Thèse ModMenace
Avancement & perspectives

Tithnara Nicolas SUN

Philippe Dhaussy (Lab-STICC)
Lionel Van Aertryck (DGA-MI)
Ciprian Teodorov (Lab-STICC)
Joel Champeau (Lab-STICC)

Sommaire

- Réification de la surface d'attaque
  - Définitions
  - Arbres d'attaque
  - Cyber Threat Intelligence
  - STIX
- Point de vue dynamique
  - Théorie des jeux…
  - …appliquée à la Cyber
  - Perspectives
- Moteur d'exécution
  - Ebauche de concept

Introduction
Sujet de thèse

- ModMenace – Modèle système dynamique pour l'analyse de la menace
- Axes de recherche étudiés jusqu'ici :

Réification de la surface d'attaque

Aspect dynamique

Partie I : Réification de la Surface d'Attaque

A)Définitions

B)Arbres d'attaque

C)Cyber Threat Intelligence

D)STIX

Définitions

Surface d'attaque :

Ensemble des **points d'entrée** et des **points de communication** qu'un système possède avec l'extérieur.[1]

Zone de contention entre l'attaquant & la défense.

[1] Analyse et réduction de la surface d'attaque / Mickael Dorigny / https://www.information-security.fr/ / 19 Décembre 2015

Définitions

Attaquant, Threat Actor, Adversaire :

Entité ayant pour objectif de **nuire** au système. [2][3]

Vulnérabilité, Faille :

Erreur ou **faiblesse** de conception, d'implémentation ou de fonctionnement. [2][3]

[2] Towards Threat, Attack, and Vulnerability Taxonomies / Dennis Hollingworth / Network Associates laboratories USA / 2003
[3] Trust in Cyberspace / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999

Définitions

Menace, Threat :

Adversaire motivé et capable d'**exploiter** une **vulnérabilité**. [2][3]

Définition ambiguë : Expression d'une intention de nuire / Indication d'une telle intention.

Attaque, Incident :

Acte malveillant, moyen [séquence d'actions] d'exploiter une vulnérabilité. [2][3]

Partie I : Réification de la Surface d'Attaque

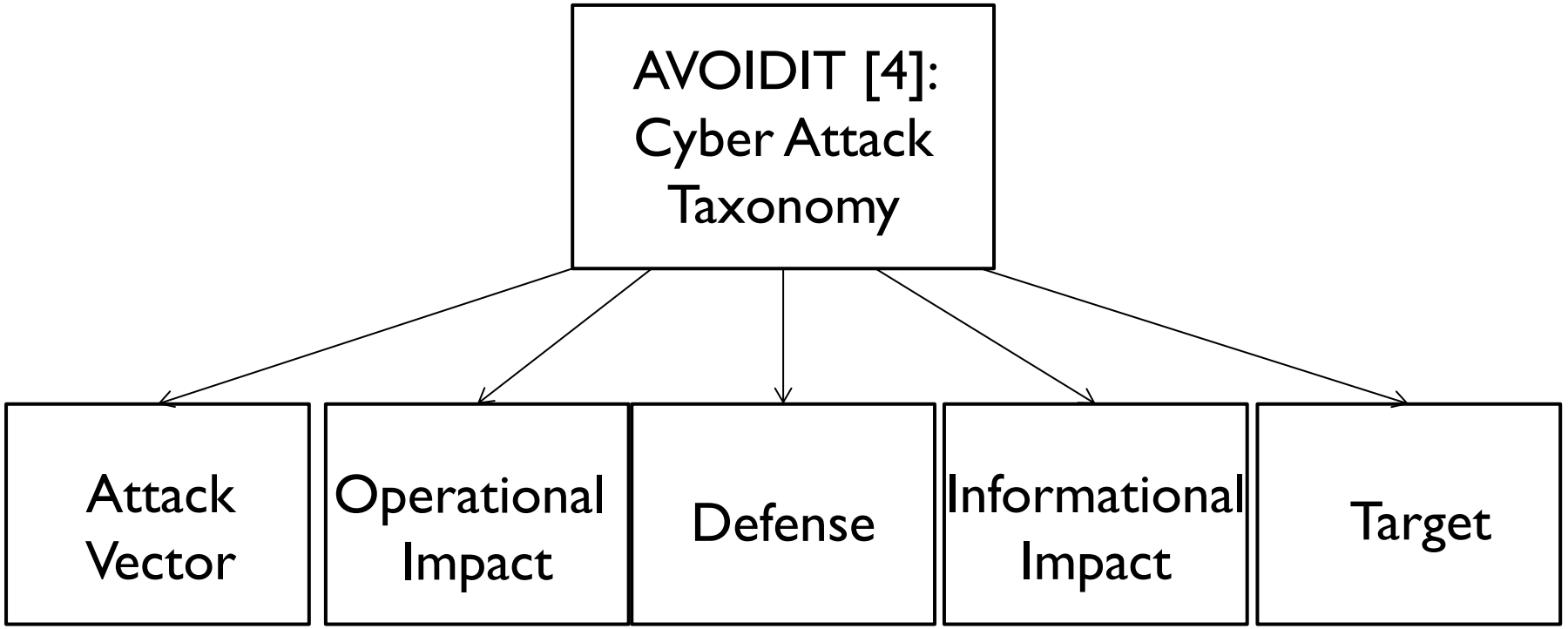
A) Définitions

B) Arbres d'attaque

C) Cyber Threat Intelligence

D) STIX

Arbres d'Attaque

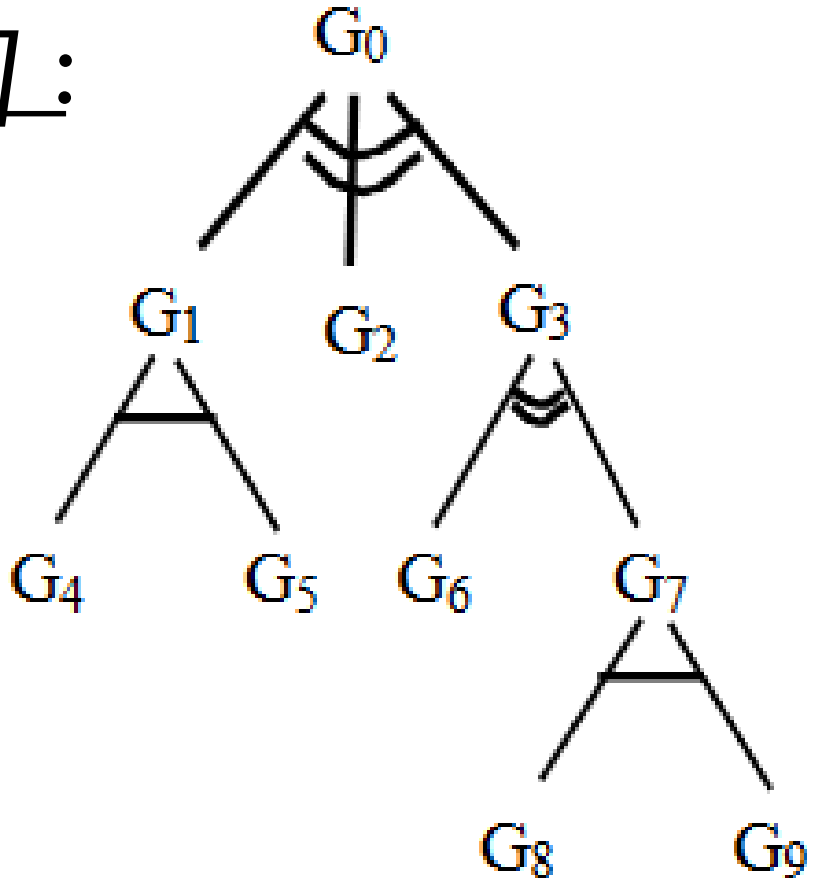


[4] *AVOIDIT : A Cyber Attack Taxonomy* / Chris B. Simmons, Sajjan G. Shiva, Harkeerat Bedi, Dipankar Dasgupta / University of Memphis, Memphis, Tennessee, USA / Juin 2014

Arbres d'Attaque

Arbres d'Attaque [5] :

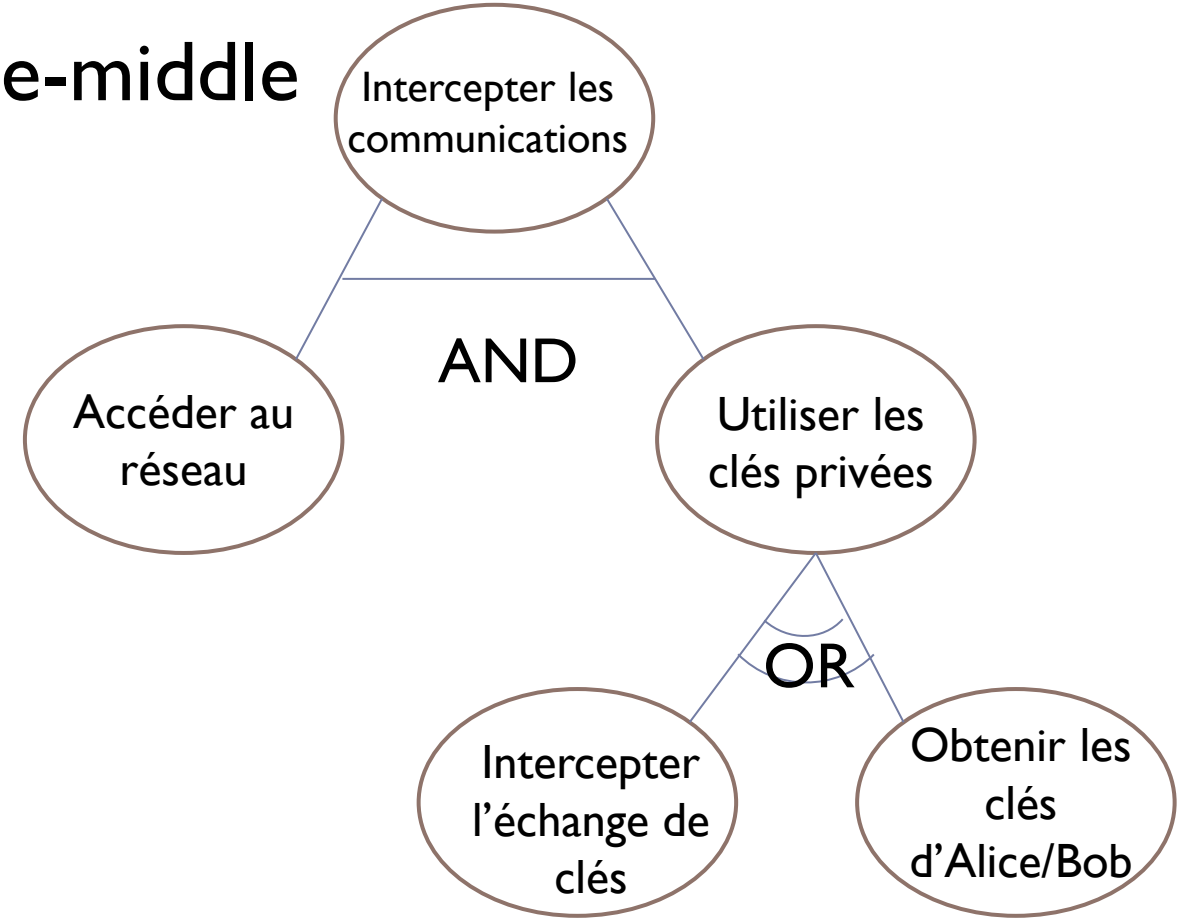
- Nœud = Objectif
- Racine = Objectif principal
- Nœud interne
  - Condition AND
  - Condition OR



[5] *Attack Modeling for Information Security and Survivability* / Andrew P. Moore, Robert J. Ellison, Richard C. Linger/ Software Engineering Institute, Carnegie Mellon University, USA / Mars 2001

Arbres d'Attaque

- Man-in-the-middle



Partie I : Réification de la Surface d'Attaque

A)Définitions

B)Arbres d'attaque

C)Cyber Threat Intelligence

D)STIX

Cyber Threat Intelligence

Cyber Threat Intelligence :

Connaissance sur les **adversaires**, leurs **motivations**, leurs **intentions** et leurs **méthodes**, **collectée**, **analysée** et **partagée** entre différents agents à différents niveaux pour protéger les biens critiques. [6]

[6] *Definitive Guide to Cyber Threat Intelligence* / Jon Friedman, Mark Bouchard, CISSP / CyberEdge Group Annapolis, USA / 2015

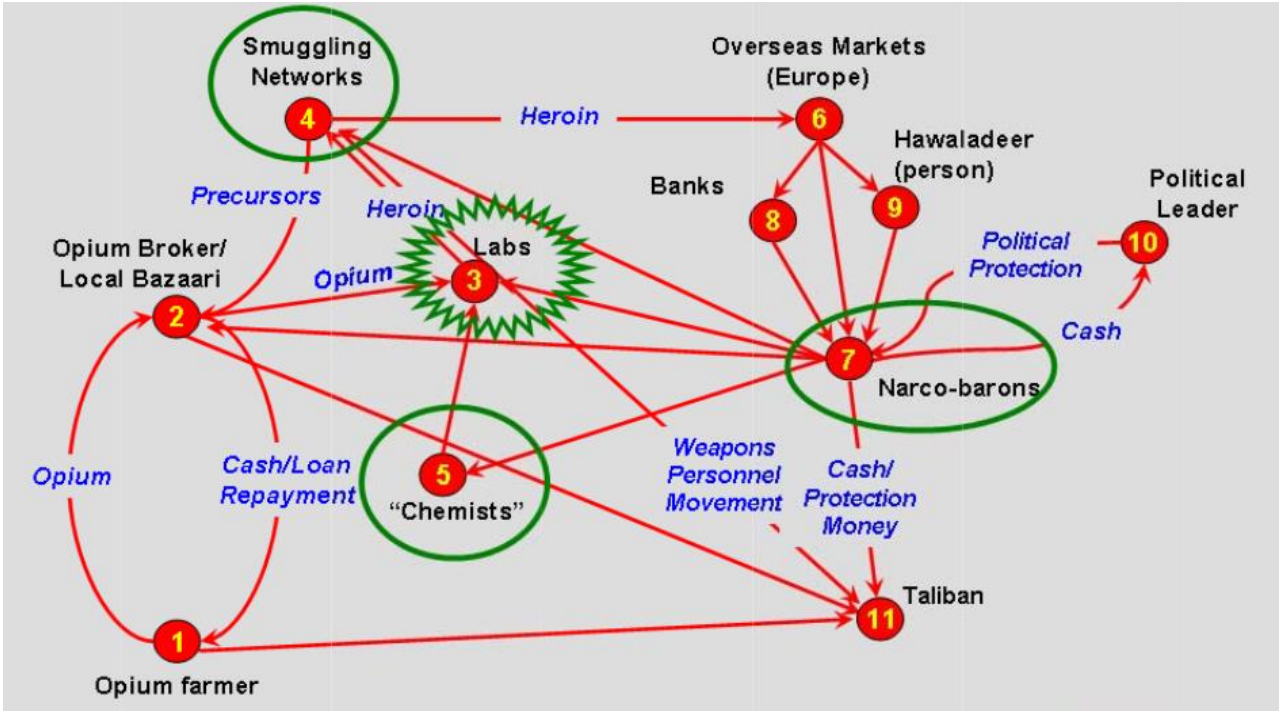
Cyber Threat Intelligence

Trois niveaux de guerre [7]

[7] *Redefining the Center of Gravity* in *Joint Force Quarterly (JFQ) issue 59* / Dale C. Eikmeier / Washington D.C. USA / 2010

Cyber Threat Intelligence

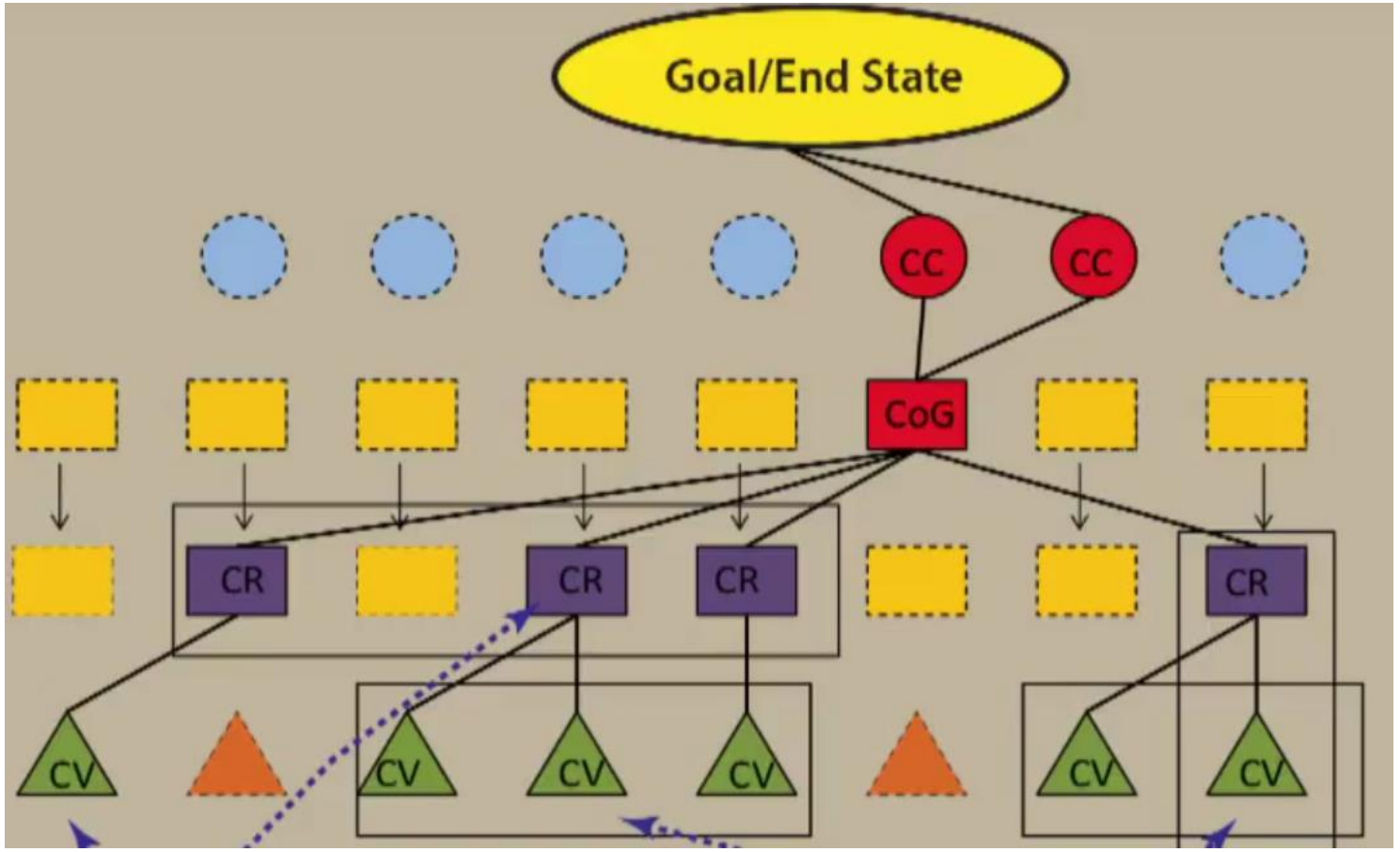
- **RAFT** [7]
  - **R**elations
  - **A**cteurs
  - **F**onctions
  - **T**ensions



Cyber Threat Intelligence

- **CoG (Center of Gravity)** : L'entité principale qui possède la **capacité intrinsèque** de **parvenir** à l'**objectif** du système [7]
- Cible de l'attaquant
- Approche efficace en ressource

- Méthodologie d'identification du CoG [7]



Partie I : Réification de la Surface d'Attaque

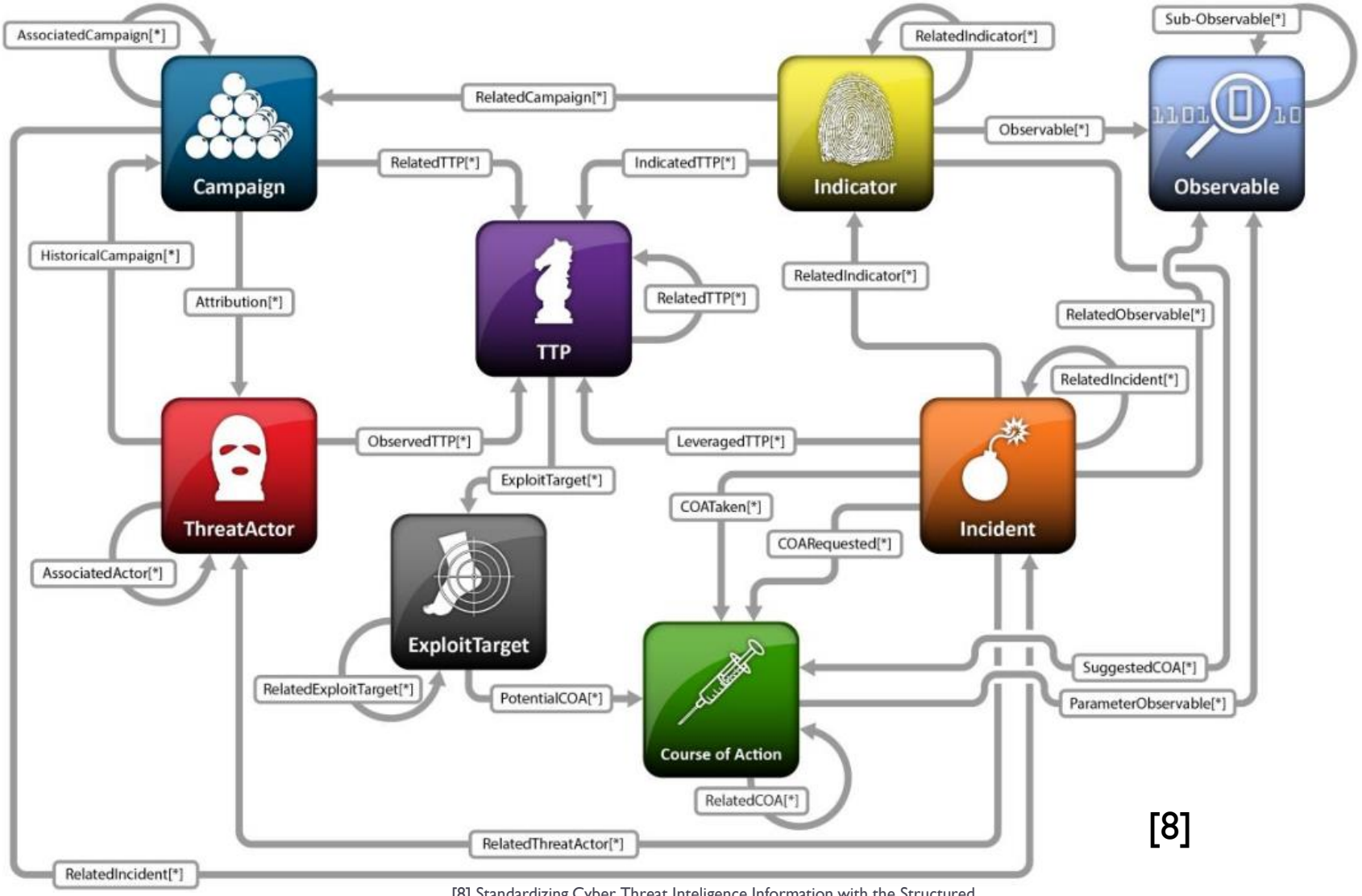
A)Définitions

B)Arbres d'attaque

C)Cyber Threat Intelligence

D)STIX

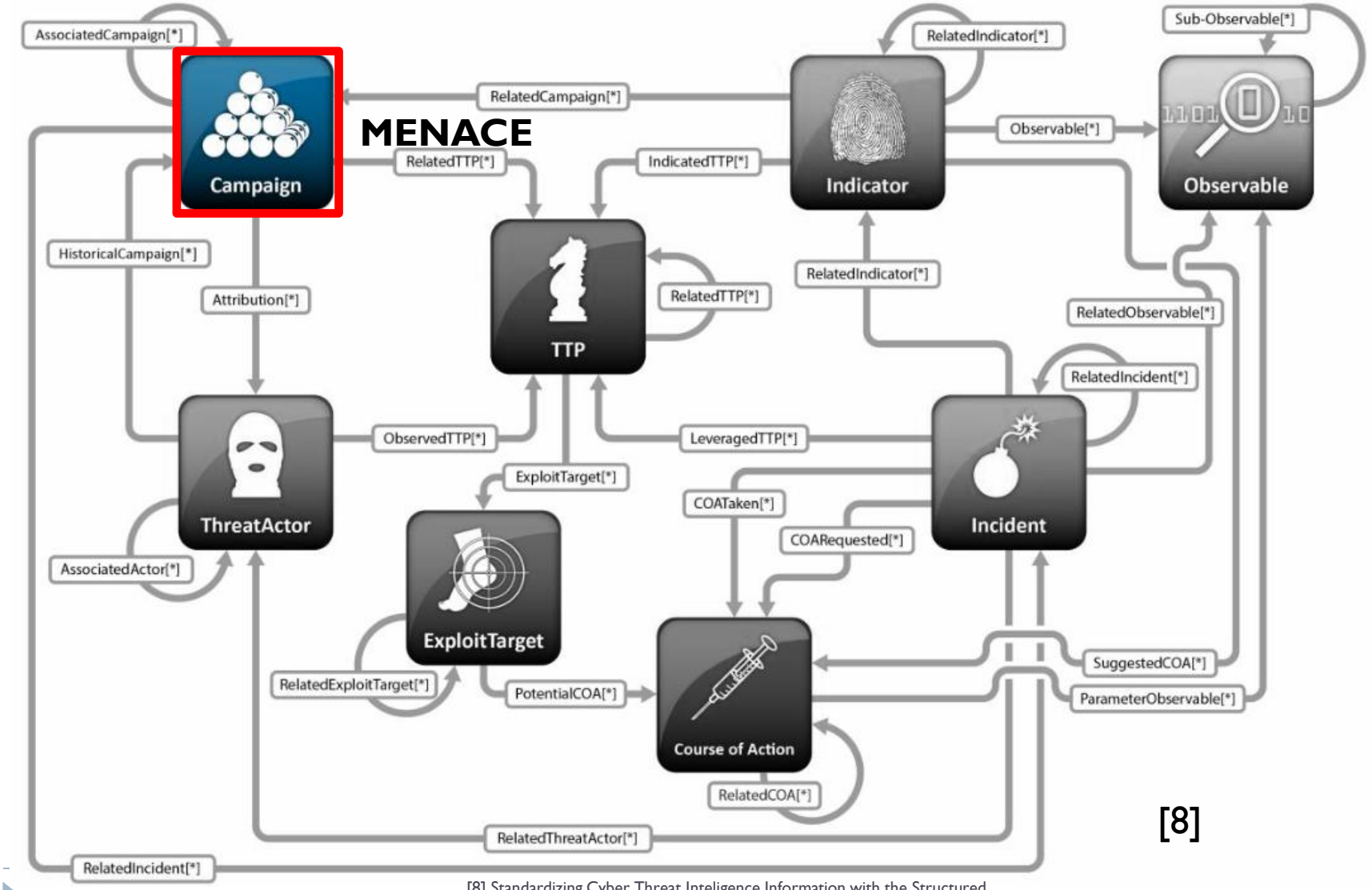
STIX



[8]

[8] Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX) / Sean Barnum / The MITRE Corporation / 20 Février 2014

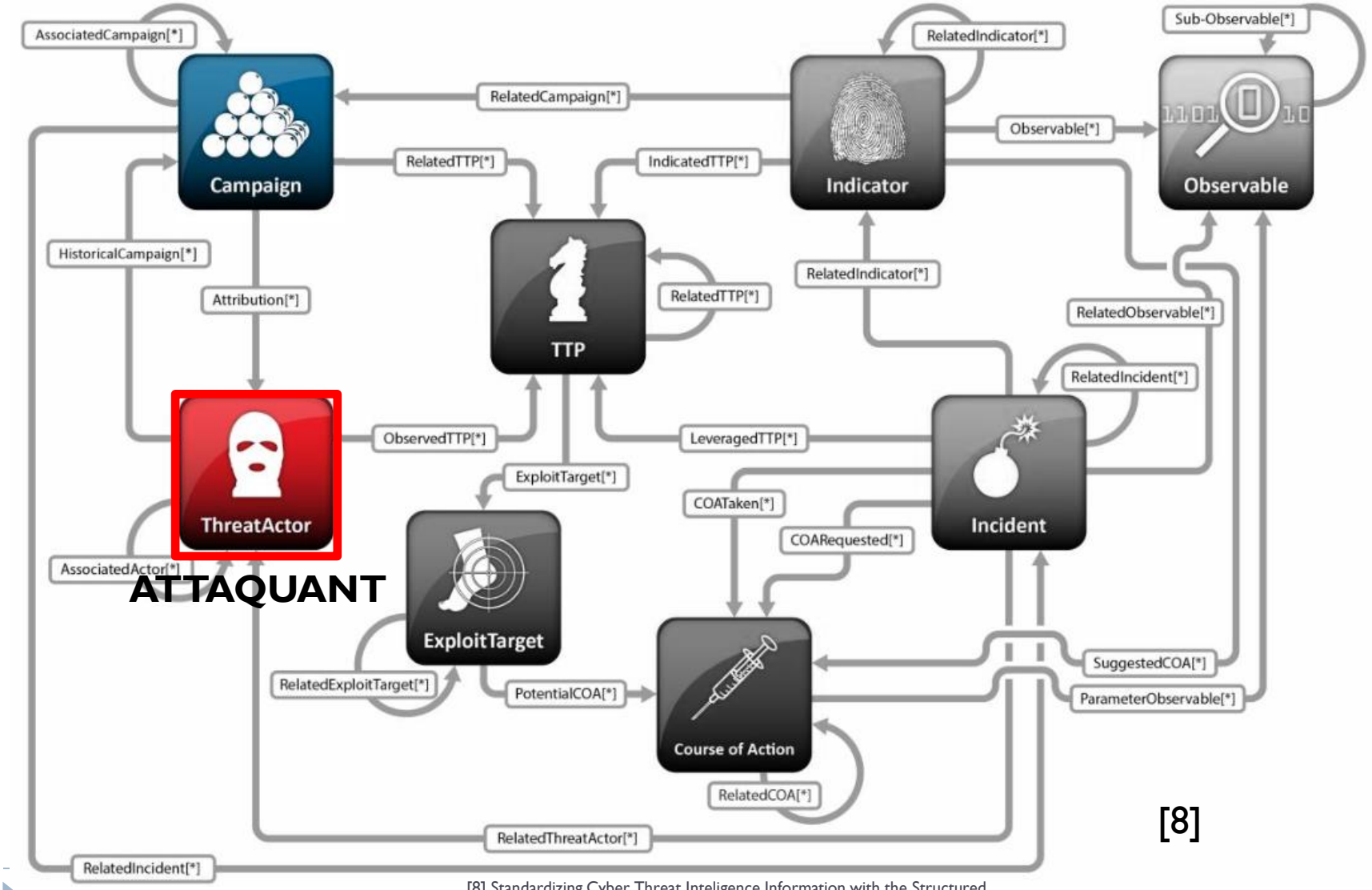
STIX



[8]

[8] Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX) / Sean Barnum / The MITRE Corporation / 20 Février 2014

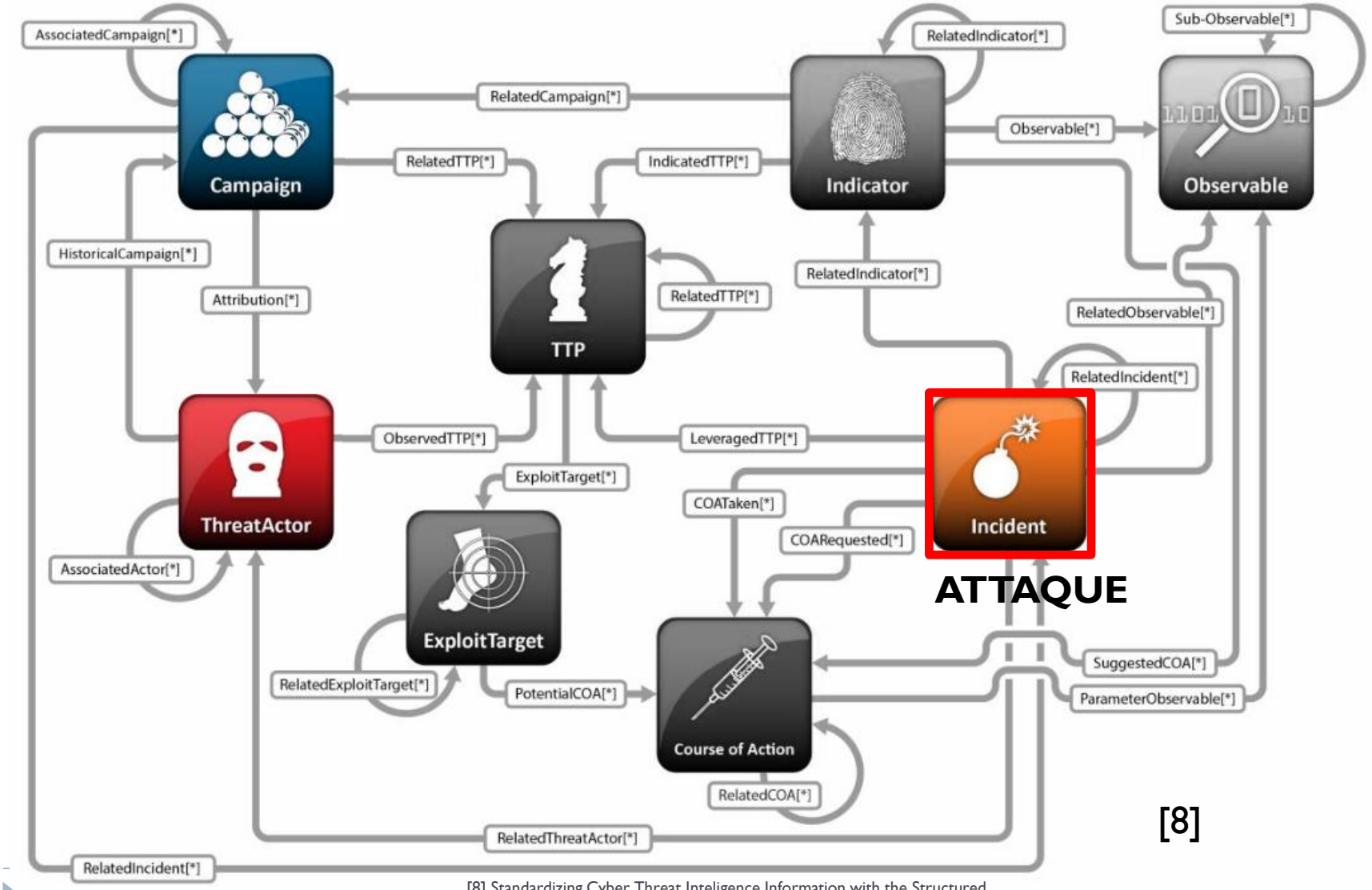
STIX



[8]

[8] Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX) / Sean Barnum / The MITRE Corporation / 20 Février 2014

STIX



[8]

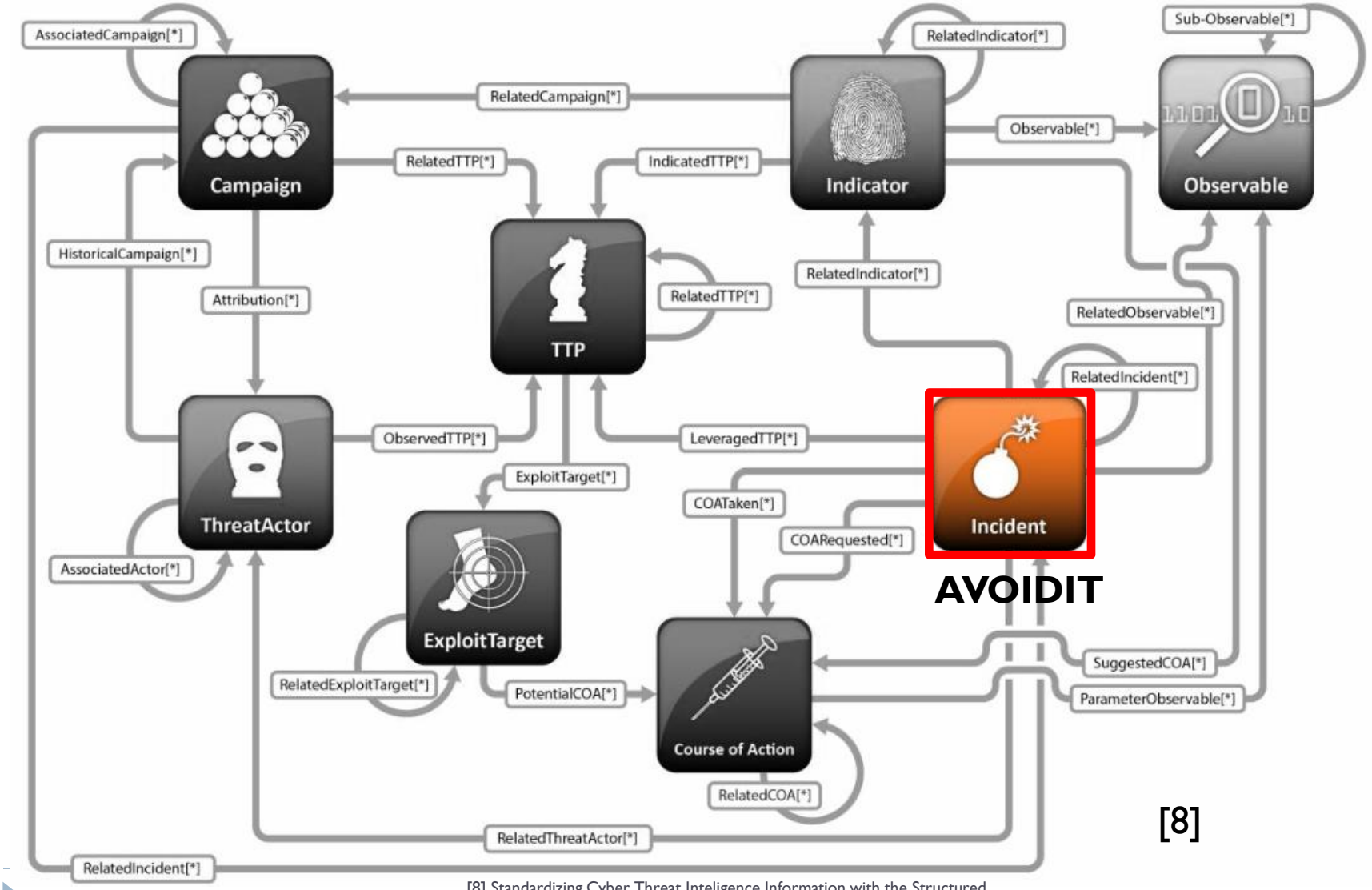
[8] Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX) / Sean Barnum / The MITRE Corporation / 20 Février 2014

STIX

[8]

[8] Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX) / Sean Barnum / The MITRE Corporation / 20 Février 2014

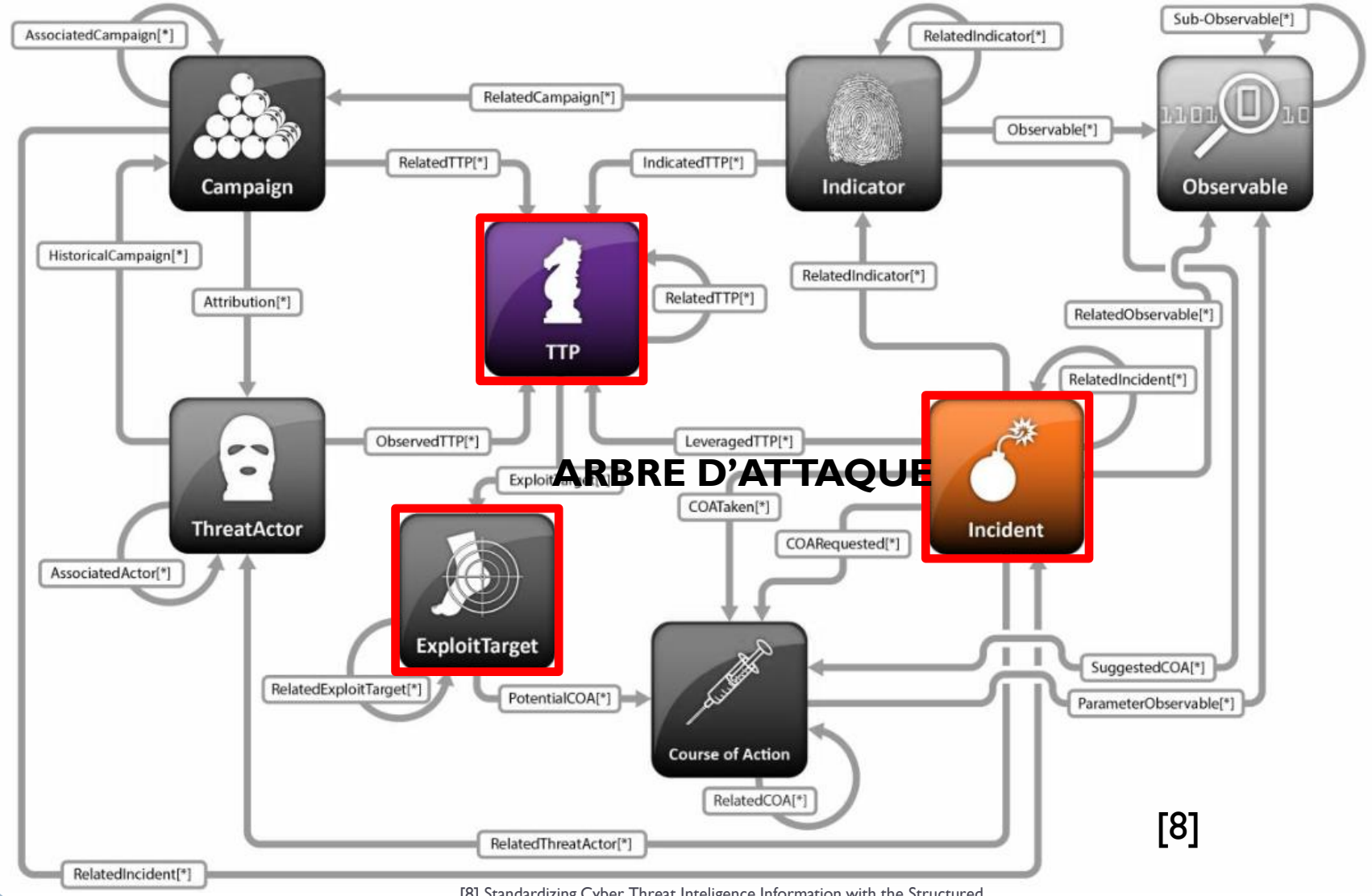
STIX



[8]

[8] Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX) / Sean Barnum / The MITRE Corporation / 20 Février 2014

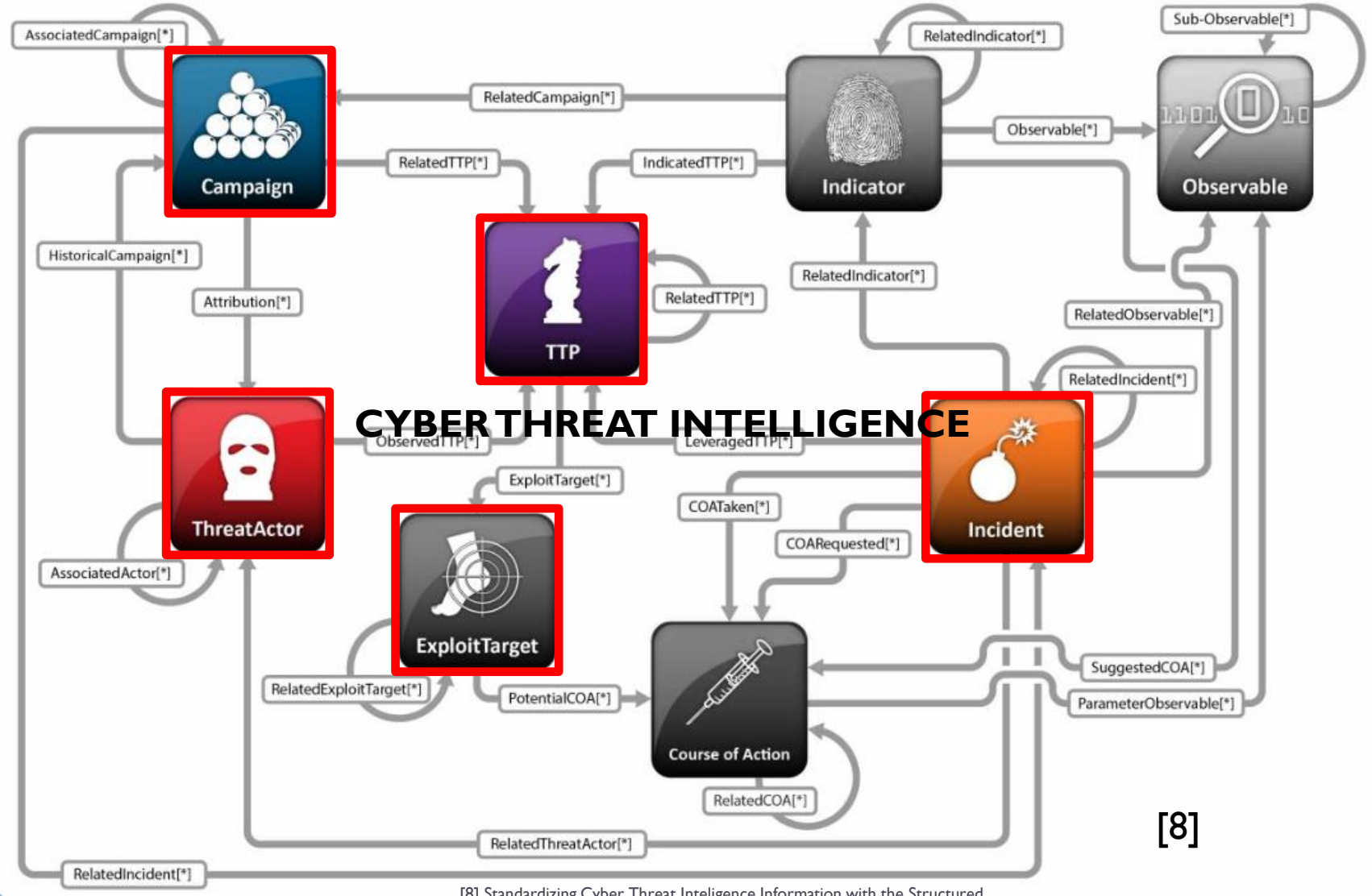
STIX



[8]

[8] Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX) / Sean Barnum / The MITRE Corporation / 20 Février 2014

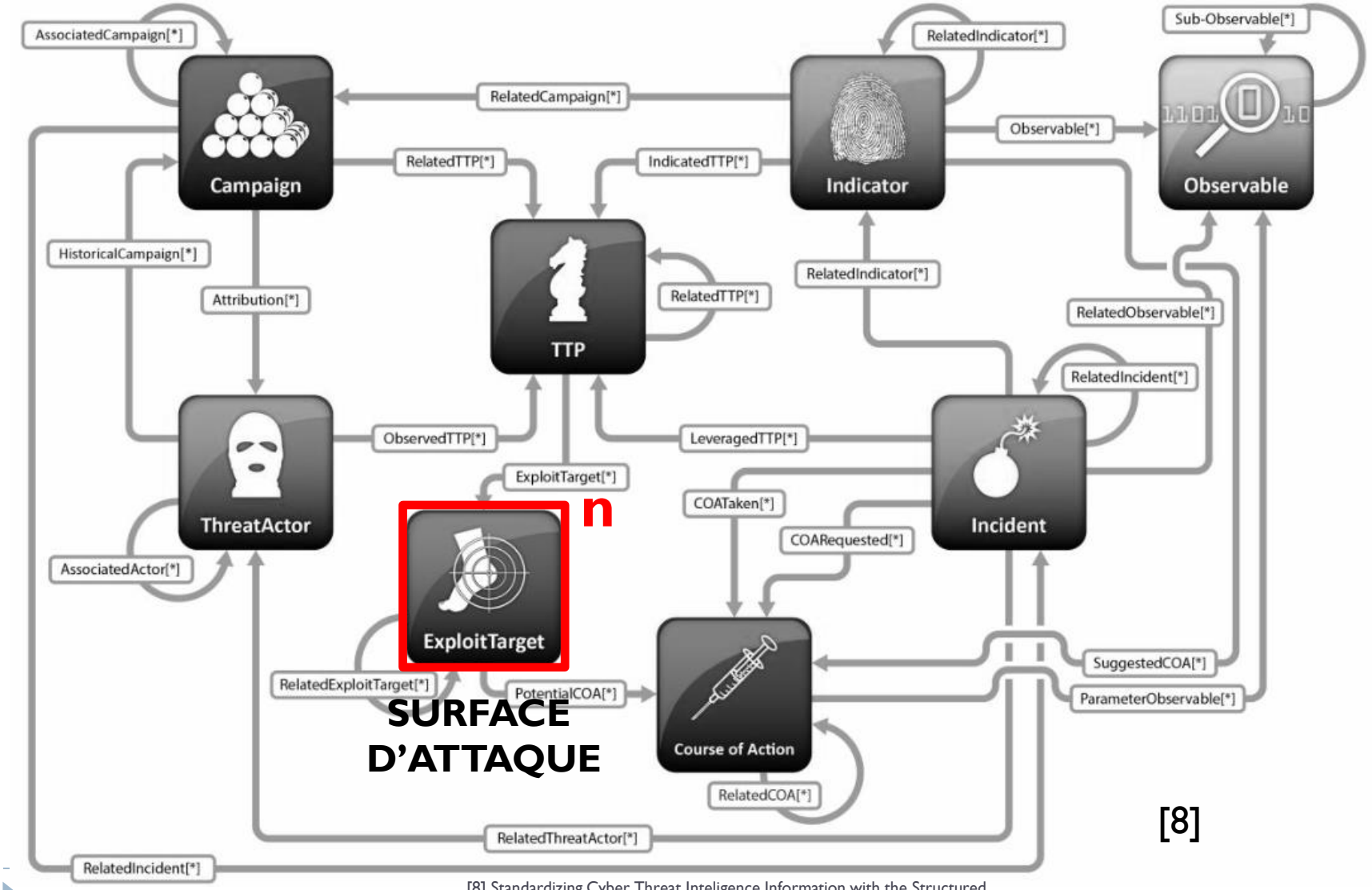
STIX



[8]

[8] Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX) / Sean Barnum / The MITRE Corporation / 20 Février 2014

STIX



SURFACE D'ATTAQUE

[8]

[8] Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX) / Sean Barnum / The MITRE Corporation / 20 Février 2014

Partie II : Point de Vue Dynamique

A)Théorie des jeux…

B)…appliquée à la Cyber

C)Perspectives

Théorie des jeux

Théorie des jeux [9] :

Domaine mathématique s'intéressant aux **problèmes de décisions** entre **différents joueurs** qui sont conscients de leurs **interactions**. Tous les joueurs sont supposés rationnels.

Jeu :

Ensemble de stratégies et de gains de tous les joueurs.

[9] *CyberWar Games: Strategic Jostling Among Traditional Adversaries* / Sanjay Goel, Yuan Hong / University of New York, New York, USA / 2015

Théorie des jeux

Gain :

Fonction numérique évaluant l'état du jeu.

- ***Jeu à somme nulle*** : le gain d'un joueur est l'exact opposé de celui des autres joueurs.
- ***Jeu à somme constante*** : la somme des gains de tous les joueurs est constante.
- ***Jeu à somme non-nulle*** : le gain n'est soumis à aucune restriction structurelle.

Rationalité :

Choix optimal dans le cadre d'une connaissance parfaite et complète.

Théorie des jeux

Information complète :

Le joueur **connait** l'identité des autres joueurs et les gains associés à la stratégie qu'ils adoptent.

Information parfaite :

Le joueur est capable d'**observer** la stratégie des autres joueurs.

Jeu Bayésien :

Modèle de jeu **probabiliste** dans un cadre d'information incomplète.

Dilemme des prisonniers :

A\B	B reste silencieux (Coopération)	B parle (Trahison)
A reste silencieux (Coopération)	(1,1)	(5,0)
A parle (Trahison)	(0,5)	(3,3)

Partie II : Point de Vue Dynamique

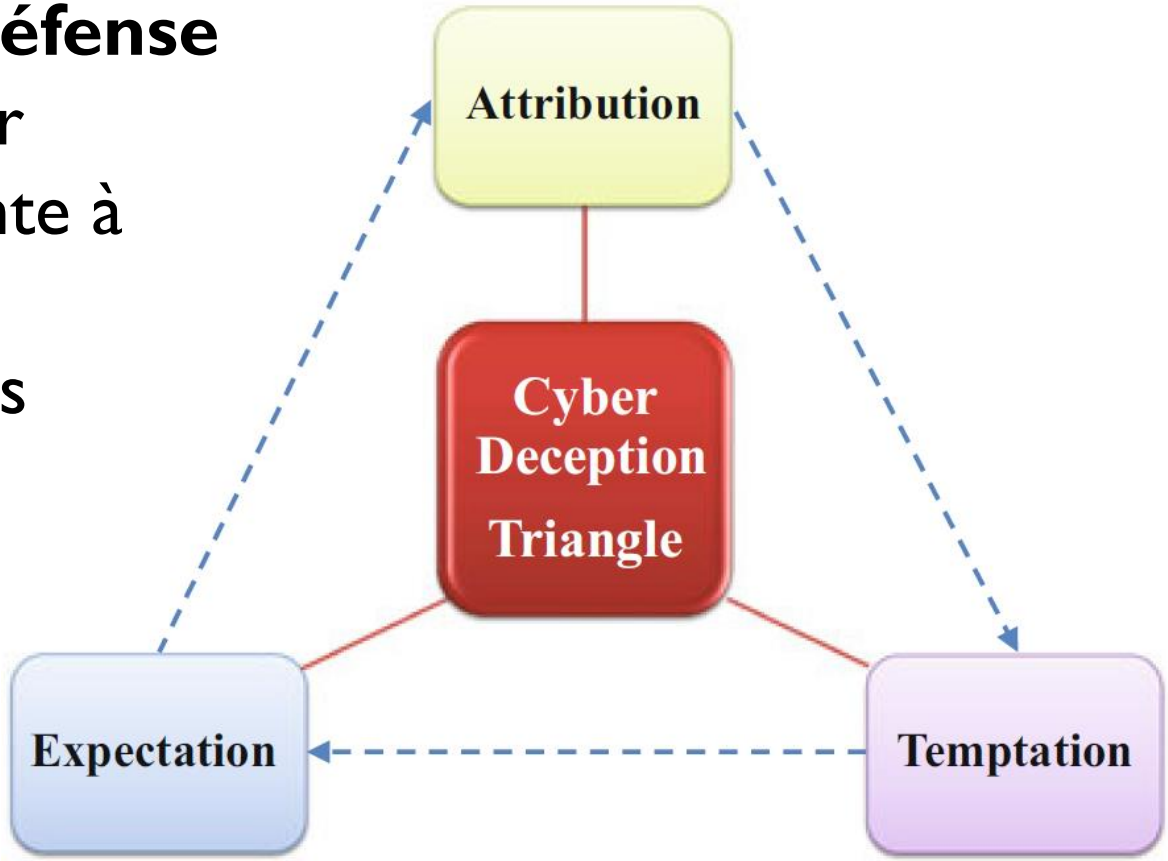
A) Théorie des jeux…

B)…appliquée à la Cyber

C) Perspectives

Exemple : Defense-by-Deception

Mécanisme de défense qui vise à renverser l'asymétrie inhérente à la cyberguerre notamment par des **leurres**. [10]



[10] *Attribution, Temptation, and Expectation : A Formal Framework for Defense-by-Deception in Cyberwarfare* / Ehab Al-Shaer, Mohammad Ashiqur Rahman / University of North Carolina, Charlotte, USA / 2015

…appliquée à la Cyber

Honeypot :

Machine factice introduite dans le système afin de pouvoir observer le comportement d'un attaquant et/ou le mener sur une fausse piste. [11]

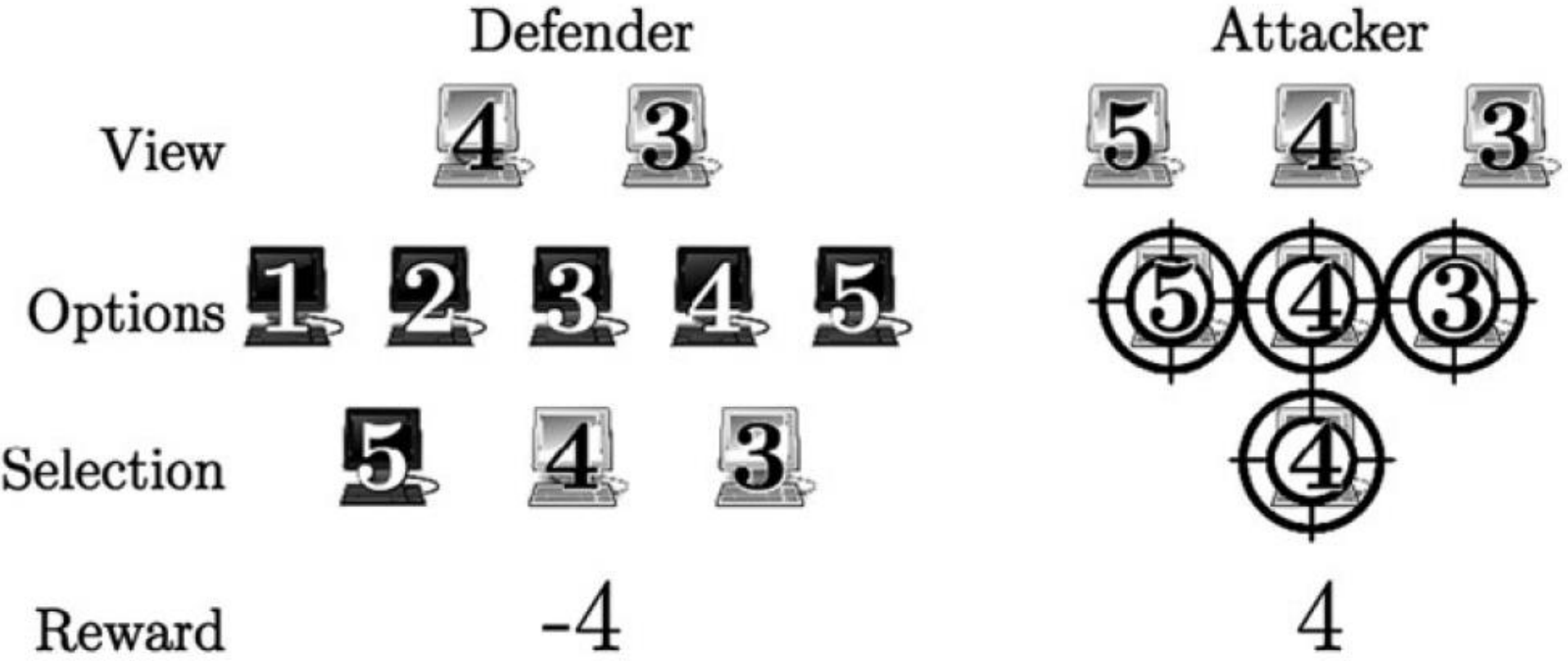
Domaine cyber :

Jeu à connaissance incomplète & imparfaite, à somme nulle.

=> Modélisation bayésienne

[11] *Game-Theoretic Foundations for the Strategic Use of Honeypots in Network Security* / Christopher Kiekintveld, Viliam Lisý, Radek Píbil / University of Texas, El Paso, USA / Czech Technical University, Prague, Czech Republic / 2015

…appliquée à la Cyber



Exemple de modèle de jeu [11]

…appliquée à la Cyber

Défense\Attaque	Vrai 3	Vrai 4	Honeypot
Honeypot 1			
Honeypot 2			
Honeypot 3			
Honeypot 4			
Honeypot 5			

…appliquée à la Cyber

Défense\Attaque	Vrai 3	Vrai 4	Honeypot
Honeypot 1	(-3,3)		
Honeypot 2	(-3,3)		
Honeypot 3	(-3,3)		
Honeypot 4	(-3,3)		
Honeypot 5	(-3,3)		

…appliquée à la Cyber

Défense\Attaque	Vrai 3	Vrai 4	Honeypot
Honeypot 1	(-3,3)	(-4,4)	
Honeypot 2	(-3,3)	(-4,4)	
Honeypot 3	(-3,3)	(-4,4)	
Honeypot 4	(-3,3)	(-4,4)	
Honeypot 5	(-3,3)	(-4,4)	

…appliquée à la Cyber

Défense\Attaque	Vrai 3	Vrai 4	Honeypot
Honeypot 1	(-3,3)	(-4,4)	(1,-1)
Honeypot 2	(-3,3)	(-4,4)	(2,-2)
Honeypot 3	(-3,3)	(-4,4)	(4,-4)
Honeypot 4	(-3,3)	(-4,4)	(5,-5)
Honeypot 5	(-3,3)	(-4,4)	(2,-2)

Partie II : Point de Vue Dynamique

A) Théorie des jeux…

B) …appliquée à la Cyber

C) Perspectives

Perspectives

- Stratégie de Defense-by-Deception
- Cyber Counterdeception
- Automated Adversary Profiling[12]

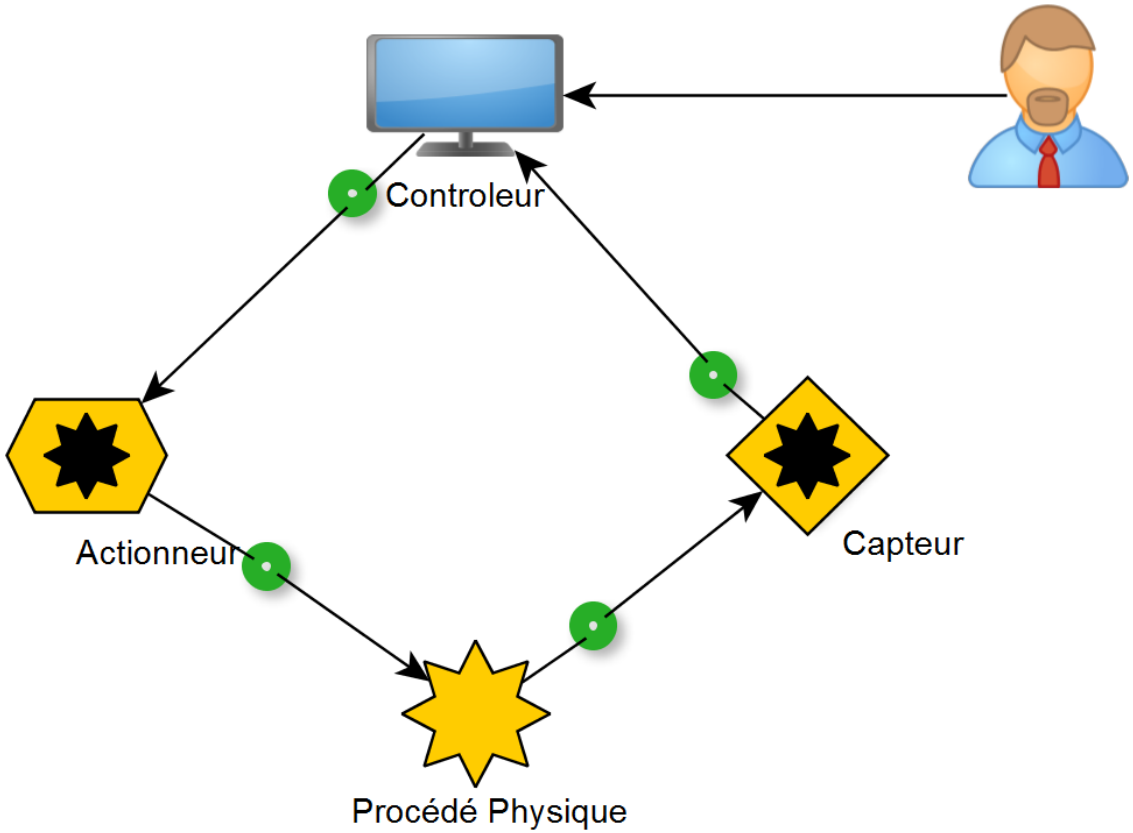
[12] *Automated Adversary Profiling* / Samuel N. Hamilton / Siege Technologies, Manchester, USA / 2015

Partie III : Moteur d'exécution

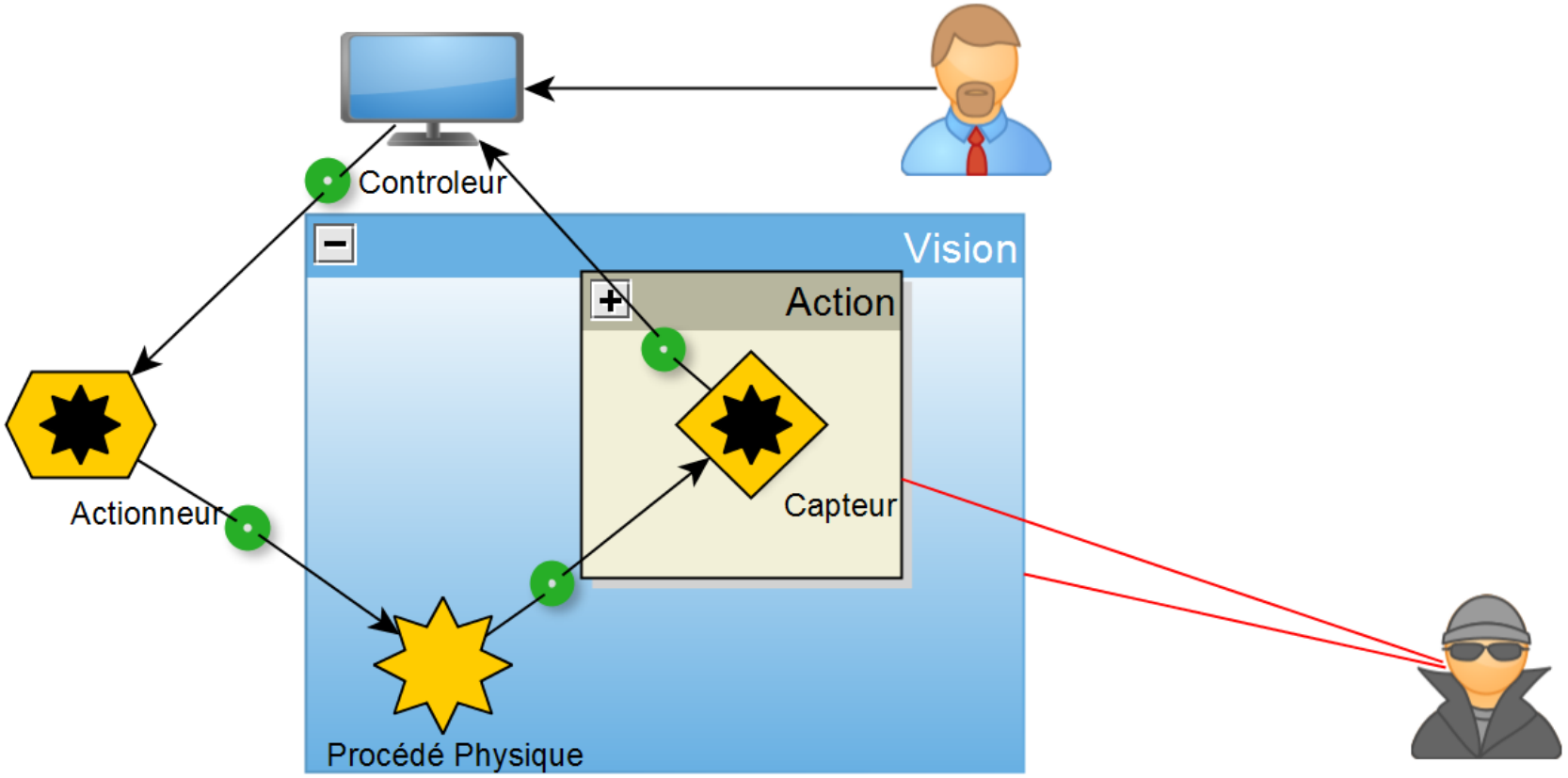
A) Système de commande

B) Ebauche de concept

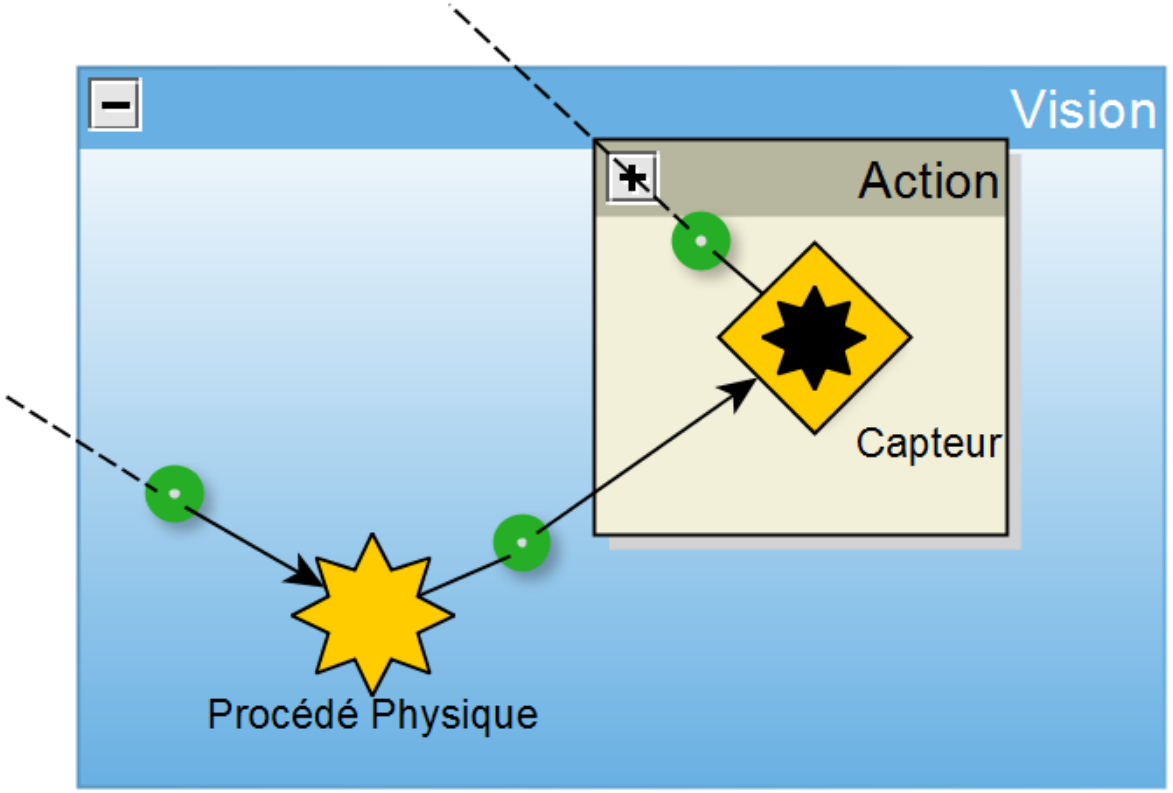
Système de commande



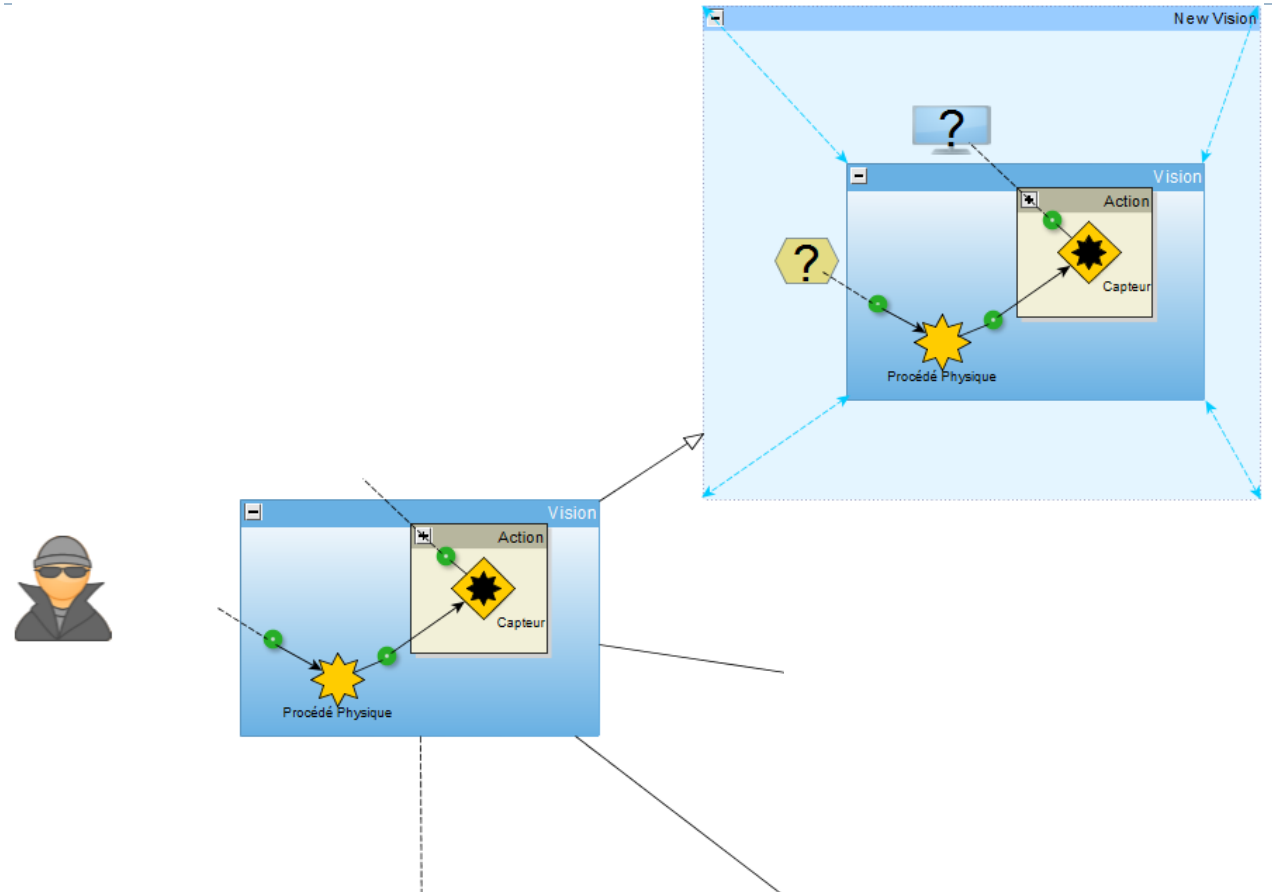
Ebauche de concept



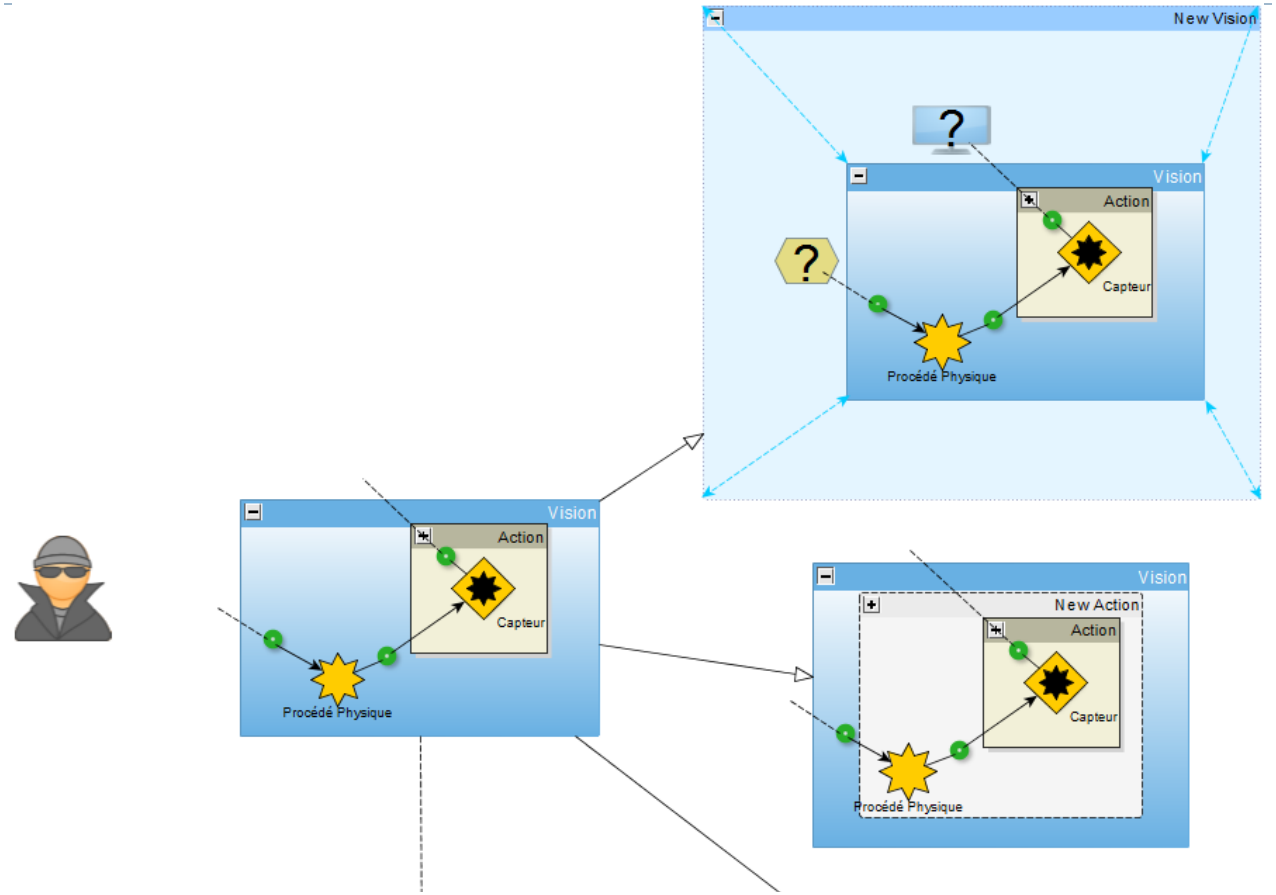
Ebauche de concept



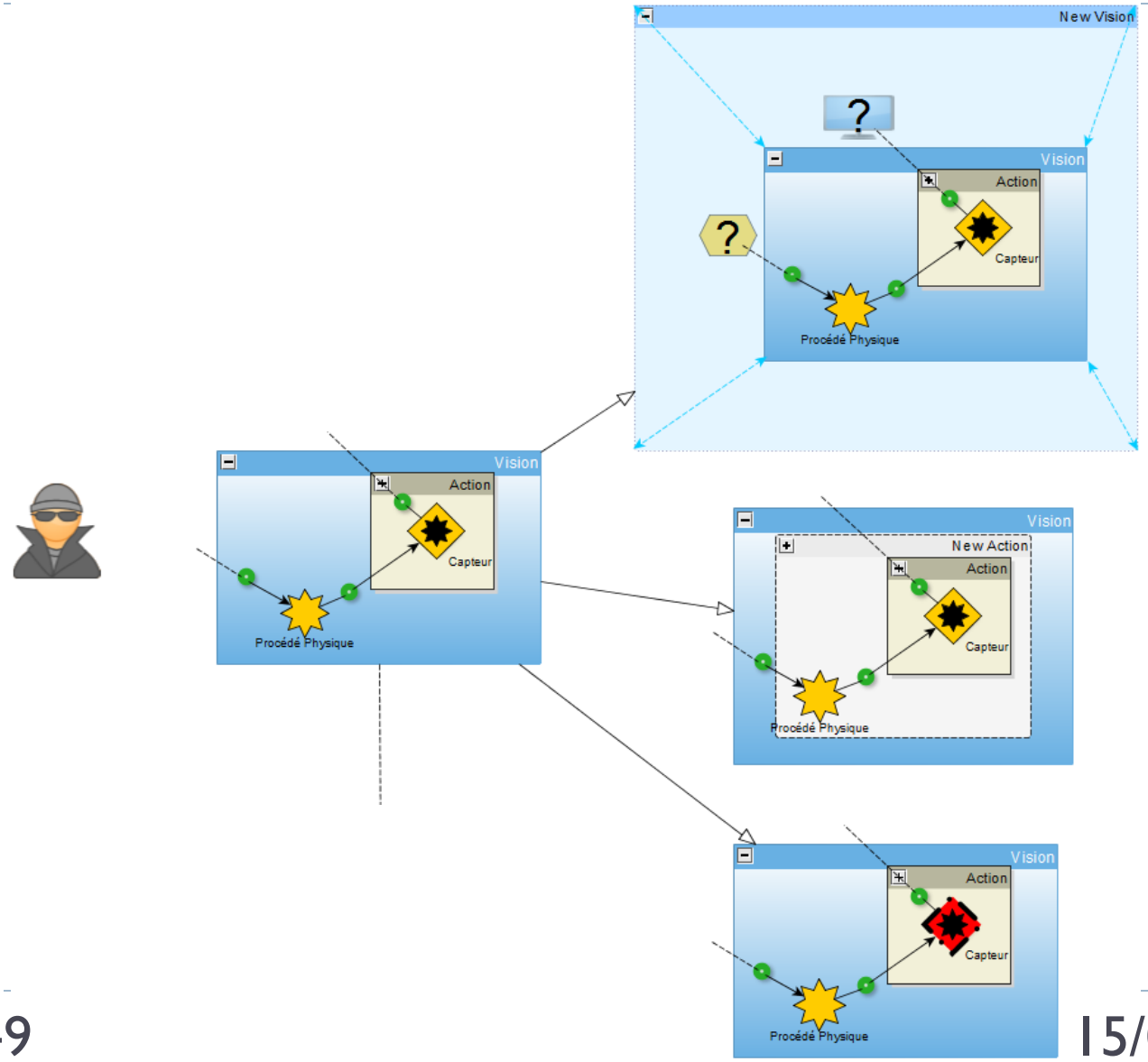
Ebauche de concept



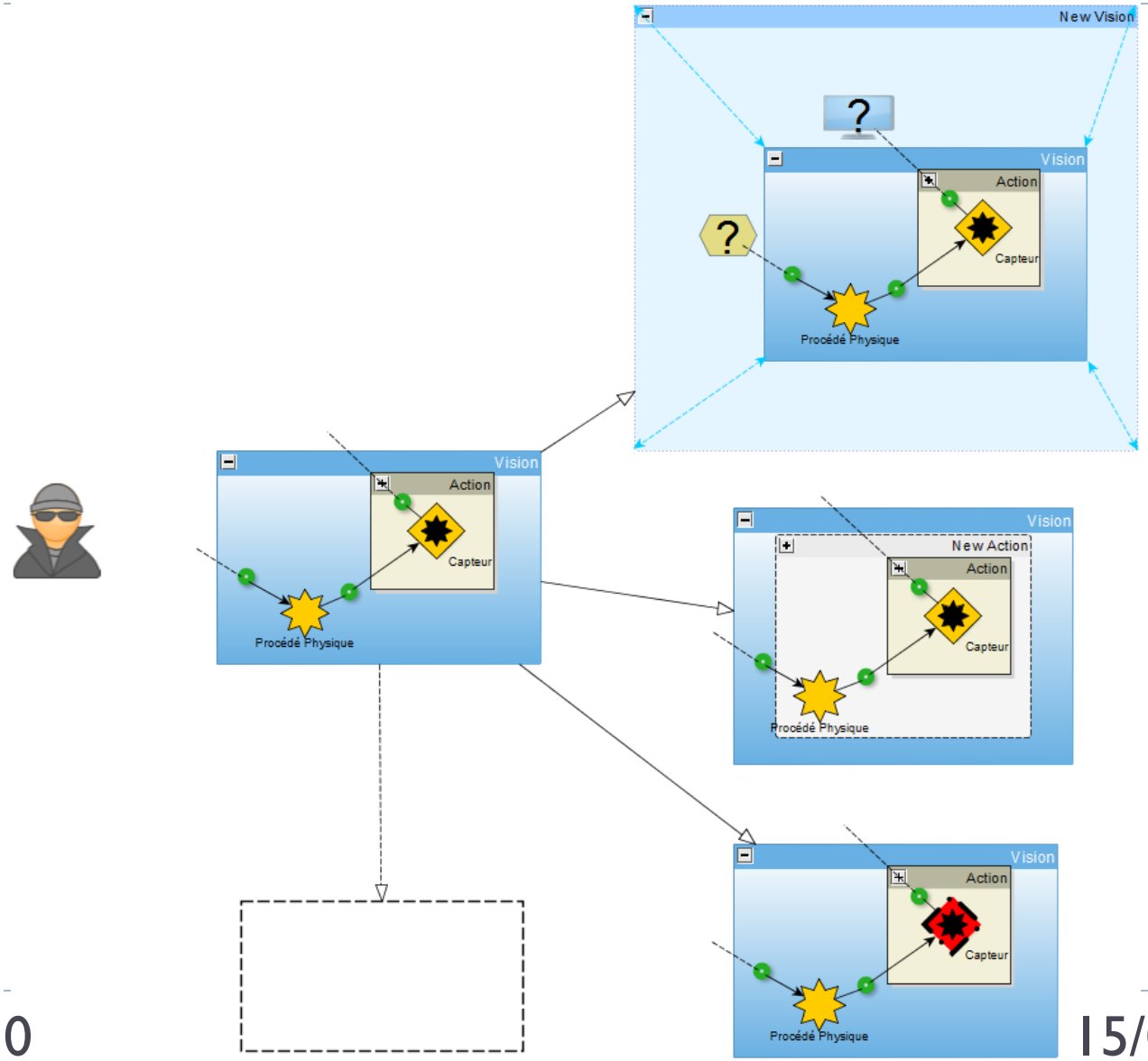
Ebauche de concept



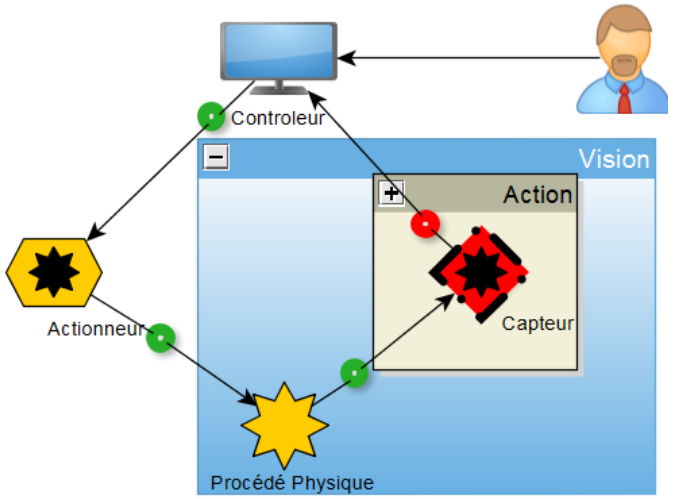
Ebauche de concept



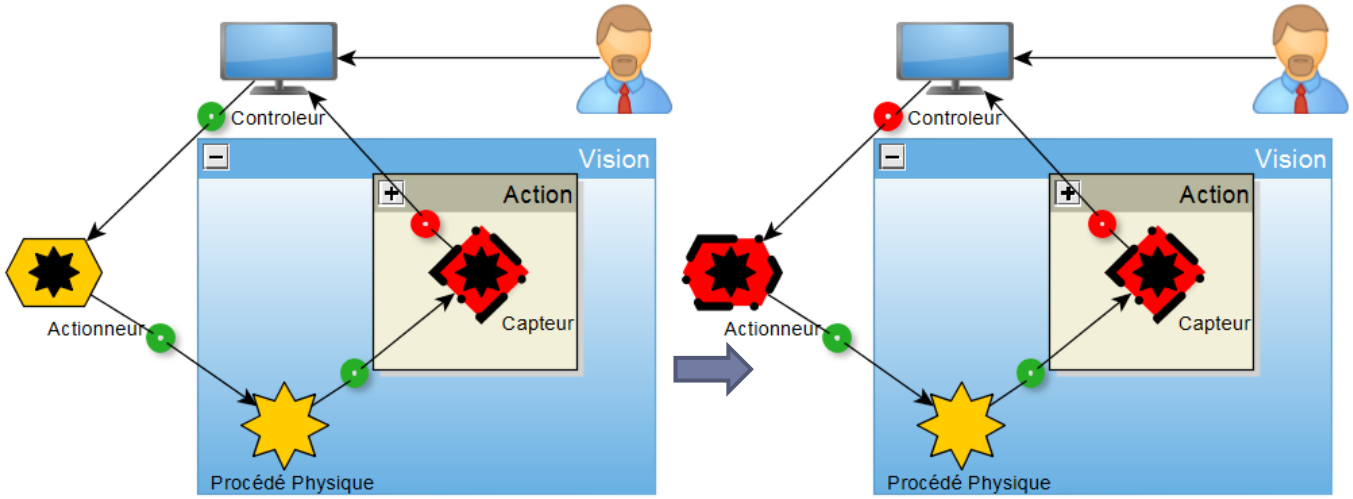
Ebauche de concept



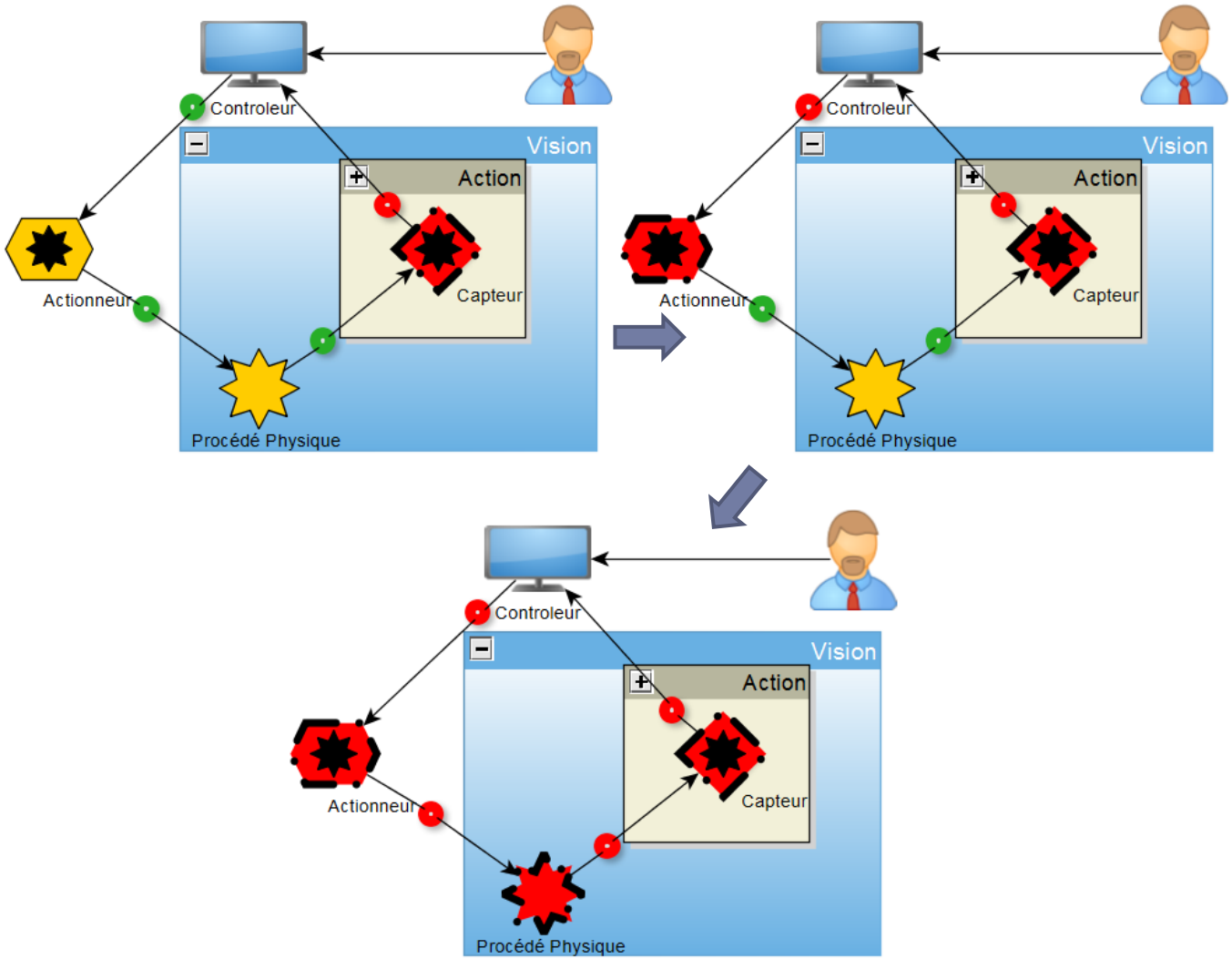
Ebauche de concept



Ebauche de concept



Ebauche de concept



Conclusion

Conclusion
Bilan

- Réification de la surface d'attaque
  - Définitions (Surface d'attaque, Attaquant, Menace, Faille & Attaque)
  - Arbres d'attaque
  - Cyber Threat Intelligence
  - STIX
- Aspect dynamique
  - Théorie des jeux
  - Defense-by-Deception
- Moteur d'exécution
  - Ebauche de concept

Conclusion
Perspectives

- STIX & la surface d'attaque
- Asymétrie inhérente à la cyber-sécurité
  - Initiative de l'attaquant (proactif)
  - Préparation et/ou remédiation du défenseur (passif/réactif)
- Maquette à raffiner

Merci de votre attention

Bibliographie

- [1] *Analyse et réduction de la surface d'attaque* / Mickael Dorigny / https://www.information-security.fr/ / 19 Décembre 2015
- [2] *Towards Threat, Attack, and Vulnerability Taxonomies* / Dennis Hollingworth / Network Associates laboratories USA / 2003
- [3] *Trust in Cyberspace* / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999
- [4] *AVOIDIT : A Cyber Attack Taxonomy* / Chris B. Simmons, Sajjan G. Shiva, Harkeerat Bedi, Dipankar Dasgupta / University of Memphis, Memphis, Tennessee, USA / Juin 2014
- [5] *Attack Modeling for Information Security and Survivability* / Andrew P. Moore, Robert J. Ellison, Richard C. Linger/ Software Engineering Institute, Carnegie Mellon University, USA / Mars 2001
- [6] *Definitive Guide to Cyber Threat Intelligence* / Jon Friedman, Mark Bouchard, CISSP / CyberEdge Group Annapolis, USA / 2015

Bibliographie

- [7] *Redefining the Center of Gravity* in *Joint Force Quarterly (JFQ) issue 59* / Dale C. Eikmeier / Washington D.C. USA / 2010
- [8] *Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX)* / Sean Barnum / The MITRE Corporation / 20 Février 2014
- [9] *CyberWar Games: Strategic Jostling Among Traditional Adversaries* / Sanjay Goel, Yuan Hong / University of New York, New York, USA / 2015
- [10] *Attribution, Temptation, and Expectation : A Formal Framework for Defense-by-Deception in Cyberwarfare* / Ehab Al-Shaer, Mohammad Ashiqur Rahman / University of North Carolina, Charlotte, USA / 2015
- [11] *Game-Theoretic Foundations for the Strategic Use of Honeypots in Network Security* / Christopher Kiekintveld, Viliam Lisý, Radek Píbil / University of Texas, El Paso, USA / Czech Technical University, Prague, Czech Republic / 2015
- [12] *Automated Adversary Profiling* / Samuel N. Hamilton / Siege Technologies, Manchester, USA / 2015