Cyber Intelligence - Conceptual Framework

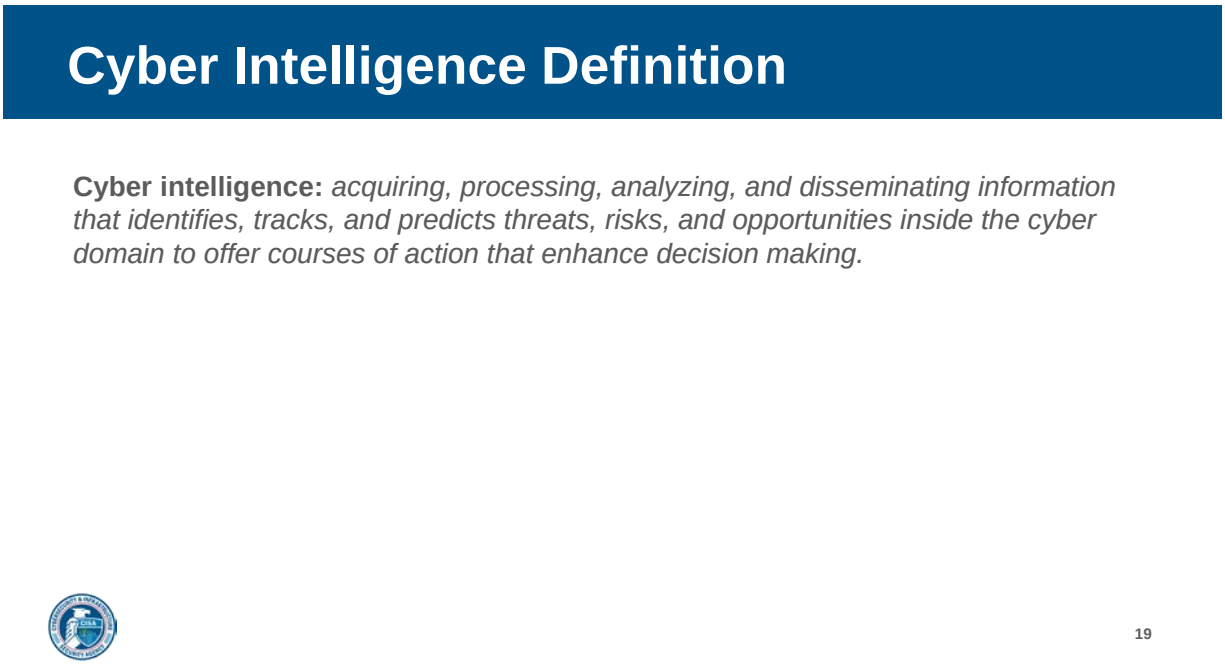
Table of Contents

Cyber Intelligence – Conceptual Framework

Cyber Intelligence – Conceptual Framework

18

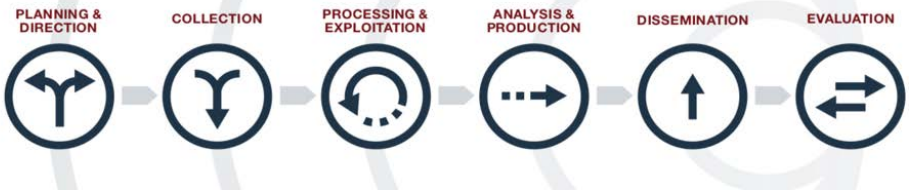
**018 Let's talk about the cyber intelligence conceptual framework.



**019 I put this definition up again as a baseline to help us think about cyber intelligence. As I discuss, it is a process how to create intelligence or a finished product of--or of something that would be considered intelligence. Let's turn to a foundational example in the intelligence cycle that is used by the intelligence community.

Background

- To produce a product or finished intelligence, there needs to be a process through which bits and pieces of information is identified, collected, and analyzed.



20

**020 To produce a product or finished intelligence, there needs to be a process through which bits and pieces of information is identified, collected, and analyzed. The intelligence cycle is a six-step process for developing raw information into finished intelligence for use by policymakers, military commanders, and other consumers in decision-making. The intelligence cycle is an imperfect process that was created during World War II. However, it is a very good process, and it works. It is a good baseline for analysts and organizations to start with and is a framework still used today. Even organizations doing cyber intelligence today use this model or have modified a version of it to fit their organizational needs.

Our recent research with organizations showed some high-performing organizations, government and industry, are using frameworks that are modeled on the traditional intelligence cycle, and and they are successfully incorporating cutting-edge technology into their cyber intelligence programs. These high-performing organizations tend have long established cyber intelligence programs and foster a complete people, processes, and technology approach to cyber intelligence.

In contrast to our 2013 report, which described the traditional intelligence cycle as limited by its linear format, we now assess that the traditional intelligence cycle as an interrelated and non-linear process. In other words, the success and failure of one or more steps in the cycle may spawn a rippling effect on the entire cycle. The traditional intelligence cycle is therefore an acceptable way for organizations to approach cyber intelligence. Our cyber intelligence model, or framework, which I will talk about, in that we offer and believe it is actually a little bit more ideal because it addresses the intersection between cyber and technology.

Version 2: Cyber Intelligence Analytic Framework

**021 This is ultimately what we came up with as the cyber intelligence framework in 2013. This framework is what we submitted to the Director of National Intelligence in 2013, and in our most recent research in 2019, we made some changes in terminology within the cyber intelligence framework. We first introduced the framework, rooted in the traditional intelligence cycle in 2013, with the components environmental context, data gathering, functional analysis, strategic analysis, and decisionmaker reporting and feedback.

To reflect terminology we heard in our most recent interviews, we changed micro-analysis or functional analysis to threat analysis, and macro-analysis is now called strategic analysis. Also, because we heard

time and again from participants whose reporting and feedback practices involved a variety of individuals, especially at the peer level, we changed decisionmaker reporting and feedback to simply reporting and feedback.
So the new cyber intelligence frameworks looks like what you see on this slide.

Notices

Notices