop foundational concepts that drive the 2018 study. First, we define cyber intelligence as acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making. Second, we propose a framework for cyber intelligence; based on the intelligence cycle, its components provide for environmental context, data gathering, Threat Analysis, Strategic Analysis, and reporting and feedback.

During the 2018 study, we interviewed 32 organizations representing a variety of sectors to understand their best practices and biggest challenges in cyber intelligence.

During conversations guided by questions designed to elicit descriptive answers, we noted organizations' successes and struggles and how they approached each component of the cyber intelligence framework. We also provided an informal assessment of how well each organization was performing for certain factors within each component. We aggregated and analyzed these answers, grouping what participants told us into themes. This report moves through the cyber intelligence framework, detailing our findings for each component. Three companion implementation guides provide practical advice about machine learning and cyber intelligence, the internet of things and cyber intelligence, and cyber threat frameworks.

There are a number of areas where organizations can take action to improve their cyber intelligence practices. They include differentiating between cyber intelligence and cybersecurity, establishing repeatable workflows, breaking down silos that fragment data and expertise, enabling leadership to understand and become more engage in cyber intelligence, establishing consistent intelligence requirement and data validation processes, and harnessing the power of emerging technologies.

Since 2013, the practice of cyber intelligence has gotten stronger. Yet it is not strong enough. In the coming years, data and compute power will continue to increase, and artificial intelligence will enable us to make sense of threats while also making threats themselves more complex. Organizations of any size can learn from and apply the best practices and performance improvement suggestions outlined in this report. Together we can achieve higher levels of performance in understanding our environment, gathering and analyzing data, and creating intelligence for decision makers.

Want more than just the top ten? See the full report Cyber Intelligence Tradecraft Report: *The State of Cyber Intelligence Practices in the United States*

1 https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

About the SEI

The Software Engineering Institute is a federally funded research and development center (FFRDC) that works with defense and government organizations, industry, and academia to advance the state of the art in software engineering and cybersecurity to benefit the public interest. Part of Carnegie Mellon University, the SEI is a national resource in pioneering emerging technologies, cybersecurity, software acquisition, and software lifecycle assurance.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu

©2019 Carnegie Mellon University | 5228 | 04.30.2019