

Dynamic System Modeling for Threat Analysis





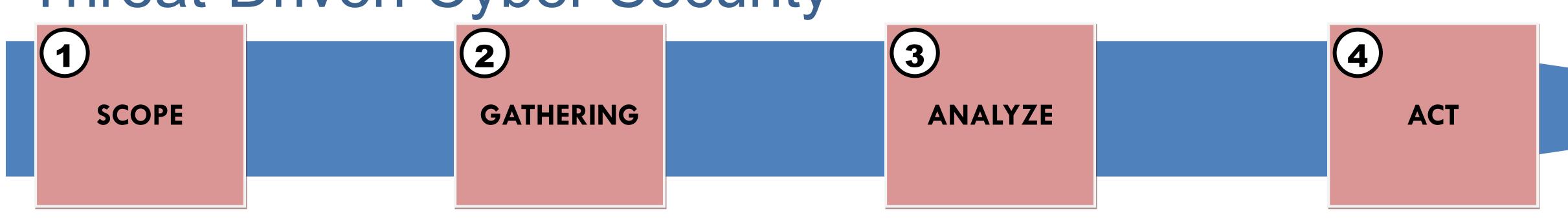
sources.

Tithnara N. SUN, Ciprian TEODOROV, Joël CHAMPEAU & Philippe DHAUSSY ENSTA Bretagne, 2018



Contact: tithnara.sun@ensta-bretagne.org

Threat-Driven Cyber Security



- of the Gather information relevant to Correlate the gathered pieces Make intelligence analysis. Exhibit the system, the defined scope. attack surface, and critical re-
- of information to **identify** the threats, vulnerabilities and potential attacks.
- decisions and take action against the threats.

Dynamic Attack-Defense Model-

How to model and build a dynamic simulation of a running system in a cyber security context ie in an environment where threat actors evolve?

Attack Surface Reification

identification Concepts and description. Relevant structures and abstractions choices.

Dynamic Model

Lifecycle of the system. Temporal dimension, interactive system and evolving attackers and defenders.

Implementation & Simulation

Runnable and non-cyber-agentuser-friendly simulation. Compatibility with other security tools.

First Model Power Source Power Interface Cyber System Controller User Interface Point of view Action range Cyber Actuator Cyber Sensor Structural Interface Structural Interface Actuator Sensor **Game Theory** Physical Process

Cyber Physical System: Group of interacting entities. Target of the attackers. Definition in an environment.

Actor: Attacker or defender of the system. Interactions with the system through an evolving point of view and action range.

Actions: Available evolution attempts of an actor's interactions with the system. Both textual and graphical (modification, insertion, deletion)

Research Directions

Cyber Threat Intelligence Cyber-related vocabulary **Operational Design** Military operation planning

Embedded Systems

Cyber physical system modeling

Attack Trees

Step-by-step attack modeling **Model-Checking** Formal verification method

Multiplayer scenarii modeling

Temporal Graphs

Evolving data structure

Automata

Conditional state-machines

Composite Structure