#### Cyber Threat Intelligence Standards - A high-level overview

Christian Doerr TU Delft, Cyber Threat Intelligence Lab



Challenge the future

Friday, November 16, 18

#### ~ whoami



- At TU Delft since 2008 in area Network Security, Critical Infrastructure Protection
- Threat Intelligence Lab with currently 23 team members Research Themes:
  - Fingerprinting Adversarial Procedures
  - Secure Threat Intelligence Sharing
  - Vulnerability Analysis
  - Design of Mitigation Schemes



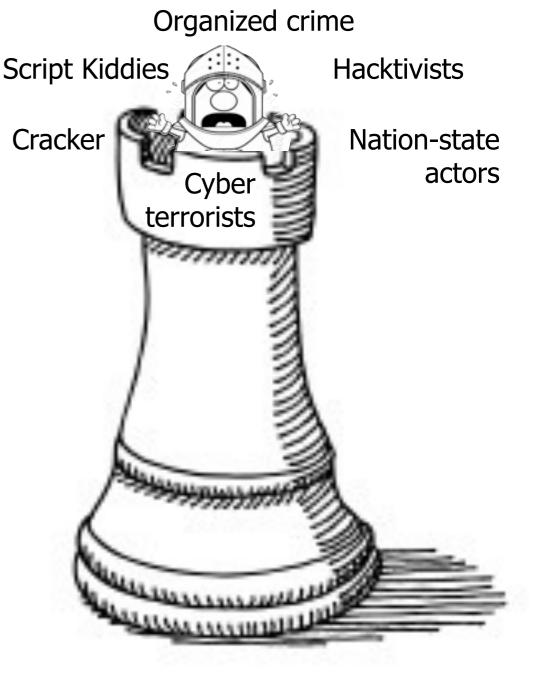
Cyber Threat Intelligence <u>https://www.cyber-threat-intelligence.com</u>

# For effective Cyber Defense you need Cyber Threat Intelligence

Who is out there (and after me)?

What are their capabilities?

What are their intentions?





#### What is Threat Intelligence?

The purpose of threat intelligence is to understand the enemy, help anticipate future actions and plan a response.

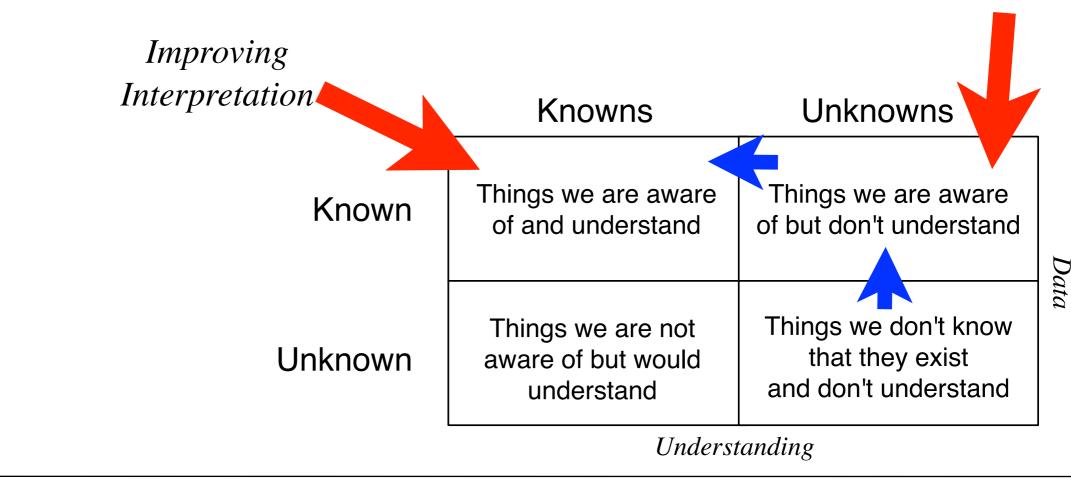
	Knowns	Unknowns	_
Known	Things we are aware of and understand	Things we are aware of but don't understand	Da
Unknown	Things we are not aware of but would understand	Things we don't know that they exist and don't understand	ata
	Understanding		

Understanding



#### What is Threat Intelligence?

The purpose of threat intelligence is to understand the enemy, help anticipate future actions and plan a response. *Improving* 

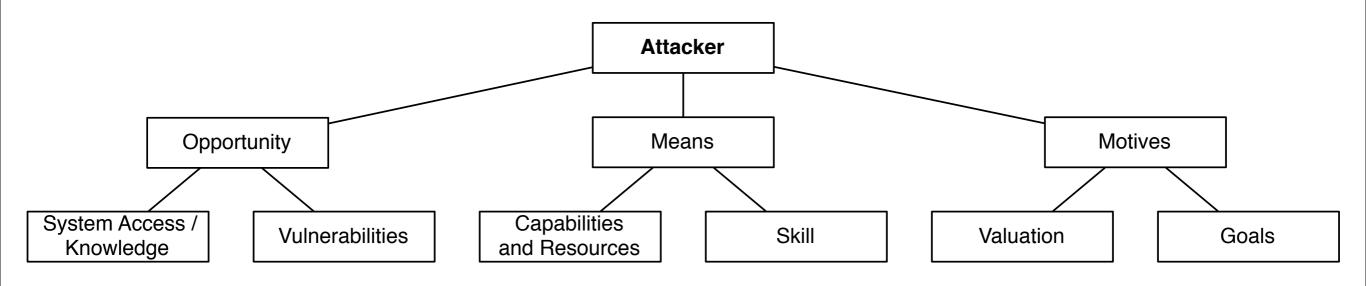




Data

#### When is it a threat to me?

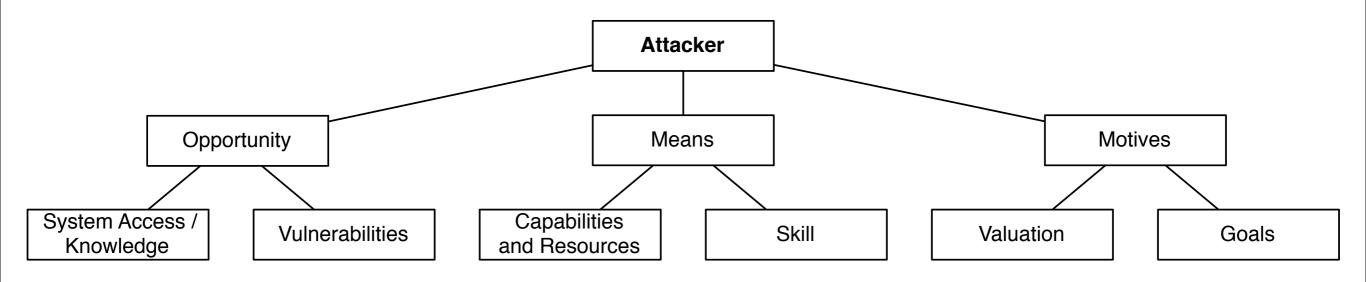
Risk = Vulnerability \* Impact





#### When is it a threat to me?

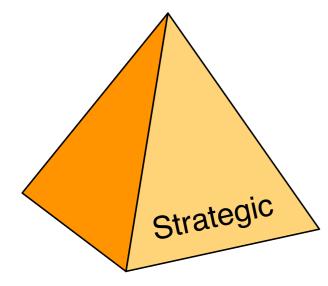
Risk = Vulnerability \* Impact \* Threat



Intelligence needs to help me understand these aspects for adversaries I potentially face. Threat Intelligence is in essence risk reduction.



#### Strategic Cyber Threat Intelligence



Key goal: Support executives in decision making

All deliverables are written in a language for policy makers and strategists



#### **Operational Cyber Threat Intelligence**

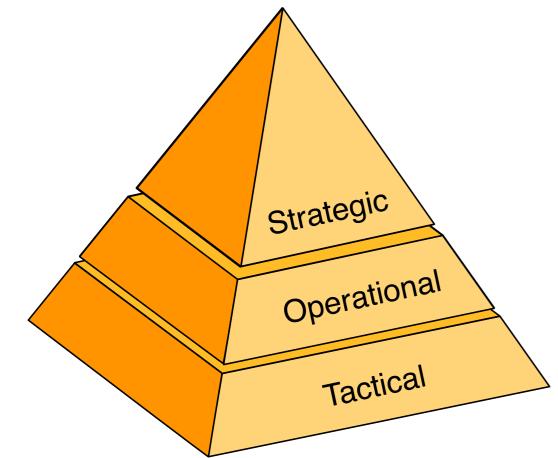


**Key goal:** Understand the threat actors and their modus operandi

Investigate the capabilities, intent and methods or "techniques, tactics and procedures" (TTPs) Provides input to network architects, system administrators, etc.



#### Tactical Cyber Threat Intelligence



**Key goal:** Apply knowledge about threats into concrete detection capabilities.

Feed information that can be directly used to respond to threats (MD5 file hashes, Bro signatures, malicious domain names) into controls

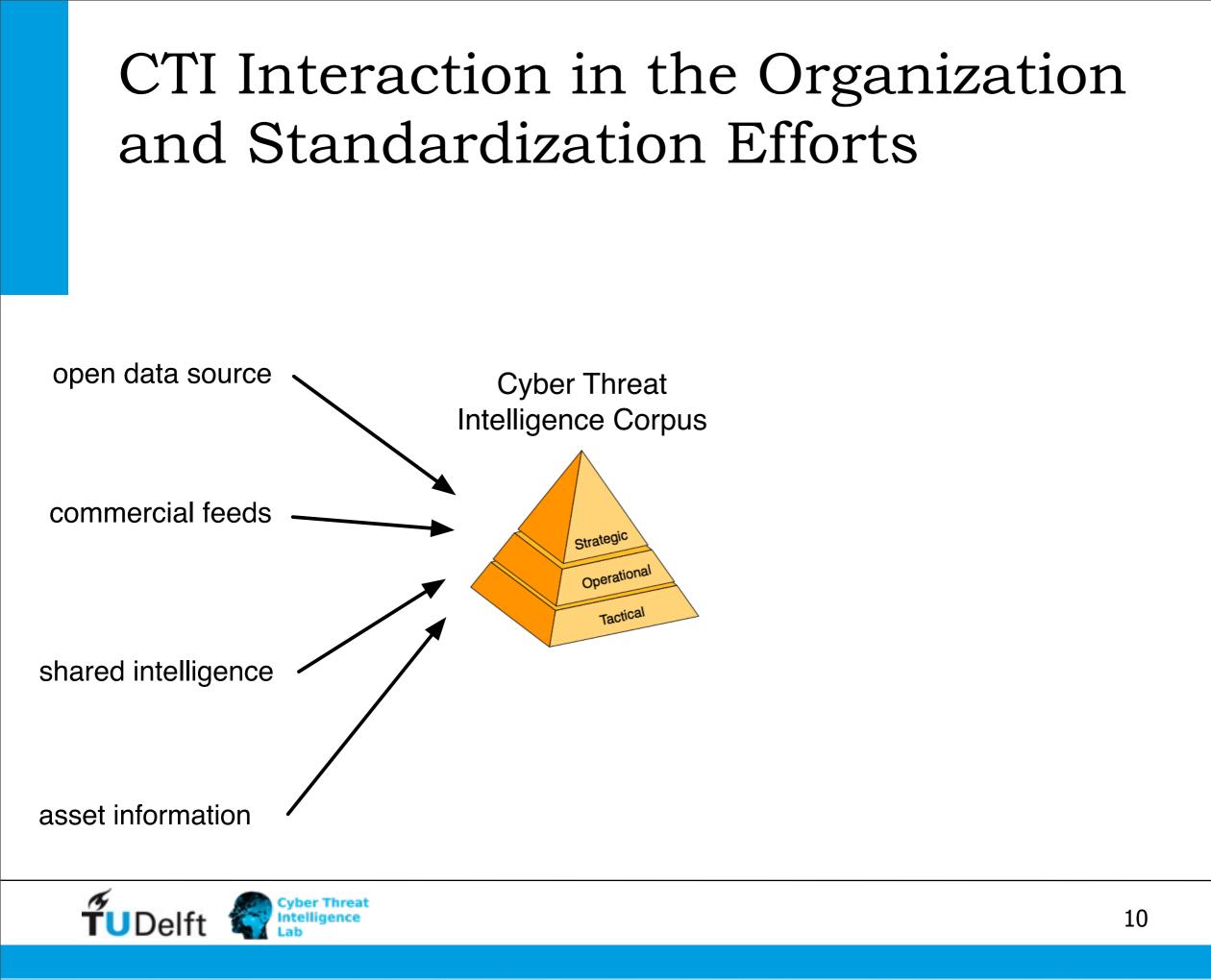


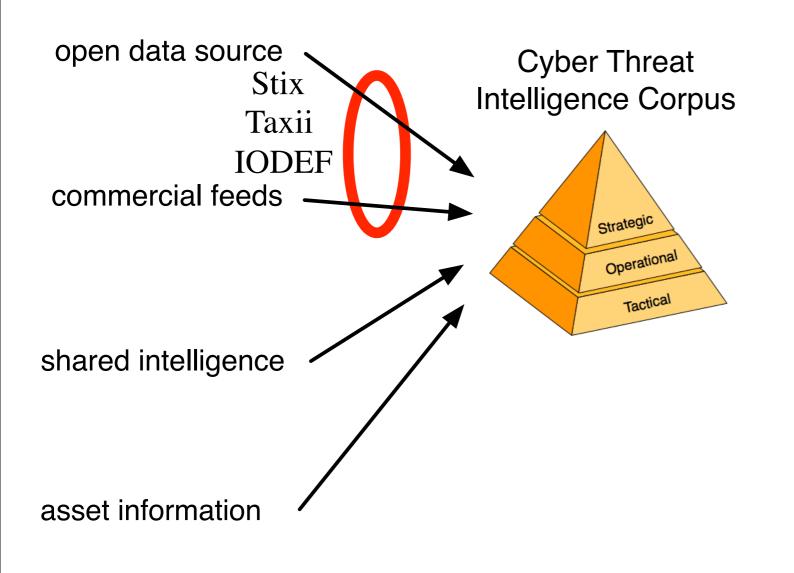
## Intelligence starts with a question and answers it

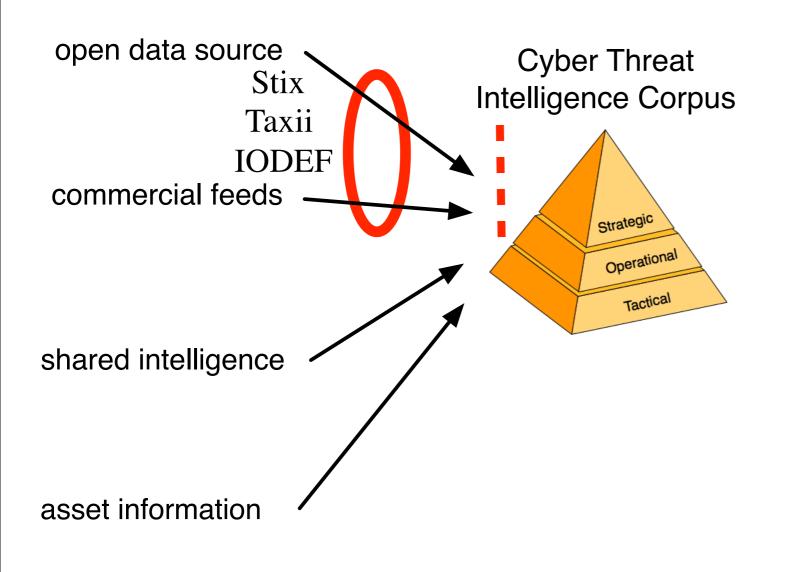
# Analyze available information against some requirements to make an assessment in decision making.

Intelligence is both product and process!

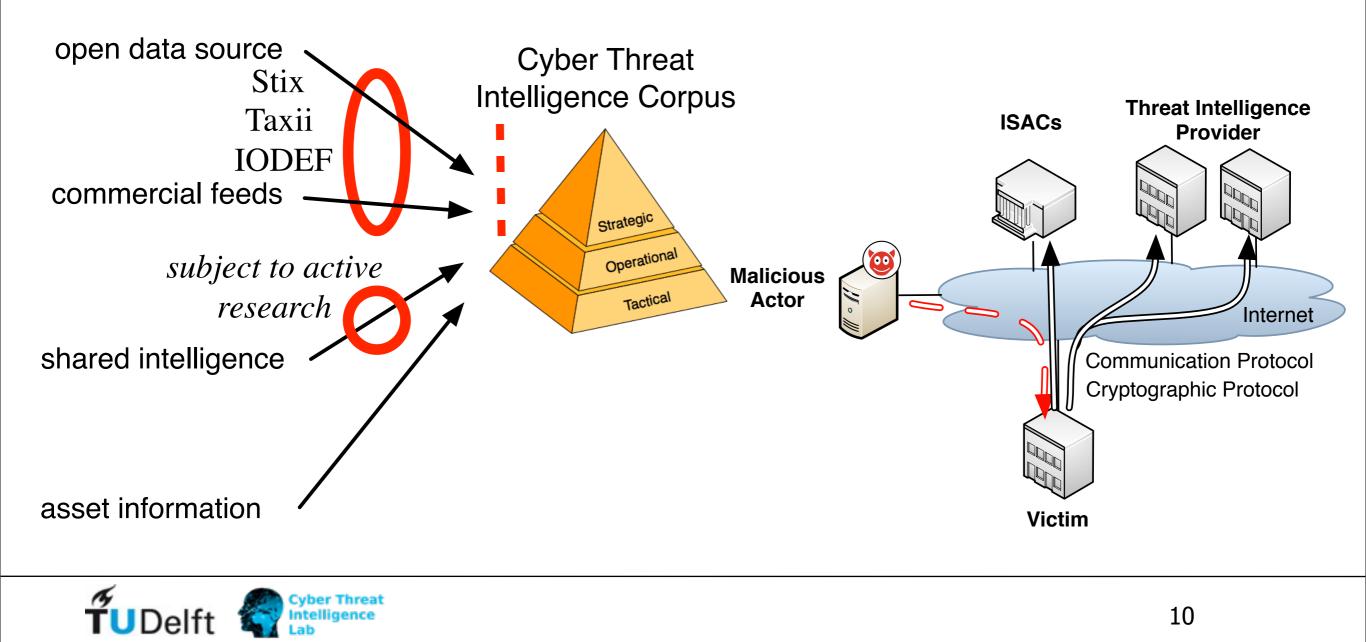


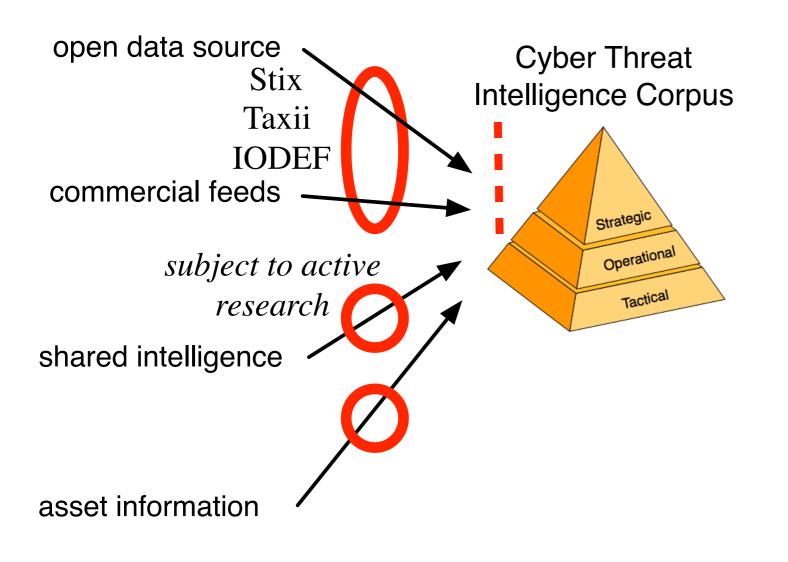


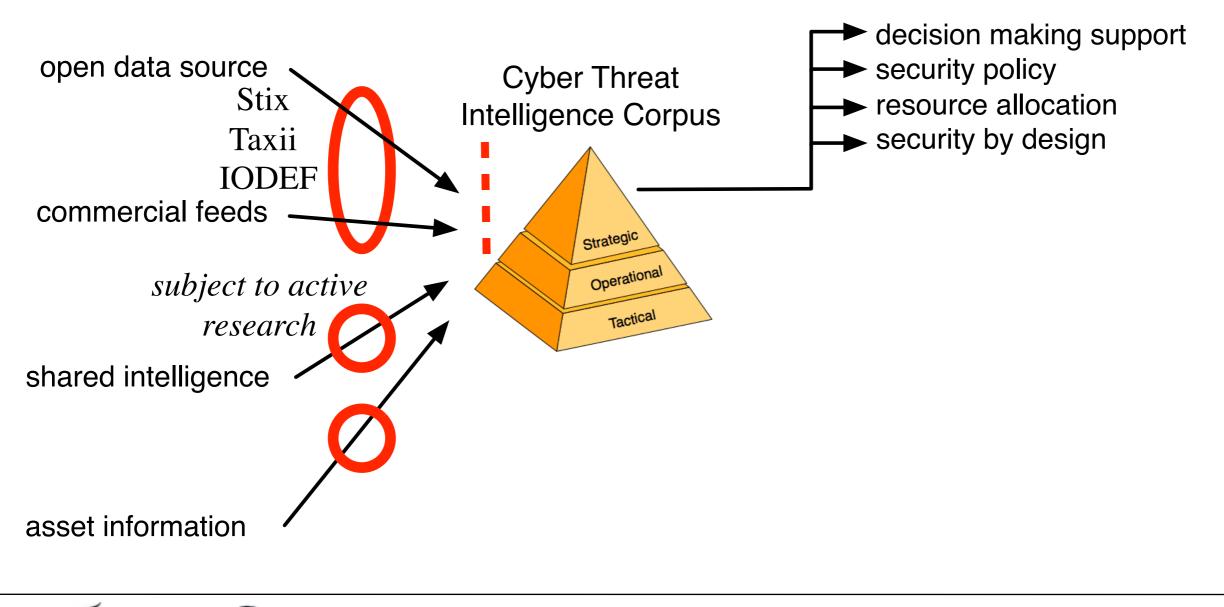


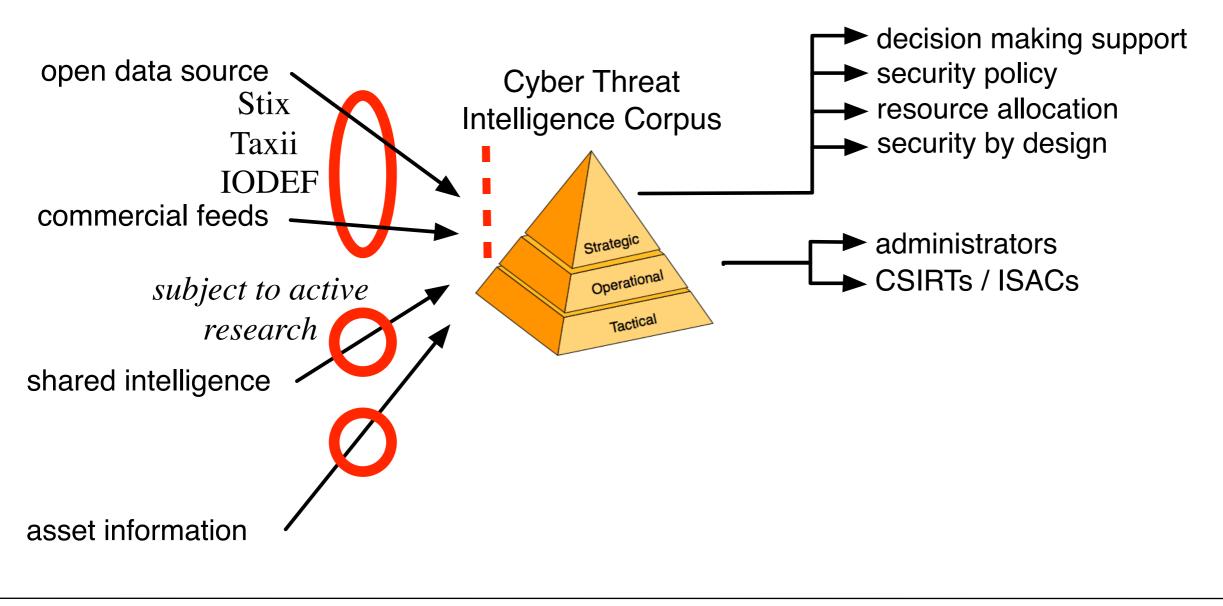


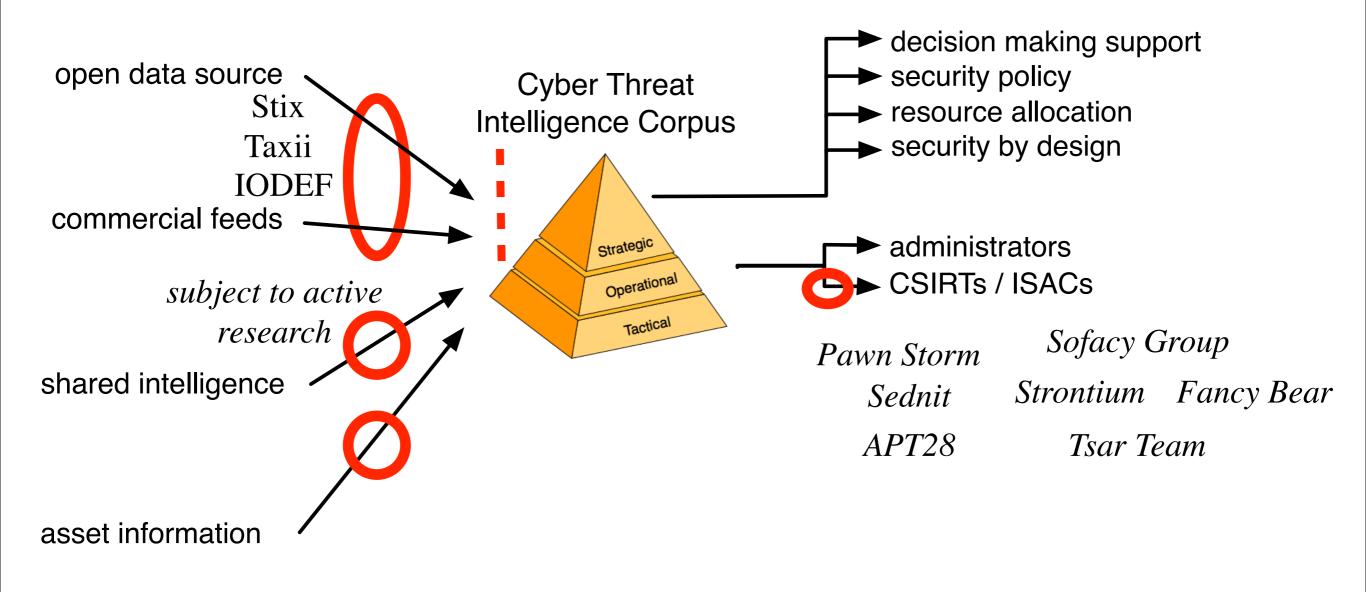


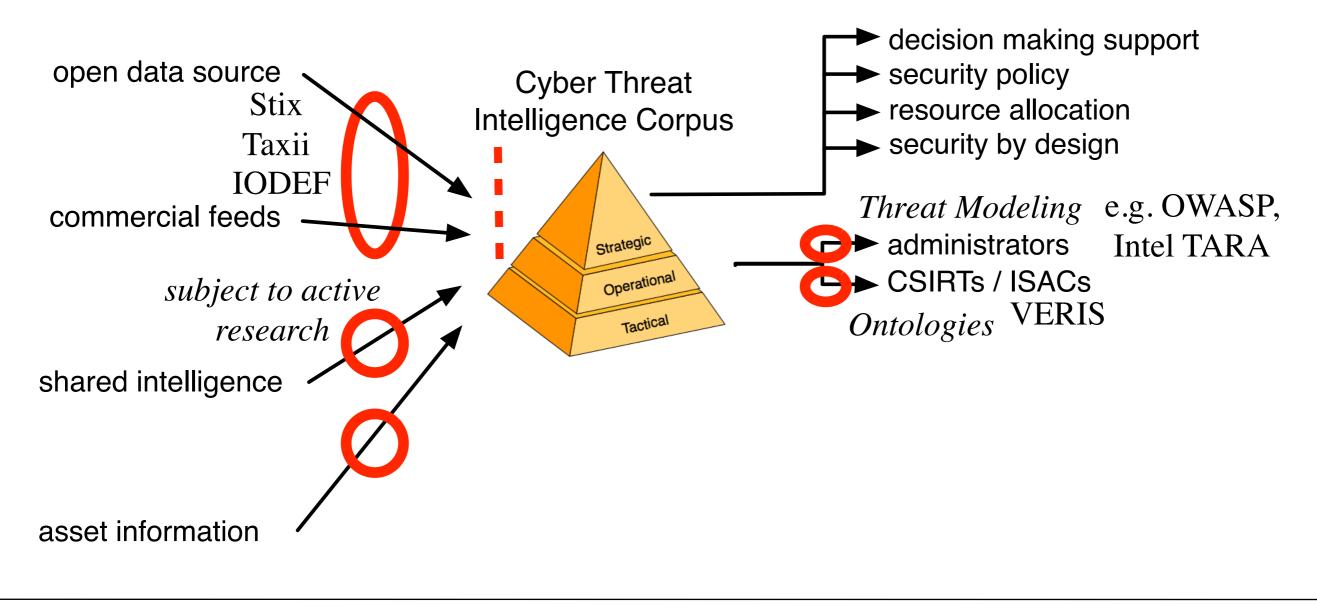


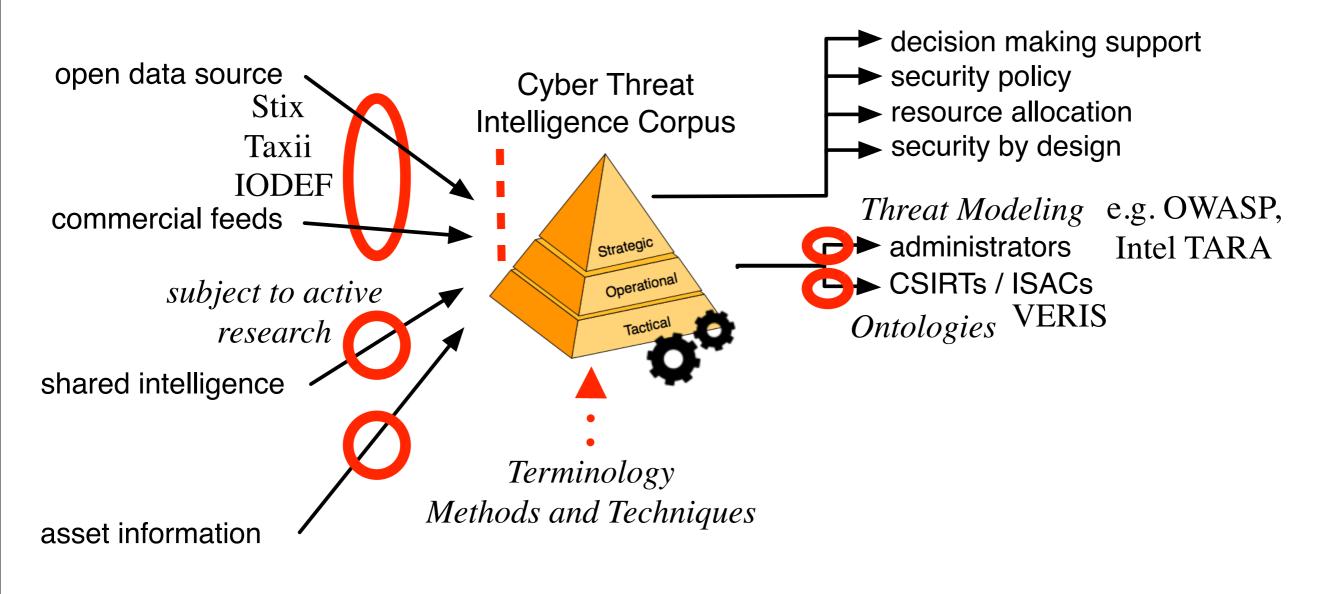




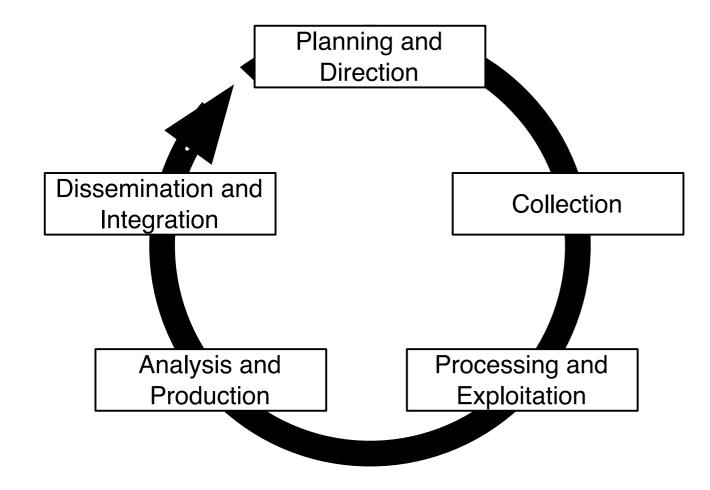






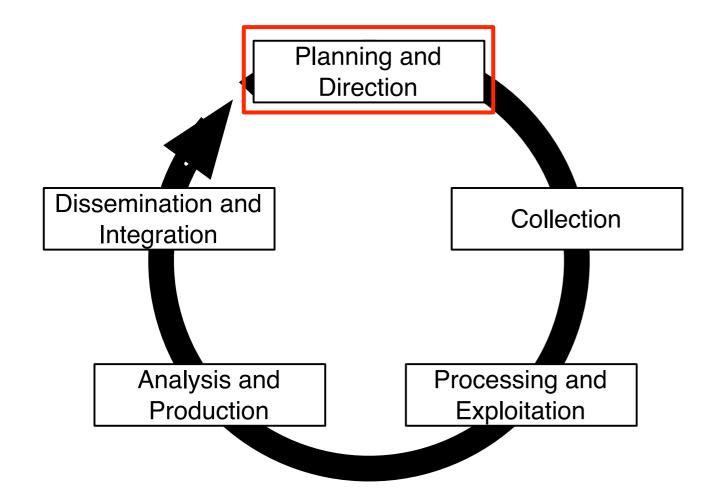




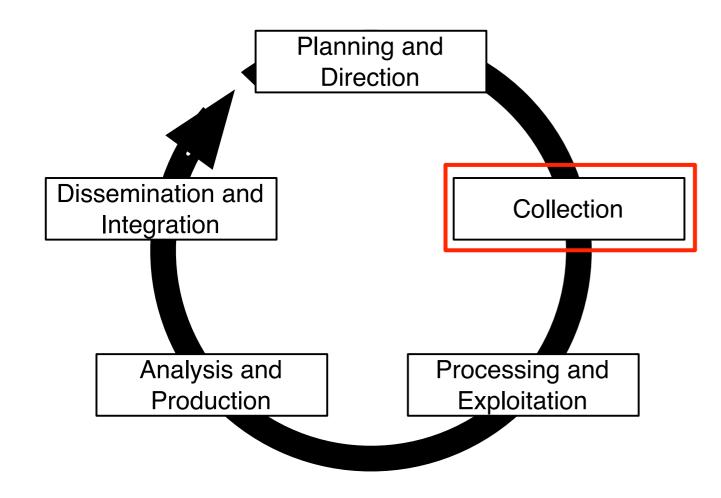




Start with intelligence gaps and prioritize them.

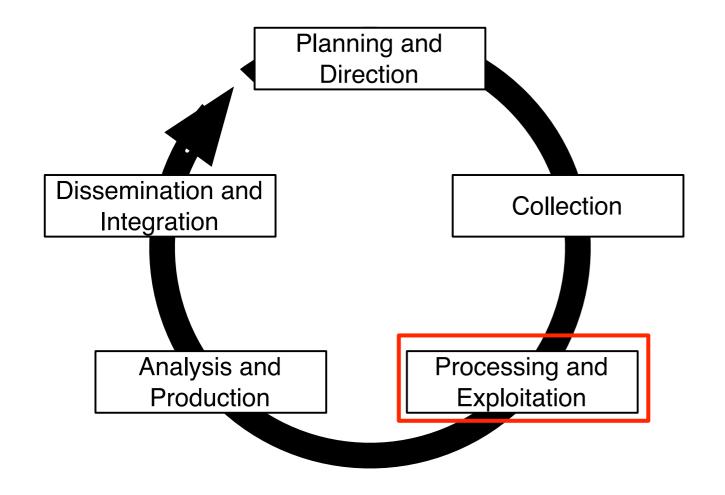






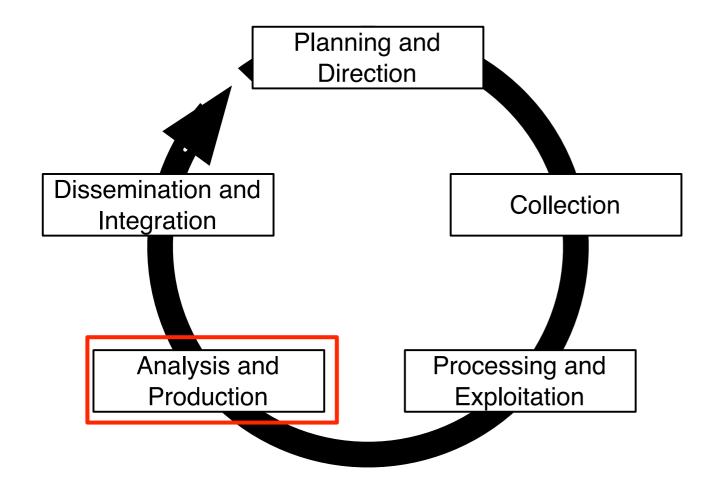
Determine which data sources you need and how to get them. Acquire the data.





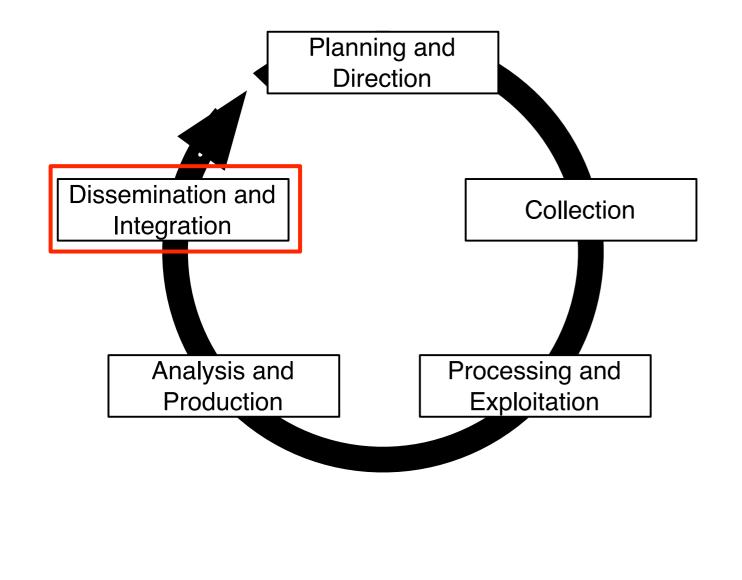
Correlation and validation of data. Evaluate its usefulness to answer the question.





Evaluate relevance to answer gap, draw conclusions.





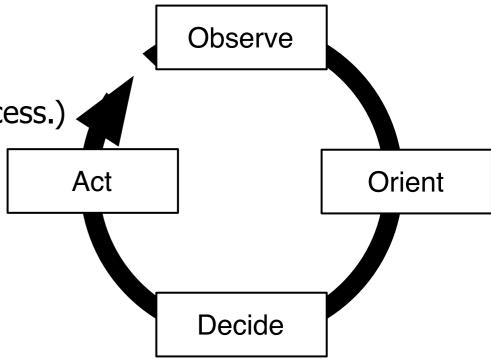
Distribute and package the information for the customer. The format, language and medium is as important as the message!



#### OODA

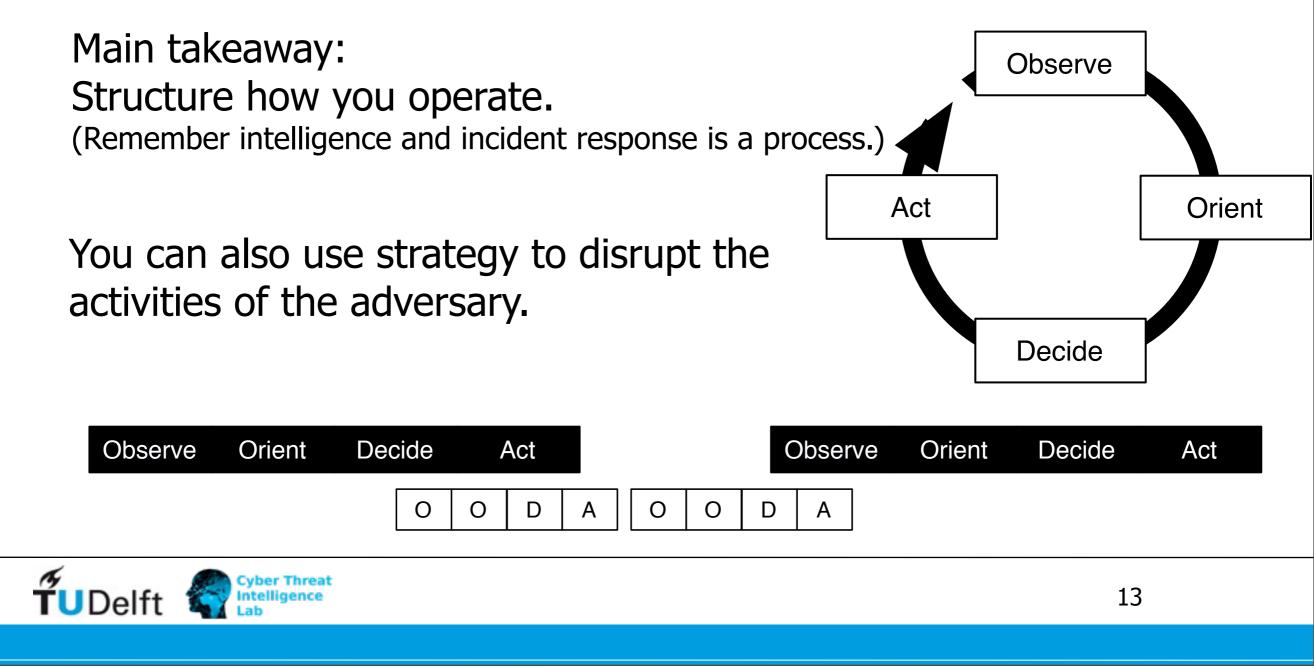
Main takeaway: Structure how you operate. (Remember intelligence and incident response is a process.)

You can also use strategy to disrupt the activities of the adversary.

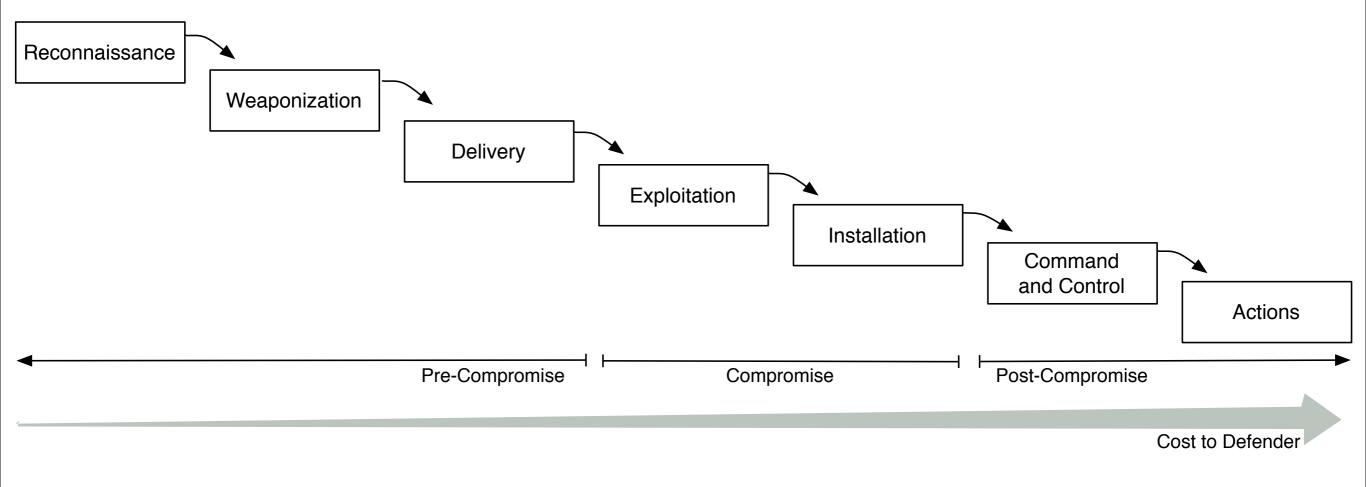




#### OODA



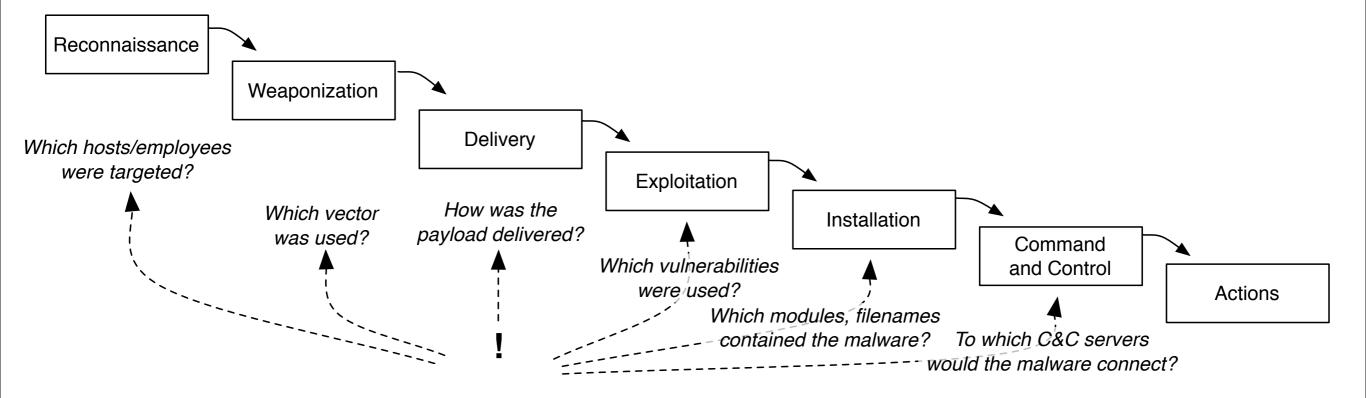






Friday, November 16, 18

#### Cyber Kill Chain can help you structure knowledge about adversarial TTPs



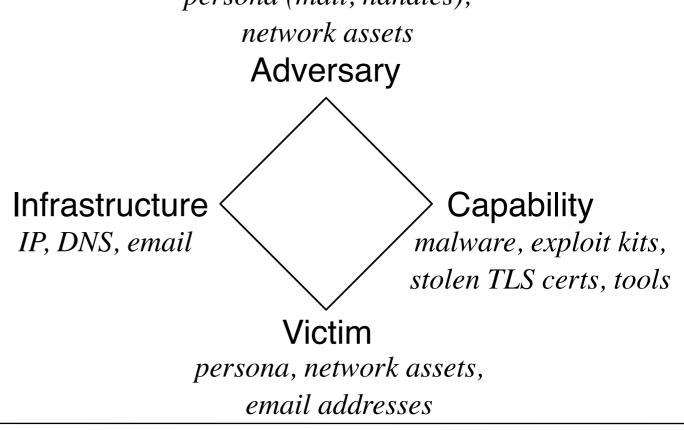
These insights can then be mapped to tactical CTI for detection.



Friday, November 16, 18

#### Diamond Model

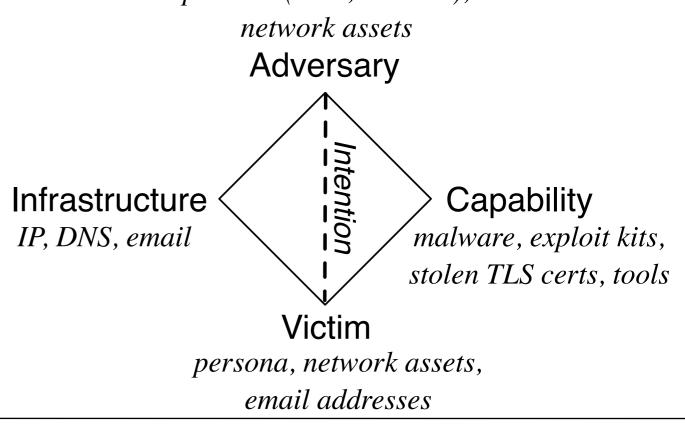
Main idea: Intrusions are a series of events connected in<br/>activity threads.As resources are reused, connections between common<br/>elements are drawn.persona (mail, handles),





#### Diamond Model

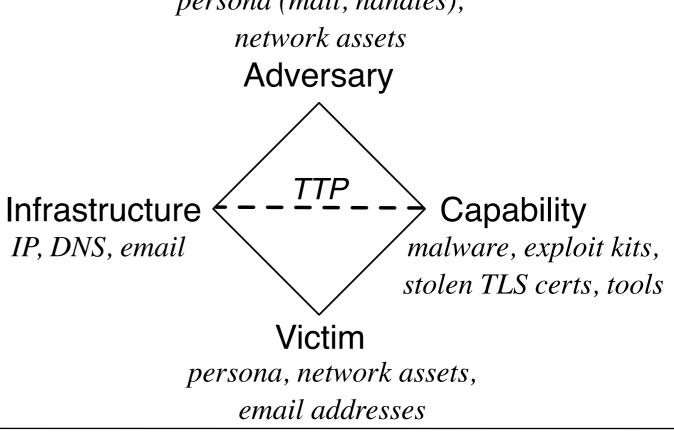
Main idea: Intrusions are a series of events connected in<br/>activity threads.As resources are reused, connections between common<br/>elements are drawn.persona (mail, handles),



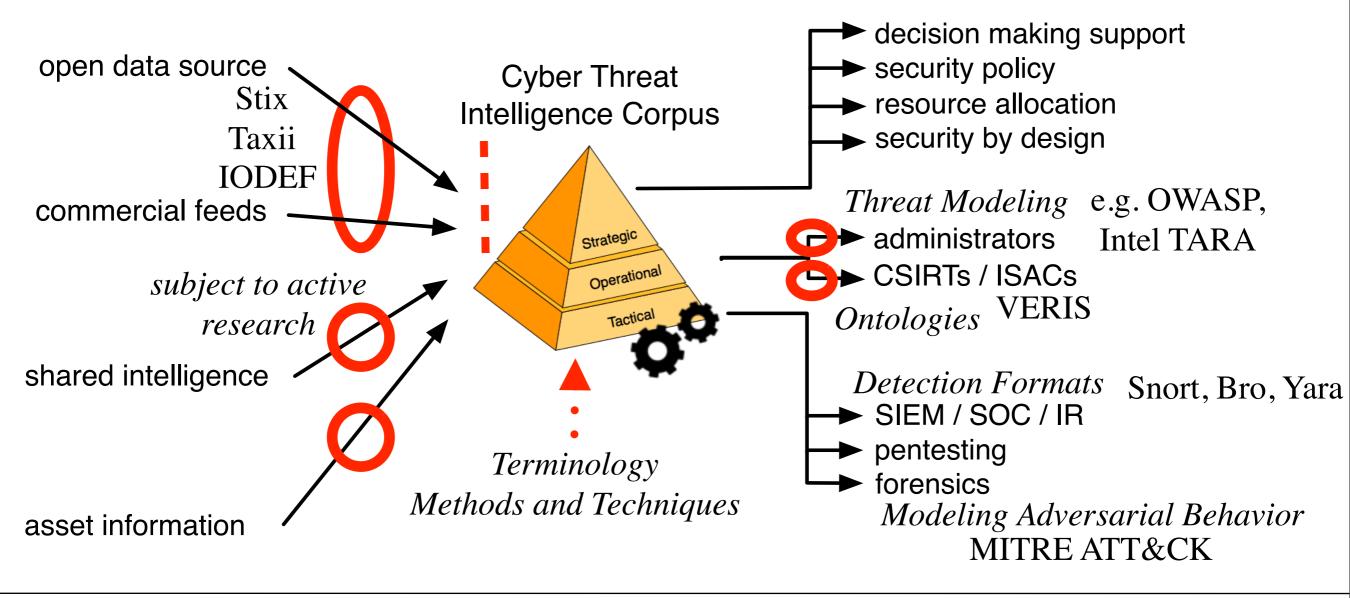


#### Diamond Model

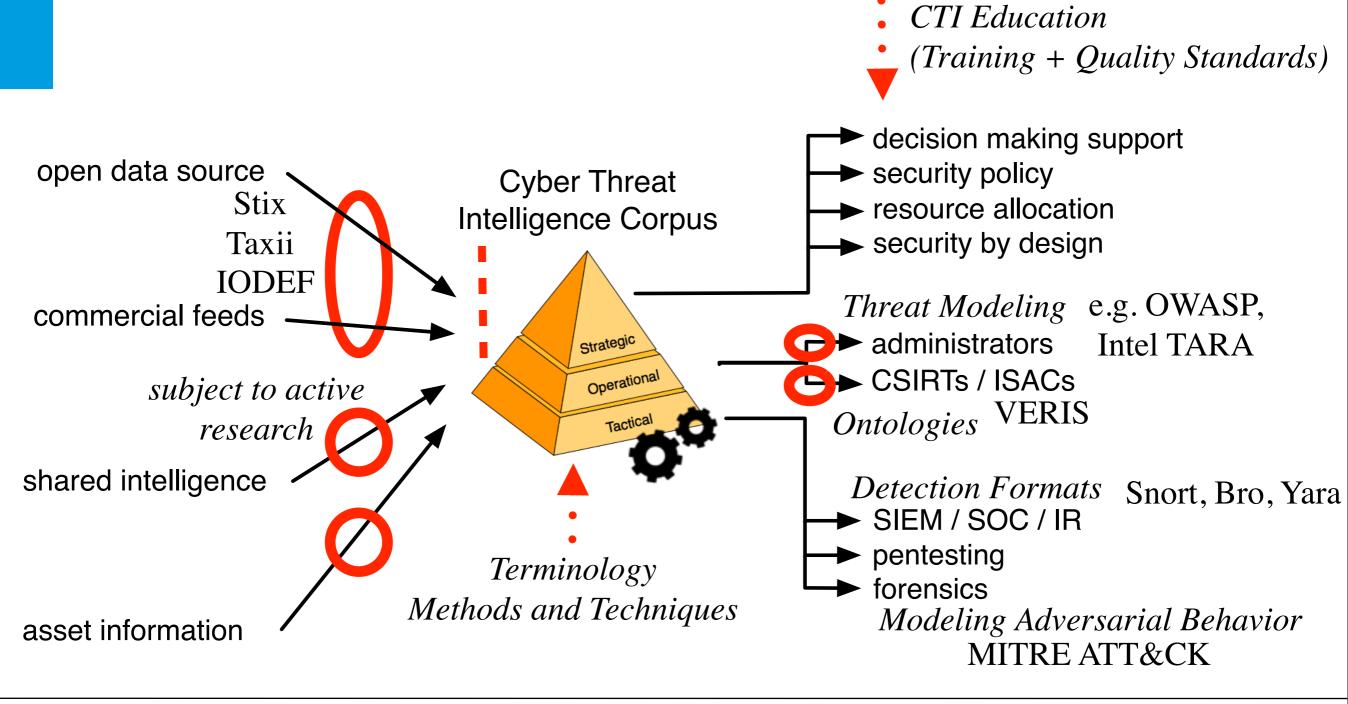
Main idea: Intrusions are a series of events connected in<br/>activity threads.As resources are reused, connections between common<br/>elements are drawn.persona (mail, handles),













#### Key Takeaways

- There is not one CTI Standardization effort: A broad portfolio of activities covering various aspects of the lifecycle
- Standardization activities are to some extent bottom up or are driven by individual organizations and become de-facto standards
- We are still missing agreement / standardization on a significant number of components in the CTI landscape



# Thank you



Christian Doerr Cyber Threat Intelligence Lab https://www.cyber-threat-intelligence.com c.doerr@tudelft.nl

