Cyberwarfare Defense Plan  
Part 1: Identifying Supply Chain Security Management Issues and Sources of Threat Information

Truc L. Huynh, Computer Science

Matt Kolter, Computer Science

Purdue University Fort Wayne

**Cyberwarfare Defense Plan  
Part 1: Identifying Supply Chain Security Management Issues and Sources of Threat Information**

Intelligence is collecting, analyzing, and disseminating an adversary's capabilities, plans, intentions, and operations. According to (1), the Intelligence Operations model usually has five steps. They are planning and direction, collection, processing and exploration, analysis and production, and dissemination.

# Phrase 1: Planning and Direction

According to (1), there are several activities to make sure the right plan is created:

* Identify Intelligent requirement: the subject that needs information collection:
  + Priority Intelligent Requirements (PIRs): Question by decision-makers
  + Essential Elements of Information (EEIs): specific pieces of information that can answer the priority intelligent requirements.
* Develop an intelligence architecture: identify the systems and processes that will be used later in this plan
* Prepare a collection plan: identify methods that will be used to gather the essential elements of information
* Issue requests to collectors: orders are issued to intelligent collectors based on the collection plan

# Collection

Intelligent professionals gather the essential elements of information (EEIs). The types of assets used during the collection Phrase “depend upon the specific information request made by decision-makers and the availability of appropriate assets” (1).

# Processing and Exploration

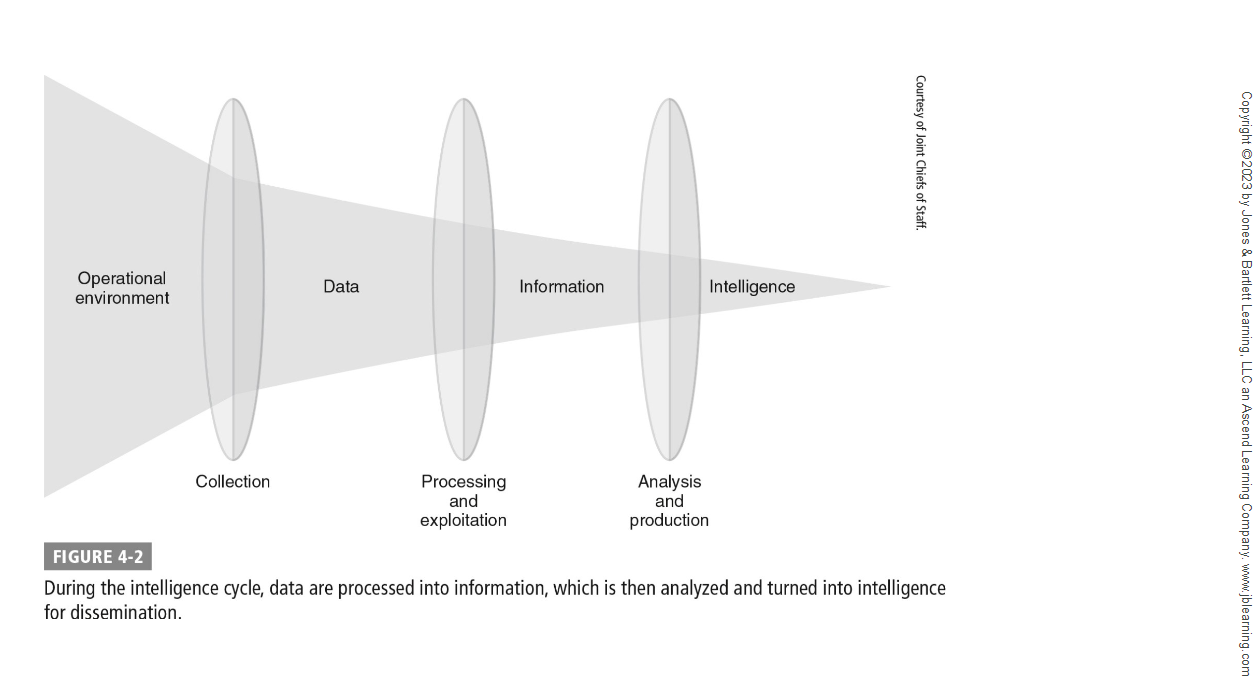
Data collected by intelligence assets must be transformed into information that analysts may use. E.g., Decrypt encrypted data, convert raw data into viewable content, and translated collected data from one language to another (Chapple & Seidl, 2022).

# Analyst and Production

Analysts must interpret information and develop an assessment that satisfies the priority intelligence requirement (PIR). Analysts must make a judgment about the reliability of the information from all the sources even though they may have conflicts (Chapple & Seidl, 2022).

# Dissemination

Delivery of finished intelligence products to the decision-makers who made the requests. Recipients of intelligence products integrate information into their own processes (Chapple & Seidl, 2022).



References

Chapple, M., & Seidl, D. (2023). Chapter 4: Intelligent Operations. In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 9–20). essay, Jones & Bartlett Learning. (1)