Cybersituational Awareness - Appunti

Francesco Lorenzoni

Febrero 2025

Contents

Part I

Introduction to ACG

Chapter 1

Ciberconciencia Situacional

There are tasks (tareas) each monday. Each monday the lectures are asynchronous, and a task if given which lasts one or two weeks. The tarea may be commited by email if the deadline expires but it is preferrable to finish in time.

1.1 Introducción

1. Conciencia Situacional
   i. Situational Awareness
   ii. Situational Awareness in Physical World
   iii. Situational Awareness in Cyberspace
2. Visualización
   i. Cyberintelligence Visualization
   ii. Visualization Charts
3. Herramientas de ciberconciencia situacional
   i. Cybersituational Awareness Tools
   ii. Sources on Intelligence
   iii. Risk and Consequences Analysis
4. Conciencia situacional hibrida
   i. Hybrid situational awareness
   ii. Cyber-Hybrid Situational Awareness Tools
5. Seguridad de sistemas ciberfisicos y protección de infraestructuras críticas
   i. Cyber-Physical Systems (CPS)
      Un CPS es un sistema que tiene una parte cibernética y otra física. Así de sencillo, según el prof. Esteve.
   ii. CPS Vulnerabilities
   iii. Industrial Control Systems Cyberdefense
   iv. Critical Infrastructure Protection

"Ciberconciencia situational significa *Saber lo que està pasando en el ciberspacio"* — Manuel Esteve

Un punto fundamental para saber lo que està pasando en el ciberspacio es la **visualización**. La visualización es una herramienta fundamental para la ciberconciencia situacional. En otras palabras, es necesario cabir lo que es importante que se visualice sobre el monitor pantalla ("videowall") y lo que no.

1.2 Conciencia Situacional

Definition 1.1 (Situational Awareness) *Situational awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*

Está también otra definición de conciencia situacional, que se encuentra en el *United States Army Field* manual:

Definition 1.2 (Situational Awareness - II) *Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, competitive and other operations within the battlespace in order to facilitate decision making. An informational perspective and skill that fosters an ability to determine quickly the context and relevance of events that are unfolding*

Ambas definiciones pueden adaptarse al contexto cyber de Internet. De aquí se deriva la definición de *Cyber* Situational Awareness dada anteriormente "saber lo que está pasando en el ciberspacio". Hay otras definiciones también:

Definition 1.3 (Cyber Situational Awareness) *Comprehensive cyber situation awareness involves three key areas: computing and network components, threat information, and misison dependencies*

MITRE

Definition 1.4 (Cyber Situational Awareness) *Gathering real-time information about an organization's computer networks in order to provide an effective response to an attack*

Computer Language Dictionary

1.2.1 Situation Understanding

Definition 1.5 (Situation Understanding) *Understanding involves having a sufficient level of knowledge to be able to draw inferences about the possible consequences of the situation, as well as sufficient awareness of the situation to predict future patterns*

Note that the following concepts related with situational awareness and are "similar" but they are not the same:

- ◇ Data
- ◇ Information
- ◇ Perceptions
- ◇ Intelligence
- ◇ Knowledge

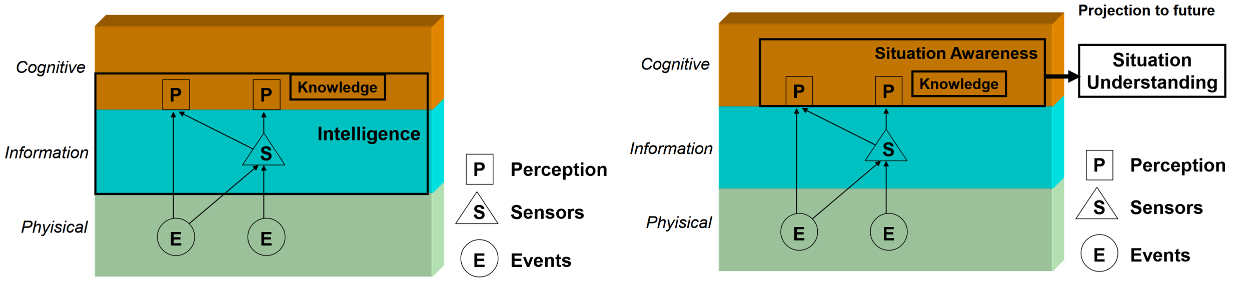

Figure 1.1: Producing Cyber Situational Awareness

1.2.2 Situational Awareness in Cyberspace

Cyber situational awareness involves three areas:

1. Networks and systems - *Network Awareness*
2. Threats and incidents (including APT and any other kind of attacks) - *Threat Awareness*
3. Fullfillment of the mission - *Mission Awareness*

- ◇ Network awareness:
  - – Assets and configuration management
  - – Vulnerabilities auditing
  - – Patch management
  - – Sharing of incident awareness
- ◇ Threat awareness
  - – Internal incidents and suspicious behavior tracking
  - – Knowledge of external threats, by mean of intelligence activities
  - – HUMINT, OSINT, SIGINT)
  - – Share threat intelligence with goverment organizations (CERTs) or industry associations
- ◇ Mission awareness:
  - – Develop a Common Operational Picture to understand all dependences and components to operate/develop missions in cyberspace
  - – Select the best response deccisions during incident management
  - – Risk assesment before any response task execution
  - – Find out mission impact during forensic analysis, after incident
  - – Ellaborate defense plannig for future incidents management

Situational awareness can be generated at three traditional military command and control **levels**:

1. **Tactical**
   The main goal at this level is to visualize and take care of events and situations related with assets. Sometimes this is called also *Technical level*

2. **Operational**
   Main goal at this level is to summarize tactical level details and putting them in context of impact to organization misión.
3. **Strategical**

Es fundamental cabir que la ciberconciencia situational se puede costruir a partir desde cuatro fuentes de información de cyber intelligence techniques:

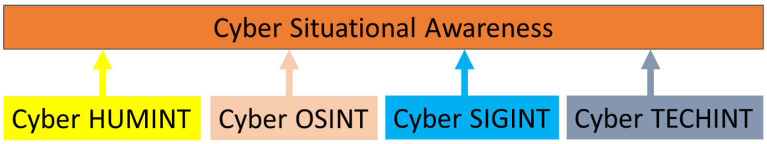

Figure 1.2: Cyber intelligence techniques

- Cyber `HUMINT` - Human Intelligence, una fuente de información, por ejemplo, son *usuarios*, que proporcionan información sobre los seres humanos
- Cyber `OSINT` - Open Source Intelligence
- Cyber `SIGINT` - Signal Intelligence
- Cyber `TECHINT` - Technical Intelligence