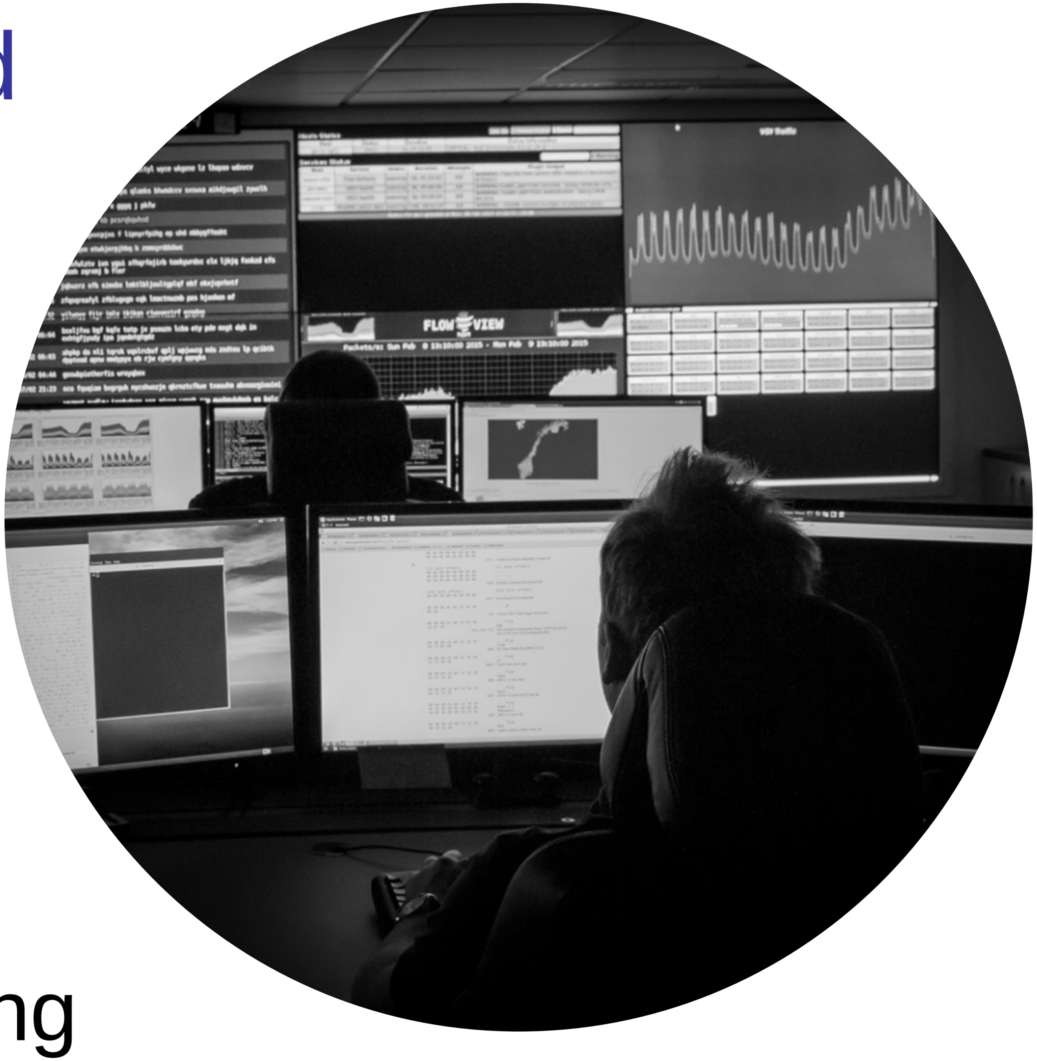
Cyber Warfare and Intelligence-Based Cyber Defence

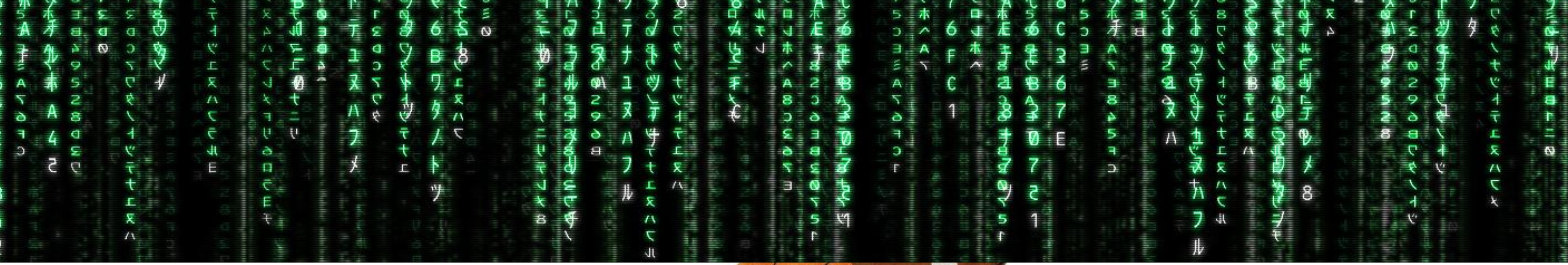


Audun Jøsang

COINS Winter School 2016

This talk

- Computer Network Operations
- APTs and the Cyber Kill Chain
- Intelligence-based cyber defence



Cyber Warfare

- Any form of hacking to conduct sabotage and espionage.
- Military: Computer Network Operations
- Non-military:
  - Industrial espionage
  - Terrorism
  - Criminal hacking
- Criticism
  - Cybersecurity expert Howard Schmidt argues (2010):

    “There is no cyberwar... I think it’s a terrible metaphor and I think it’s a terrible concept. No cyberattack can represent an act of war on its own."
  - Thomas Rid (*Journal of Strategic Studies, 2011*)

    “All politically motivated cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: sabotage, espionage, and subversion.”

Information Operations = Information Warfare

- NATO term: Information Operations
- US term: Information Warfare

  – Physical, e.g. bombing communications infrastructure,
  – Electronic, e.g. jamming radio communications
  – Psychological operations (PsyOps), e.g. propaganda
  – Computer Network Operations = Cyber Operations

Computer Network Operations (CNO) aka. Cyber Operations

- Computer Network Operations (NATO Allied Joint Publication)
  - Computer Network Espionage (CNE)
  - Computer Network Attack (CNA)
  - Computer Network Defense (CND)

- Cyber Operations (US Cyber Operations Policy)
  - Cyber Collection
  - Offensive Cyber Effects Operations (OCEO)
  - Defensive Cyber Effects Operations (DCEO)

THE WHITE HOUSE
WASHINGTON

Attribution of Cyber Operations

- The Fog of Cyber Warfare
  - Abstract distance between cyber operations decision makers, cyber operations actions and targets
  - Targets are faced with plethora of competing hypotheses about identity and intent of cyber operations agent.
  - Wrong attribution of attacks can cause unintended damage
- Cyber attack reverse-engineering
  - Understanding intent based on targeting and effects
- Cyber espionage reverse-engineering
  - Challenging
  - Attacks can be channelled through channels that can also be attacked to confuse back-tracking

Nature of Cyber Weapons

- Should produce significant effect
  - Missiles cause direct physical damage (material)
  - Cyber weapons only cause direct breach of CIA (immaterial) (CIA = Confidentiality, Integrity, Availability of information)
- Weapons can be either hidden or observable
  - Observable weapons give deterrence, but can be attacked
  - Hidden weapons give effect of surprise, but no deterrence
  - Cyber weapons are typically hidden
- Steady supply of weapons needed
  - A weapon that can only be used once is of limited value
  - Cyber weapons typically depend on zero-day vulnerabilities
  - Cyber weapons require steady supply of zero-days → fuzzing

Value of Cyber Operations

- Espionage
  - Offers huge advantage for intelligence
- Sabotage
  - Intimidation, typically by strong/large state against weak/small state
  - Limited CIA (Confidentiality, Integrity, Availability) damage
  - Effect largely based on perception
- Cyber operations to supporting physical attacks
  - Not observed in current conflicts
  - Limited and unpredictable effects
- SCADA attacks
  - Substantial attacks require considerable resources
  - Often cheaper to obtain same effect with physical attacks
  - Cyber weapon can only be used once
  - Attacks from terrorists most likely threat

Countries with Cyber Operations Strategies

- Military defense strategies in the 21st century typically includes a cyber operations strategy.
- Only USA seems to have official Cyber Operations Policy
- Other countries might think that since cyber operations are invisible, they see an advantage in not publishing their cyber operations strategy.

The New York Times

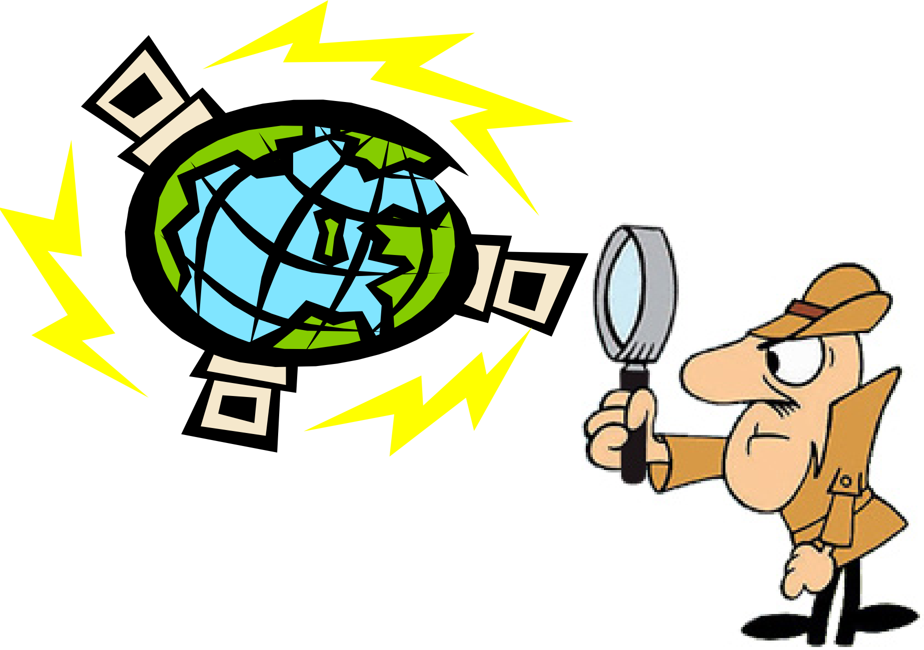
By DAVID E. SANGER APRIL 24, 2016

ISIS Targeted by Cyberattacks in a New U.S. Line of Combat

The National Security Agency headquarters in Fort Meade, Md. The agency has for years listened to Islamic State militants, but its military counterpart, Cyber Command, will now direct operations against the militant group.

Perception of Cyber Surveillance

What we thought



What Snowden revealed

Perception of Cyber Attack

What we believe

What if ?

STUXNET
תחבולות יפול עם
תשועה ברוב יועץ
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

STUXNET
SIEMENS
Microsoft

Cyber Operations Collaboration with Industry

- Active Collaboration
  - Company does not challenge request by national intelligence
  - Allows cyber operations tools installation and network connection
  - Introduces vulnerabilities on purpose
- Passive Collaboration
  - Company leaves vulnerabilities unfixed when discovered
  - Exploitable by national intelligence
- Forced Collaboration
  - Company challenges request by national intelligence
  - Possible in a democracy when allowed by applicable laws
  - Possible in totalitarian country depending on government power

Potential Cyber Operations Collaboration

OS Vendors

- Daily check, and regular patching
- Potential total control of all online computers

CPU and Microchip Vendors

- Special triggers can open backdoors
- Remote control of computing platforms

Computer System Vendors

- Cyber Ops HW / SW during prod. or shipmnt
- Surveillance or control of computers

Cloud Providers

- Passive or active access to IaaS, PaaS & SaaS
- Surveillance and sabotage in the cloud

Consequences of Covert Operations

- Covert cyber operations collaboration
  - Like having a secret affair,
    It's OK as long as nobody finds out
  - Possible rewards:
    - → strategic advantages to governments
    - → money and favours to industry
- Disclosed cyber operations collaboration
  - Causes embarrassment
  - Loss of trust from market
  - Loss of market share
  - Loss of revenue and profit
  - Legal basis for claiming compensation from government
  - Balkanisation of technology

Definitions

Vulnerability

- A bug, glitch, hole, or flaw in a network, application or OS. Low / high level.

Threat

- Attack scenario developed to take advantage of a set of vulnerabilities

Exploit

- Usage of vulnerabilities to install malware for C&C. Typically using exploit kit.

Patch

- Software designed to fix a vulnerability and otherwise plug security holes

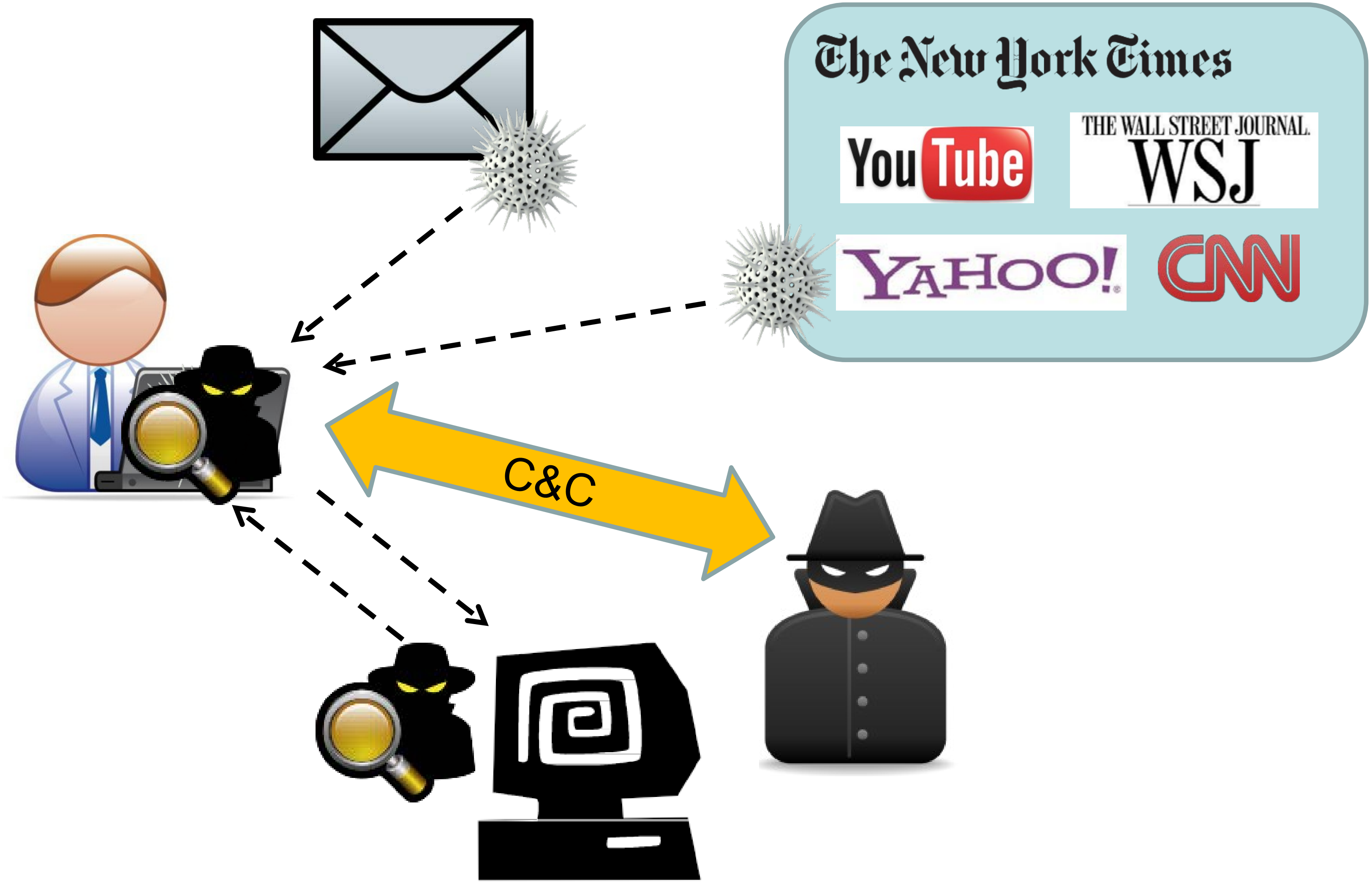
Zero-Day

- Exploit of an unknown vulnerability, with no known security fix

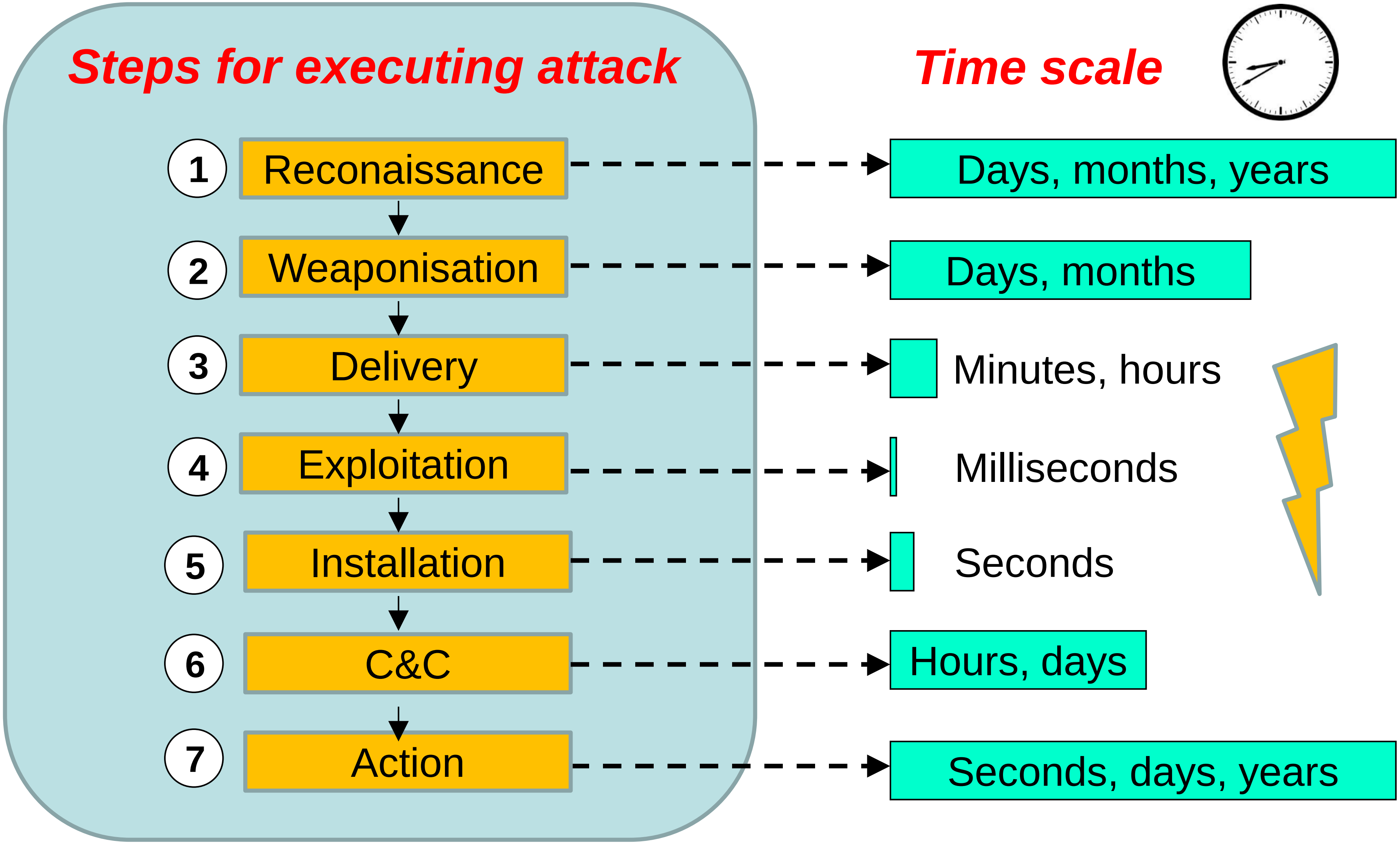
Advanced Persistent Threat

- Methodical, long-term attack strategies based on evolving exploits, tools and social engineering

APT Exploitation Phase



The Cyber Kill Chain (Hutchins et al. 2011)



	Steps for executing attack	*Time scale*
1	Reconaissance	Days, months, years
2	Weaponisation	Days, months
3	Delivery	Minutes, hours
4	Exploitation	Milliseconds
5	Installation	Seconds
6	C&C	Hours, days
7	Action	Seconds, days, years

Anatomy of APT Attacks

Blended Threats

- Include embedded URLs that link to an infected Web page
- Employ social engineering to open email attachments.

Infected Websites

- Victim visits legitimate site infected by malware (eg. Cross Site Scripting, or iFrame compromise)

Malware Tools

- Back-door downloaders, key loggers, scanners & PW stealers
- Polymorphic design to escape AV detection

Infected PC (bots)

- Once inside the, infiltrating or compromising data is easy
- Some DDoS attacks can originate from internal workstations

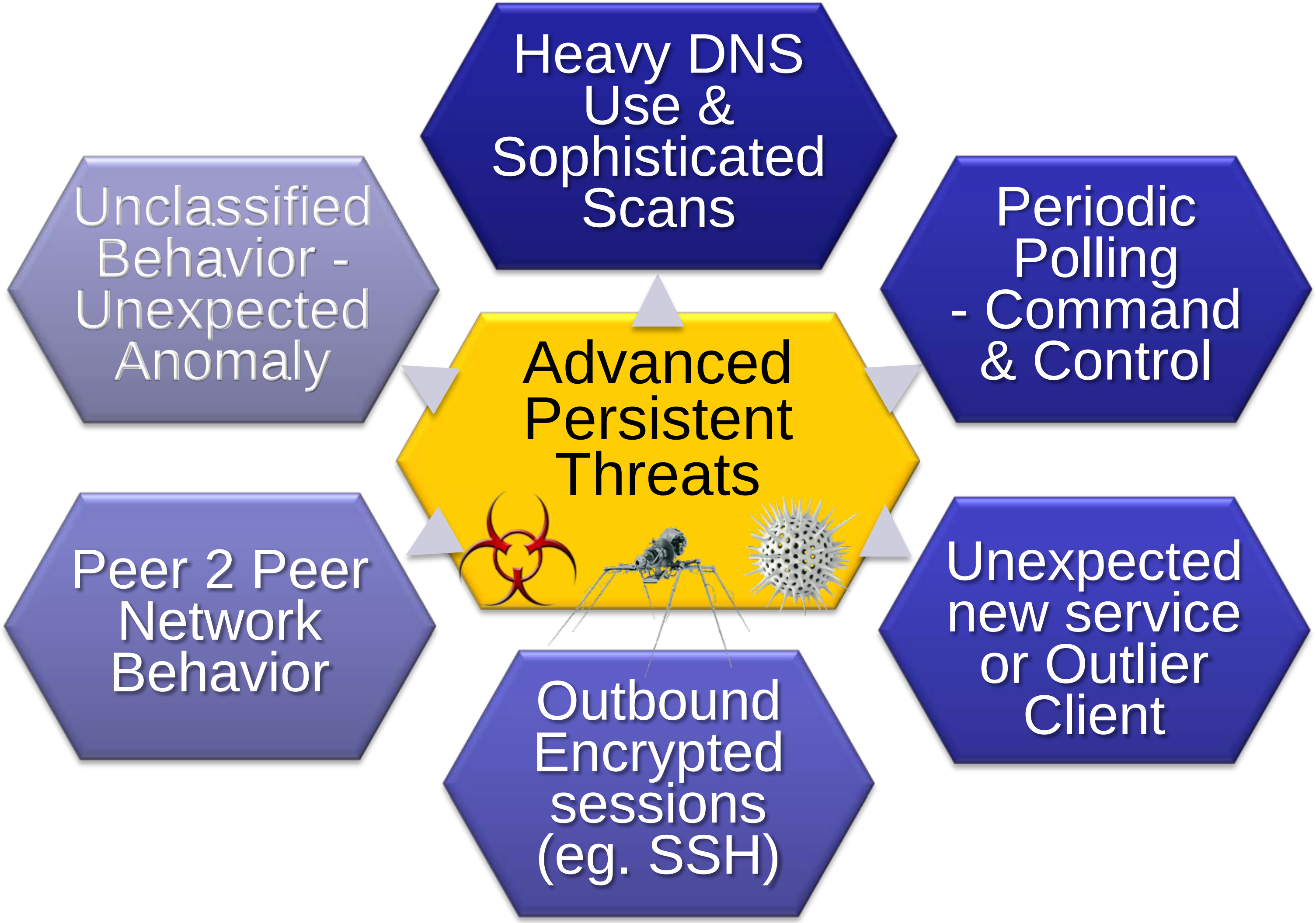
Command & Control (C&C)

- Remote servers operated by attacker control victim PCs
- Activity occurs outside of the normal hours, to evade detection

Management Console

- Interface used to control all aspects of the APT process
- Enables attackers to install new malware & measure success

Signs of ongoing APTs



Heavy DNS Use & Sophisticated Scans

Unclassified Behavior - Unexpected Anomaly

Periodic Polling - Command & Control

Advanced Persistent Threats

Peer 2 Peer Network Behavior

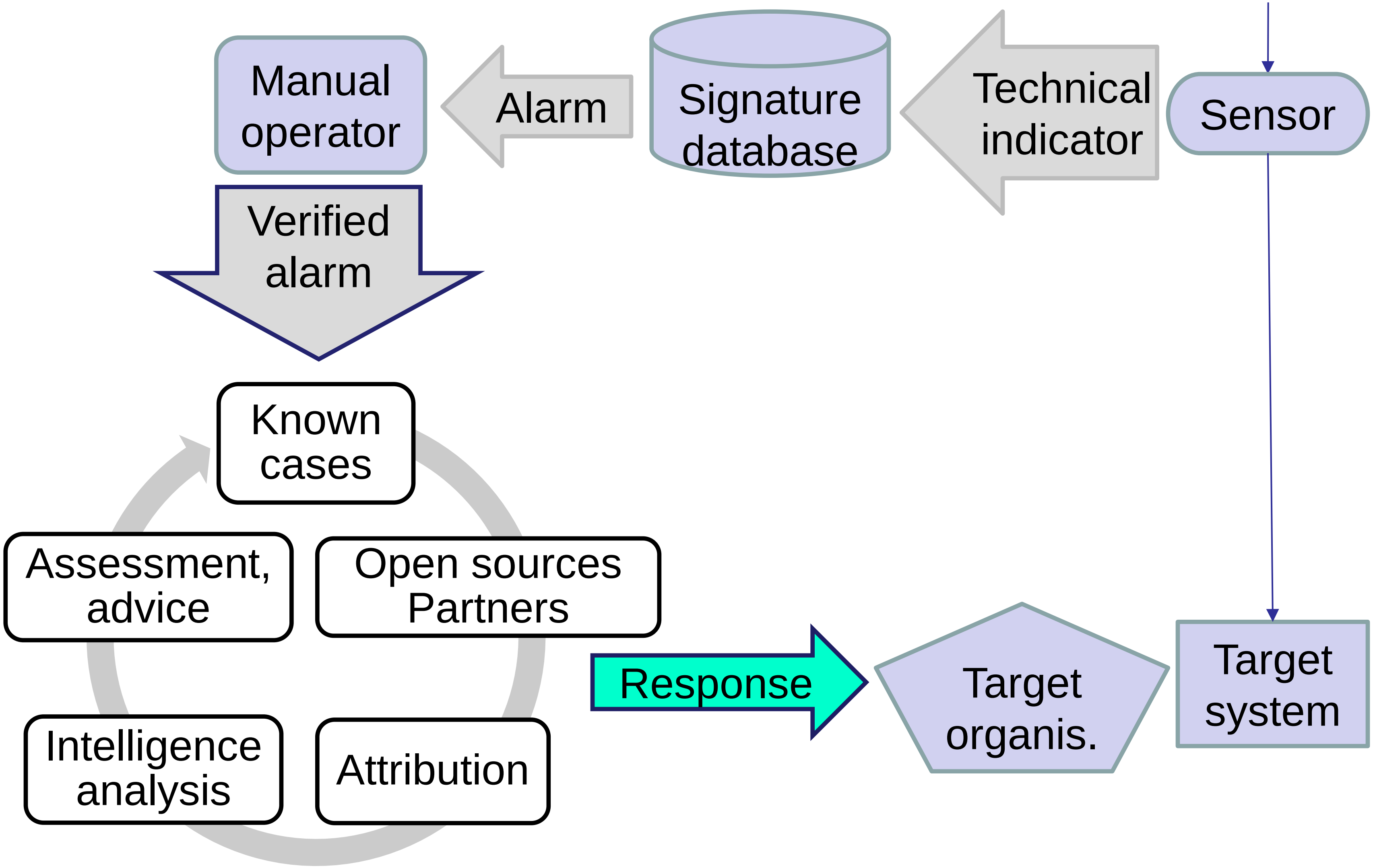
Unexpected new service or Outlier Client

Outbound Encrypted sessions (eg. SSH)

Computer Network Operations

- Defence of info systems is challenging
  - Expanding networks
  - Inter-dependency
  - Evolution of threats
- Framework for understanding CNO
  - Method for reducing complexity
  - Three major components
    - Actor
    - Operation
    - Intent

Present state of **Cyber Defence**



Manual operator

Alarm

Signature database

Technical indicator

Sensor

Verified alarm

Known cases

Assessment, advice

Open sources Partners

Intelligence analysis

Attribution

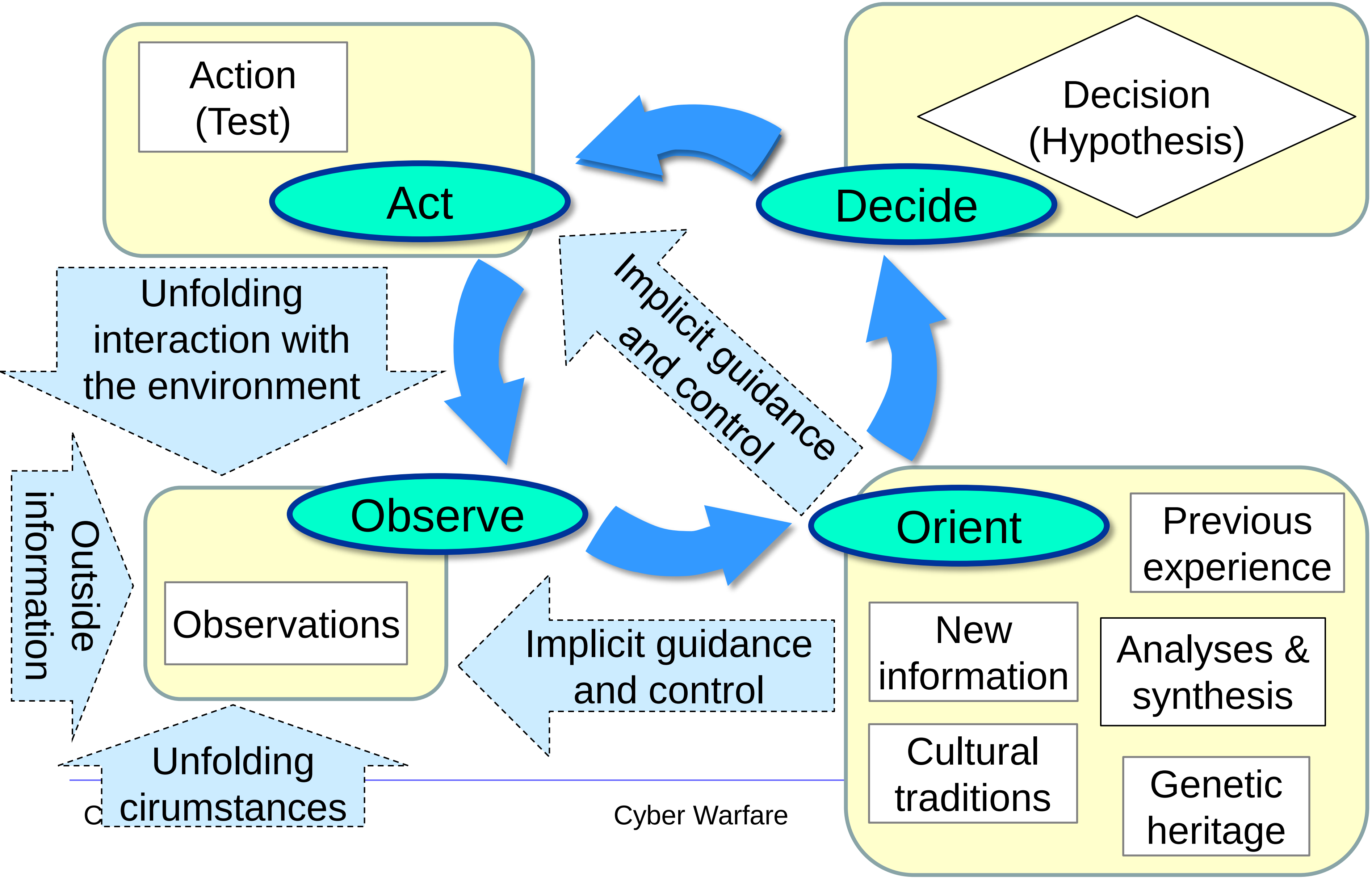
Response

Target organis.

Target system

OODA Loop

(J. R. Boyd, “the Essence of Winning and Losing,” 1995)



Action (Test)

Act

Decide

Decision (Hypothesis)

Unfolding interaction with the environment

Implicit guidance and control

Outside information

Observe

Observations

Orient

Previous experience

New information

Analyses & synthesis

Cultural traditions

Genetic heritage

Implicit guidance and control

Unfolding cirumstances

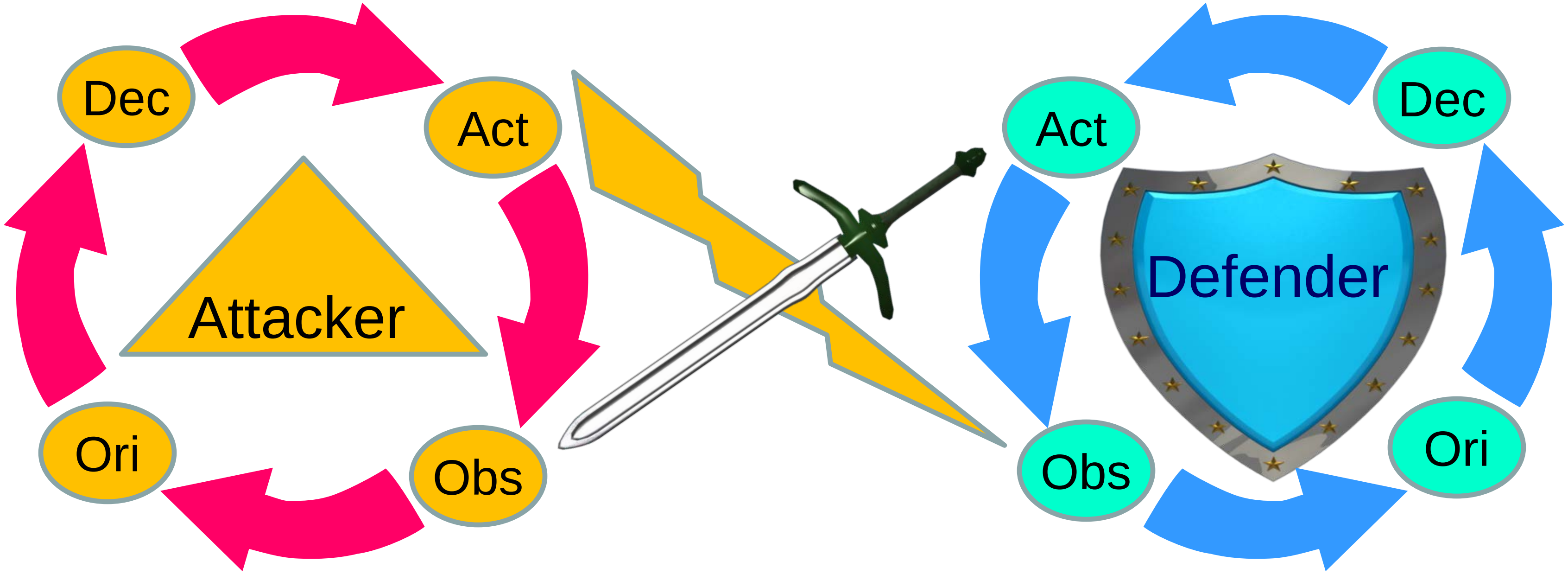
Preventive and reactive measures

- Delayed response favours the attacker
  - APT operations are conducted rapidly
  - Defenders have only hours or days to react from exploitation
- Preventive measures will only slow an attacker
- *How to effectively defend against APTs from a reactive position?*
- Consider the OODA Loop
  - **O**bserve
  - **O**rient
  - **D**ecide
  - **A**ct

OODA Loop

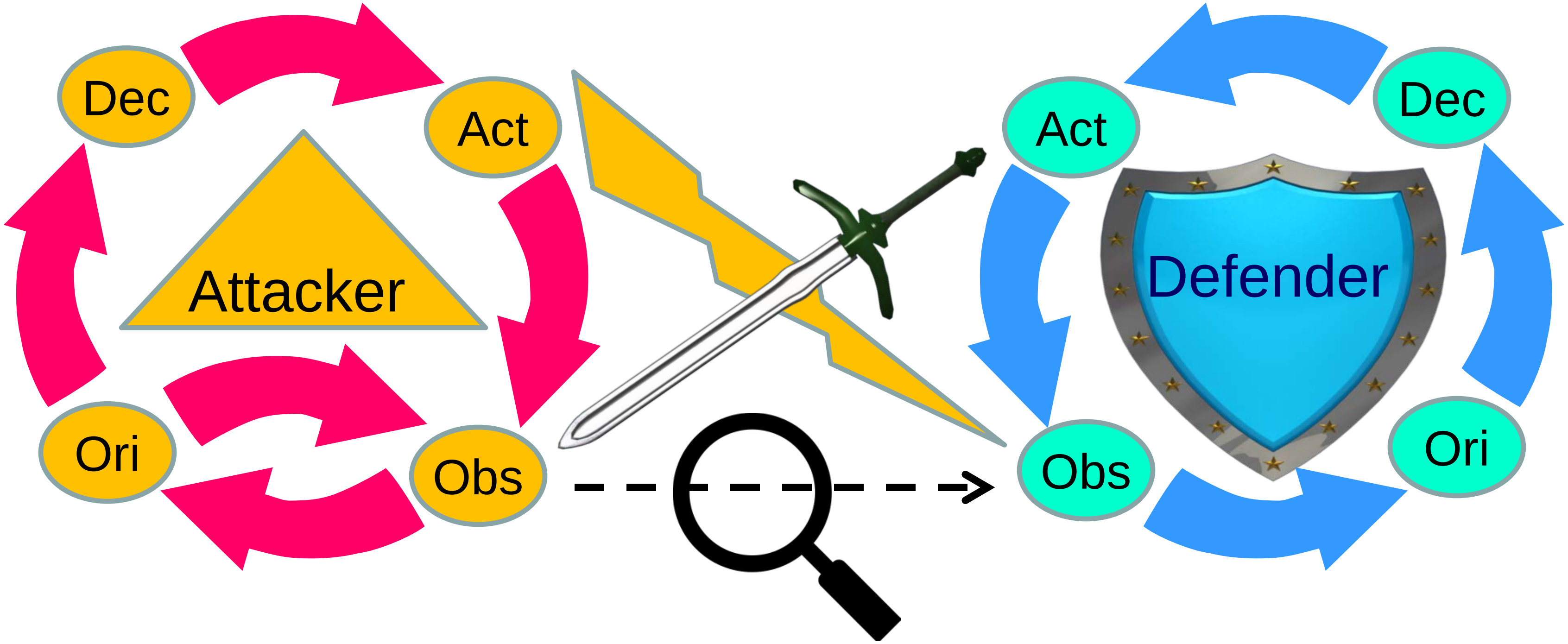
«Time is the dominant parameter. The pilot who goes through the OODA cycle in the shortest time prevails because his opponent is caught responding to situations that have already changed.»
Harry Hillaker
(chief designer
of the F-16)

Synchronous OODA loops



The attacker «wins»

Disrupting the opponent’s OODA loop



The defender «wins»

Current cyber defence challenges

- Confusion affects priorities which delays handling
- Warnings requires long «intel cycle» before response
  - Requires hours, days, or even weeks
- Partner involvement and sharing
  - Manual process
  - Partners with important information may be excluded due to workload
- Lacking information sharing standards
  - What did I just receive, and how important is it?
  - What is the basis for assessment?
  - Every partner will re-assess
  - The earlier it's shared, the less usable it is by partners – but the later it's shared, the less useful it is

Critical factors in understanding CNOs

- Different stakeholders when responding to a CNO
  - Company owners
  - Government and decision-makers
  - Armed forces
  - Intel & security analysts and handlers
  - Common need to understand three basic factors before response
- Actor
  - Who is responsible for the operation?
- Operation
  - What kind of operation is the actor conducting?
- Intent
  - What is the purpose of the operation?
  - Simplicity and speed is paramount

Actor types

- Generic levels based on principally different motives, manifestations, different capabilities and modus operandi
- State
  - Espionage, top level research, warfare
- Commercial
  - Competitive business and technology
- Organised Criminal group
  - Financial, criminal activity
- Terrorists
  - Destruction, death
- Idealists/other actors
  - Visible statements

Operation types

- Guideline - traditional military tactical objectives
  - A limited set of possible tasks
  - Based on common current understanding of the term CNO, this may include
  - Data Denial
  - Degrading
  - Disruption
  - Destruction
  - Theft
- Possibly other separate objectives as well
  - Resource access or takeover, such as in CNO Infrastructure development
  - Physical system manipulation or destruction, such as SCADA-system attacks

Intent

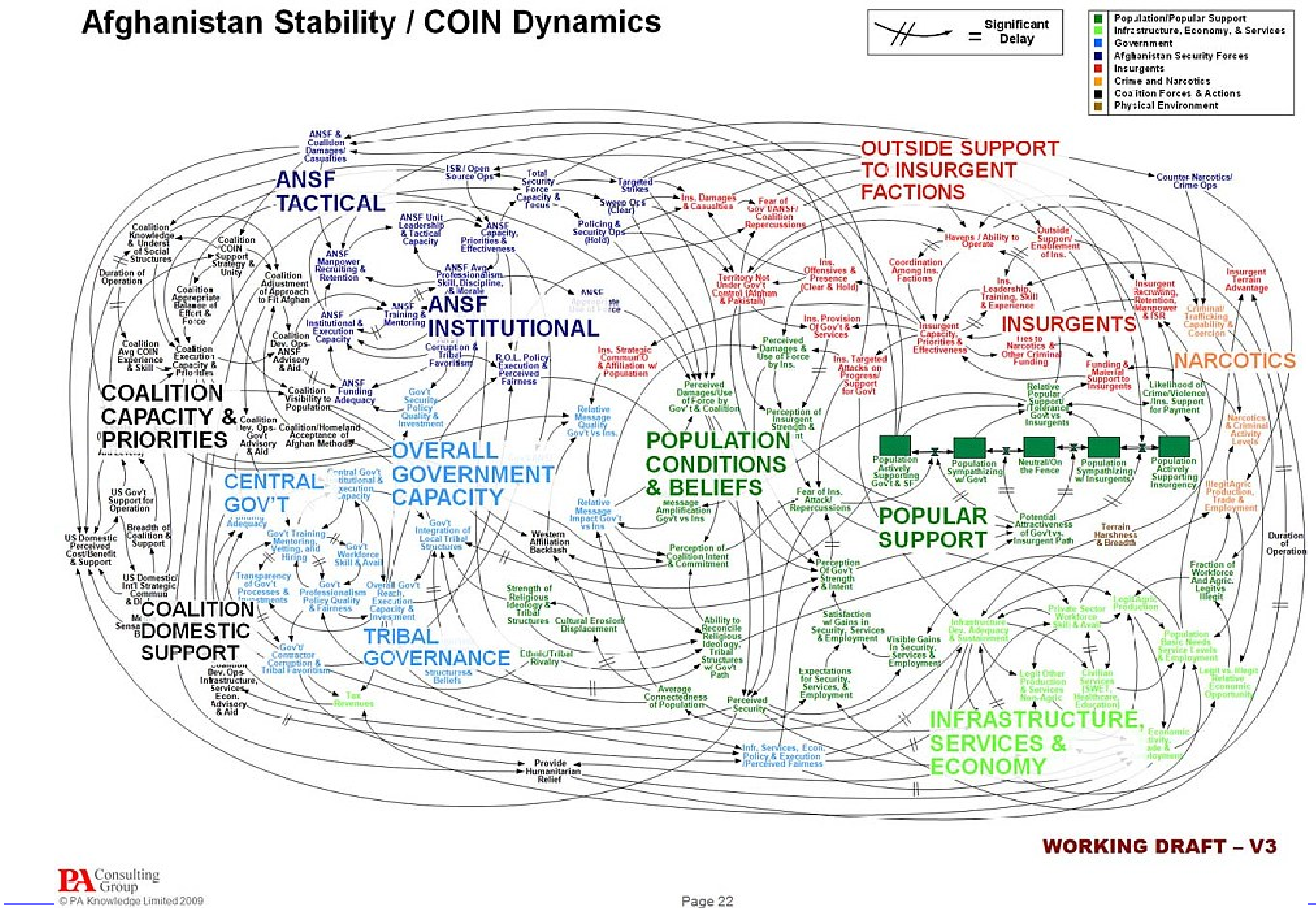
Most likely intent, given conflict type and intensity:

- Economic conflict at the hostile rhetoric level:
  - Intent: *Economic espionage*
- Political conflict at the sanctions level:
  - Intent: *Influence through information/psychological operation*
- Economic conflict at the deniable use of force level:
  - Intent: *Deny the target use of their resources*
- Territorial conflict at the conventional operations level:
  - Intent: *Territorial annexation*
- Cyber attacks:
  - Intent: *Same as related conventional conflict type*

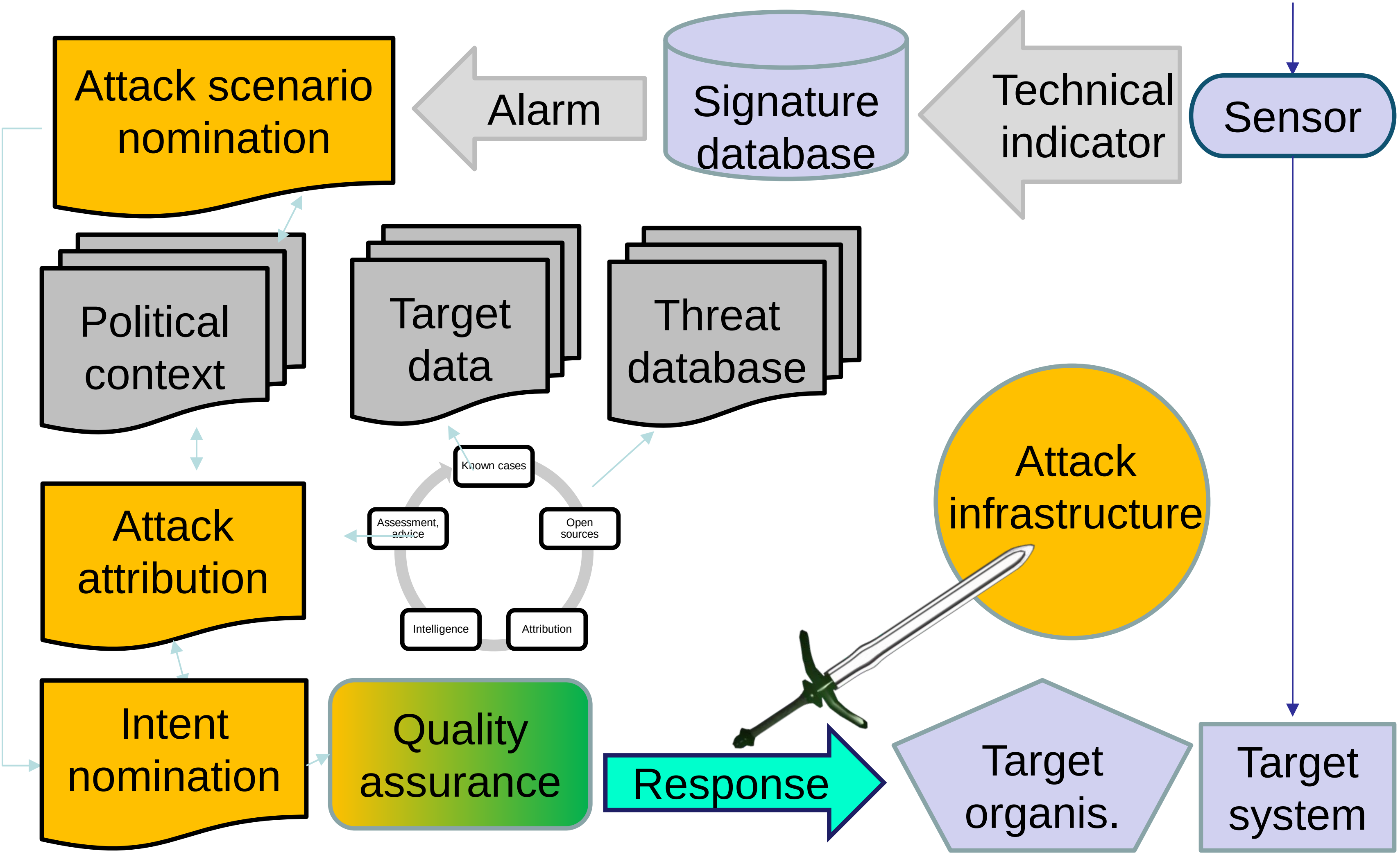
Modeling the strategic reality

- Conflict types and intensity levels needs calibration for each relevant actor in order to conduct a valid assessment of intent
- Cyber intelligence framework can describe
  - Actors with a set of known interests and capabilities
  - Operations based on the actor’s actions on a defined target,
  - Intents based on the general conflict types and intensities
- The framework can not provide the truth
- Intelligence analysis can only *reduce uncertainty*
- Offers a rational and predictable nomination of scenarios

Complexity out of control


Afghanistan Stability / COIN Dynamics
= Significant Delay
🟩 Population/Popular Support
🟩 Infrastructure, Economy, & Services
🟦 Government
🟦 Afghanistan Security Forces
🟥 Insurgents
🟧 Crime and Narcotics
⬛ Coalition Forces & Actions
🟫 Physical Environment
ANSF TACTICAL
ANSF INSTITUTIONAL
COALITION CAPACITY & PRIORITIES
CENTRAL GOV'T
OVERALL GOVERNMENT CAPACITY
COALITION DOMESTIC SUPPORT
TRIBAL GOVERNANCE
POPULATION CONDITIONS & BELIEFS
POPULAR SUPPORT
OUTSIDE SUPPORT TO INSURGENT FACTIONS
INSURGENTS
NARCOTICS
INFRASTRUCTURE, SERVICES & ECONOMY
ANSF & Coalition Damages/ Casualties
ISR / Open Source Ops
Total Security Force Capacity & Focus
Targeted Strikes
Sweep Ops (Clear)
Policing & Security Ops (Hold)
Ins. Damages & Casualties
Fear of Gov't/ANSF/ Coalition Repercussions
Counter Narcotics/ Crime Ops
ANSF Unit Leadership & Tactical Capacity
ANSF Capacity, Priorities & Effectiveness
ANSF Manpower Recruiting & Retention
ANSF Avg Professionalism, Skill, Discipline, & Morale
ANSF Training & Mentoring
ANSF Institutional & Execution Capacity
ANSF Funding Adequacy
ANSF Appropriate Use of Force
Coalition Knowledge & Underst of Social Structures
Coalition COIN Support Strategy & Unity
Duration of Operation
Coalition Appropriate Balance of Effort & Force
Coalition Adjustment of Approach to Fit Afghan
Coalition Avg COIN Experience & Skill
Coalition Execution Capacity & Priorities
Coalition Dev. Ops- ANSF Advisory & Aid
Coalition Visibility to Population
Coalition Dev. Ops- Gov't Advisory & Aid
Coalition/Homeland Acceptance of Afghan Methods
Corruption & Tribal Favoritism
R.O.L. Policy Execution & Perceived Fairness
Gov't Security Policy Quality & Investment
Relative Message Quality Gov't vs Ins.
Relative Message Impact Gov't vs Ins
Central Gov't Institutional & Execution Capacity
US Gov't Support for Operation
Breadth of Coalition & Support
US Domestic Perceived Cost/Benefit & Support
US Domestic/ Int'l Strategic Commun & DI
Gov't Training, Mentoring, Vetting, and Hiring
Gov't Workforce Skill & Avail
Transparency of Gov't Processes & Investments
Gov't Professionalism, Policy Quality & Fairness
Overall Gov't Reach, Execution Capacity & Investment
Gov't Integration of Local Tribal Structures
Western Affiliation Backlash
Gov't/ Contractor Corruption & Tribal Favoritism
Coalition Dev. Ops Infrastructure, Services, Econ. Advisory & Aid
Tax Revenues
Strength of Religious Ideology & Tribal Structures
Cultural Erosion/ Displacement
Ethnic/Tribal Rivalry
Provide Humanitarian Relief
Ins. Strategic Commun/IO & Affiliation w/ Population
Territory Not Under Gov't Control (Afghan & Pakistan)
Ins. Offensives & Presence (Clear & Hold)
Perceived Damages & Use of Force by Ins.
Ins. Provision Of Gov't & Services
Ins. Targeted Attacks on Progress/ Support for Govt
Perceived Damages/Use of Force by Gov't & Coalition
Perception of Insurgent Strength & Intent
Message Amplification Gov't vs Ins
Fear of Ins. Attack/ Repercussions
Perception of Coalition Intent & Commitment
Perception Of Gov't Strength & Intent
Ability to Reconcile Religious Ideology, Tribal Structures w/ Gov't Path
Satisfaction w/ Gains in Security, Services & Employment
Visible Gains In Security, Services & Employment
Expectations for Security, Services, & Employment
Average Connectedness of Population
Perceived Security
Infr, Services, Econ. Policy & Execution /Perceived Fairness
Havens / Ability to Operate
Outside Support/ Enablement of Ins.
Coordination Among Ins. Factions
Ins. Leadership, Training, Skill & Experience
Insurgent Capacity, Priorities & Effectiveness
Insurgent Recruiting, Retention, Manpower & ISR
Insurgent Terrain Advantage
Criminal/ Trafficking Capability & Coercion
Ties to Narcotics & Other Criminal Funding
Funding & Material Support to Insurgents
Relative Popular Support/ Tolerance Gov't vs Insurgents
Likelihood of Crime/Violence /Ins. Support for Payment
Narcotics & Criminal Activity Levels
Population Actively Supporting Gov't & SF
Population Sympathizing w/ Gov't
Neutral/On the Fence
Population Sympathizing w/ Insurgents
Population Actively Supporting Insurgency
Potential Attractiveness of Gov't vs. Insurgent Path
Terrain Harshness & Breadth
Illegit Agric. Production, Trade & Employment
Duration of Operation
Fraction of Workforce And Agric. Legit vs. Illegit
Legit Agric. Production
Private Sector Workforce Skill & Avail
Infrastructure Dev. Adequacy & Sustainment
Population Basic Needs Service Levels & Employment
Legit Other Production & Services Non-Agric
Civilian Services (SWET, Healthcare, Education)
Legit vs. Illegit Relative Economic Opportunity
Economic Activity, Trade & Employment
WORKING DRAFT – V3
PA Consulting Group
© PA Knowledge Limited 2009
Page 22

Model for Intel driven Cyber Defence



Attack scenario nomination

Alarm

Signature database

Technical indicator

Sensor

Political context

Target data

Threat database

Attack infrastructure

Attack attribution

Intent nomination

Quality assurance

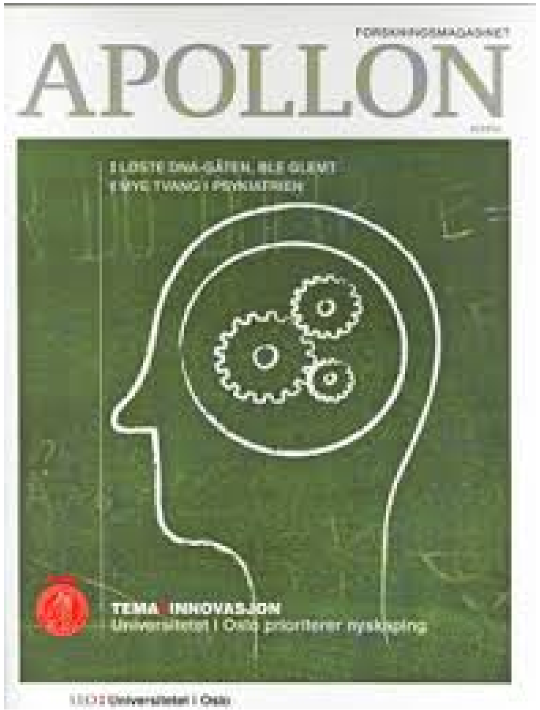
Response

Target organis.

Target system

Oslo Analytics Project

Better intelligence services based on a new mathematical logic from UiO could have averted the attack on Saddam



FORSKNINGSMAGASINET

APOLLON

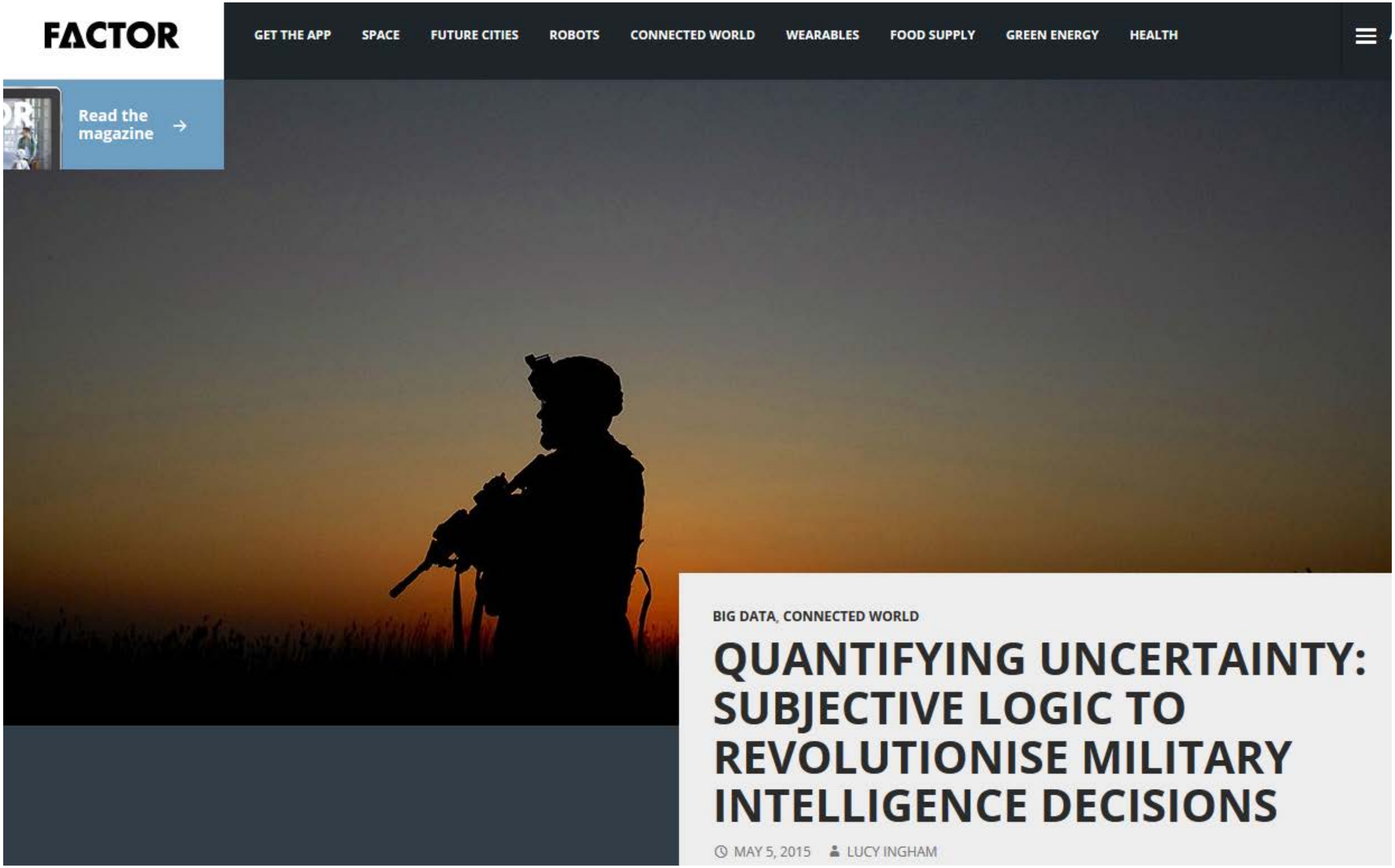
I LØSTE DNA-GÅTEN, BLE GLEMT
I MYE TVANG I PSYKIATRIEN

TEMA INNOVASJON
Universitetet i Oslo prioriterer nyskaping

UiO : Universitetet i Oslo

April 2015

Oslo Analytics Project

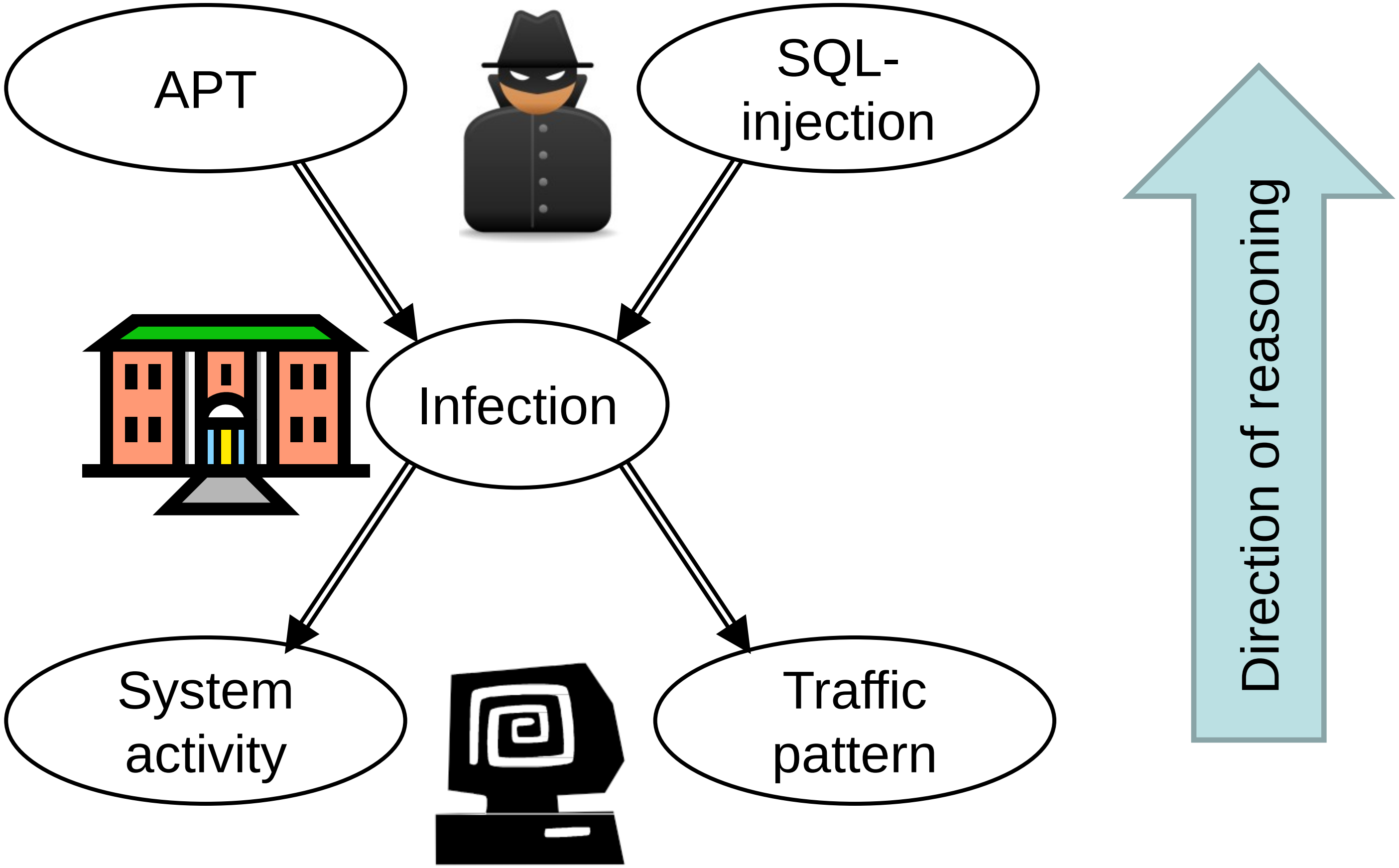


BIG DATA, CONNECTED WORLD

QUANTIFYING UNCERTAINTY: SUBJECTIVE LOGIC TO REVOLUTIONISE MILITARY INTELLIGENCE DECISIONS

MAY 5, 2015 LUCY INGHAM

Bayesian reasoning



End of Lecture