Computational Cybersecurity for Incident Handling Information Sharing

Marcos Osorno, Thomas Millar, Paul Cichonski

Presented by: Marcos Osorno

marcos.osorno@jhuapl.edu

Johns Hopkins University Applied Physics Laboratory

GFIRST 2011

US-CERT

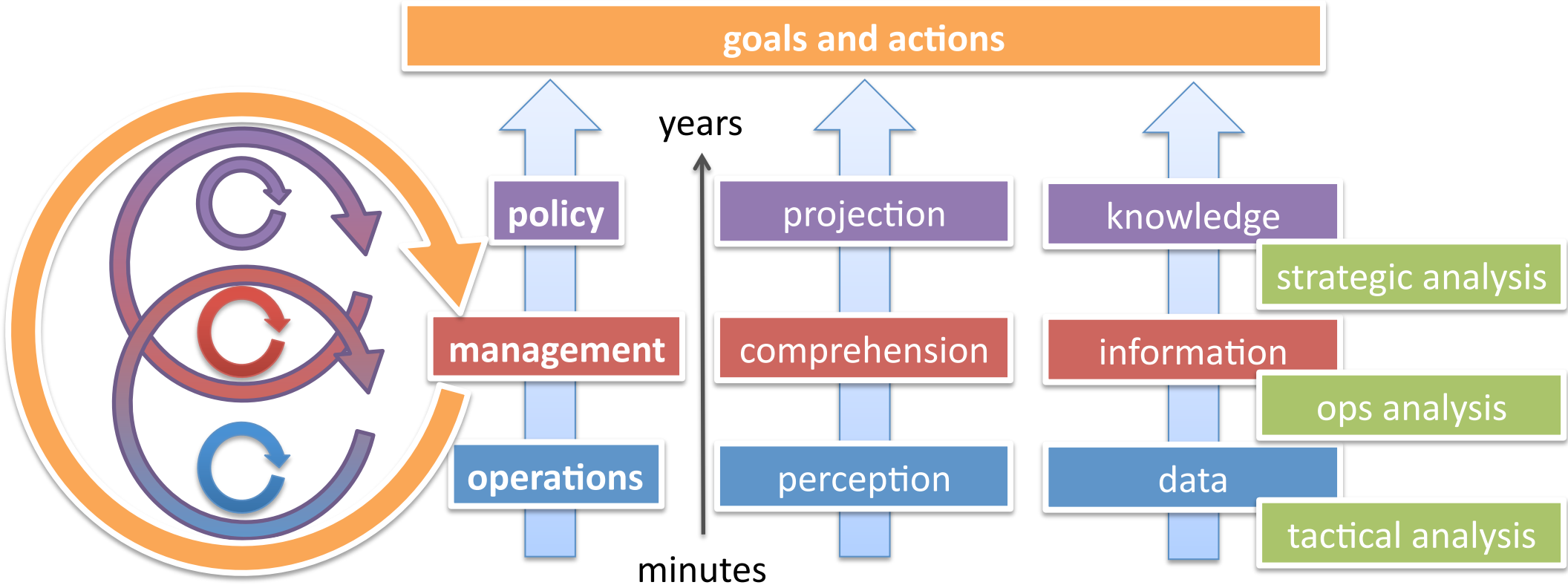
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

APL

Part I: Building a discipline

The deceptive ease by which we can extrapolate our everyday experiences (getting lost, forgetting, not paying attention, and so forth) to understand the complex events we hear or read about make us blind to the fact that such descriptions are not scientific explanations. *Dekker, Human Factors and Folk Models, 2004*

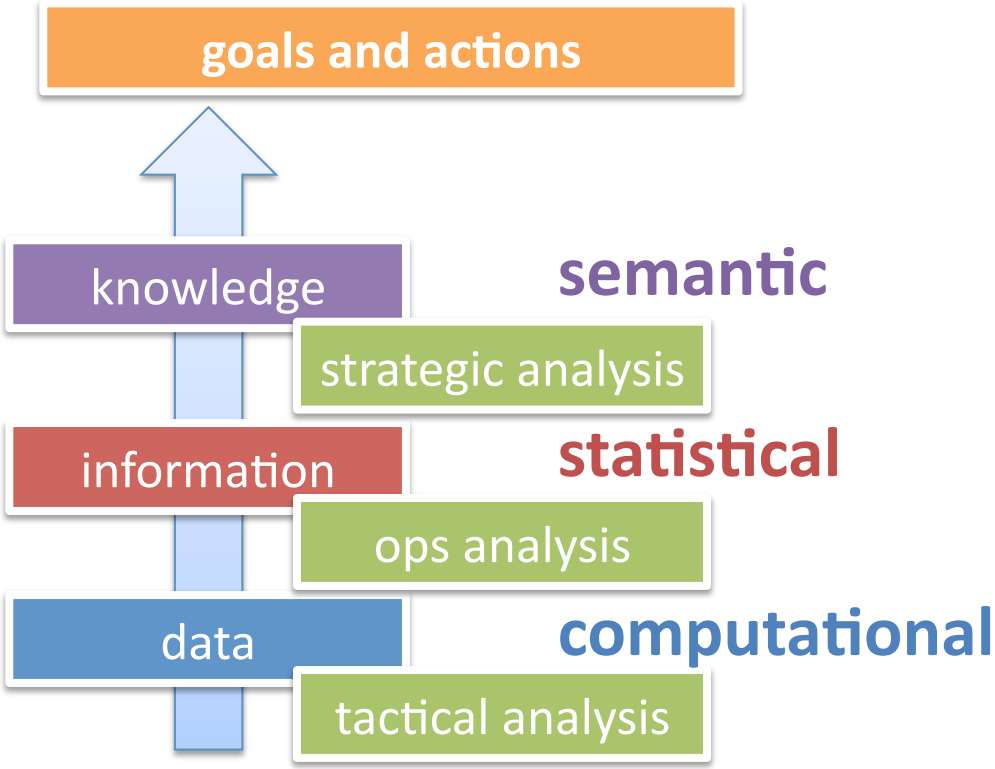
How does it fit together?



large scale, distributed

computational, *statistical*, and *semantic* **cybersecurity science**

Turning data into knowledge



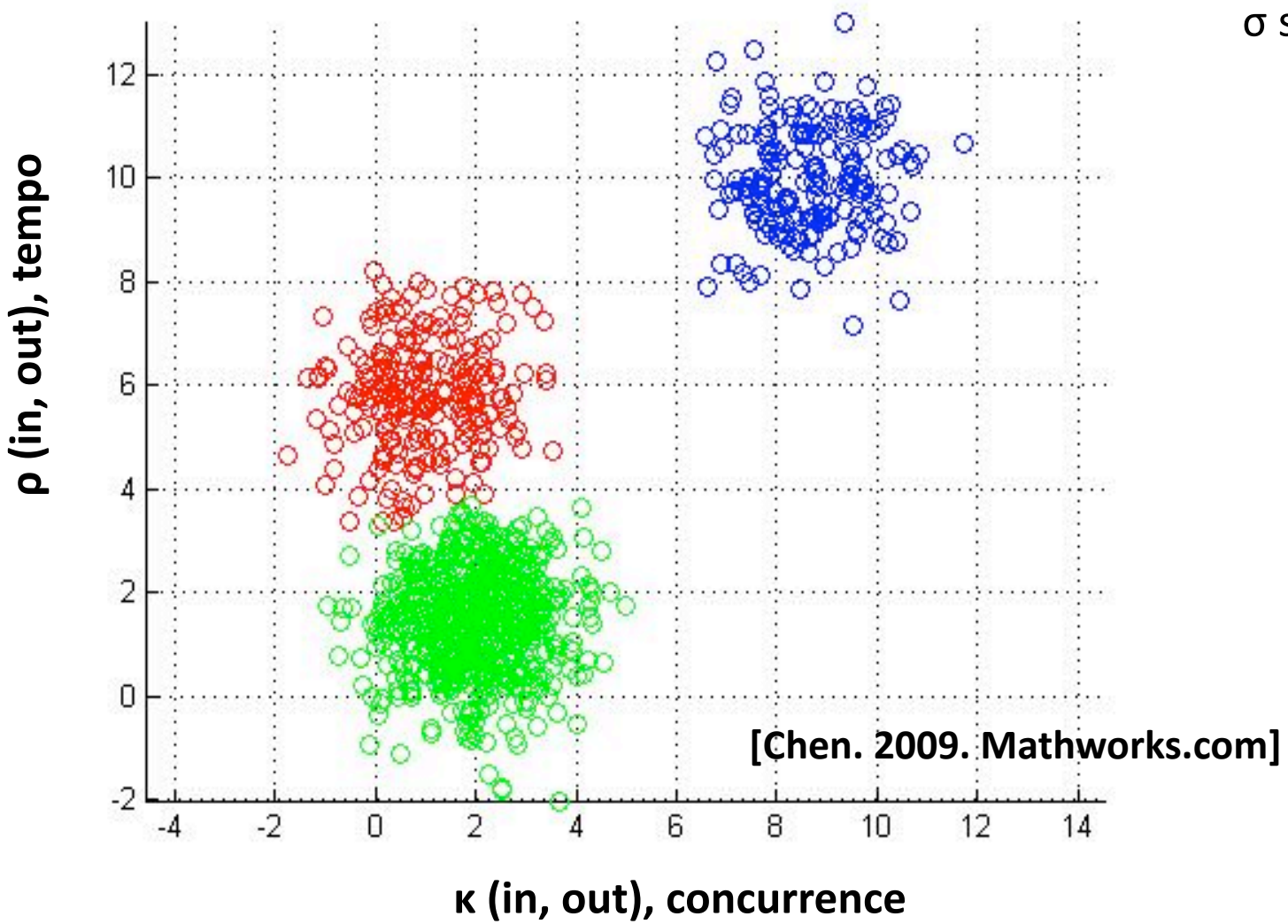
- startlingly disjoint (data vs KR, inter-schema, intra-schema)
- operators, ontologists, folksonomists
- tracing from binary to OWL
- tracing to goals, actions
- a lot of slop in the nouns (botnet, malicious, signatures, indicators etc.)
- and verbs (fusion, inference, correlation, enrichment)
- we should be <u>service</u>, <u>not schema</u> focused

large scale, distributed

computational, *statistical*, and *semantic* **cybersecurity science**

Perception

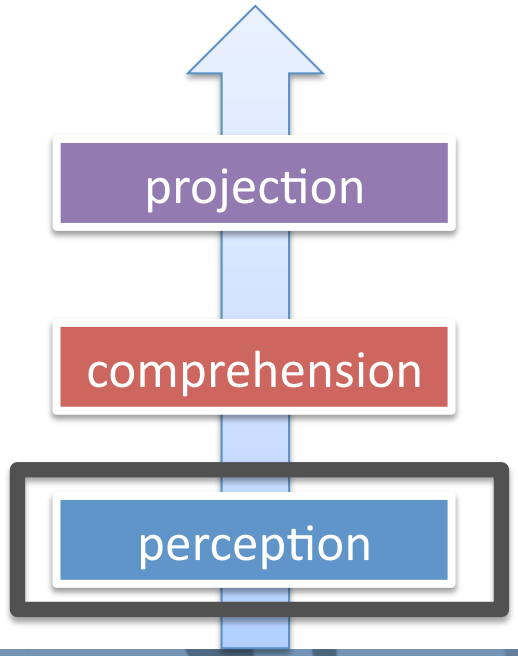
Concurrence vs Session Initiation (7 day average)



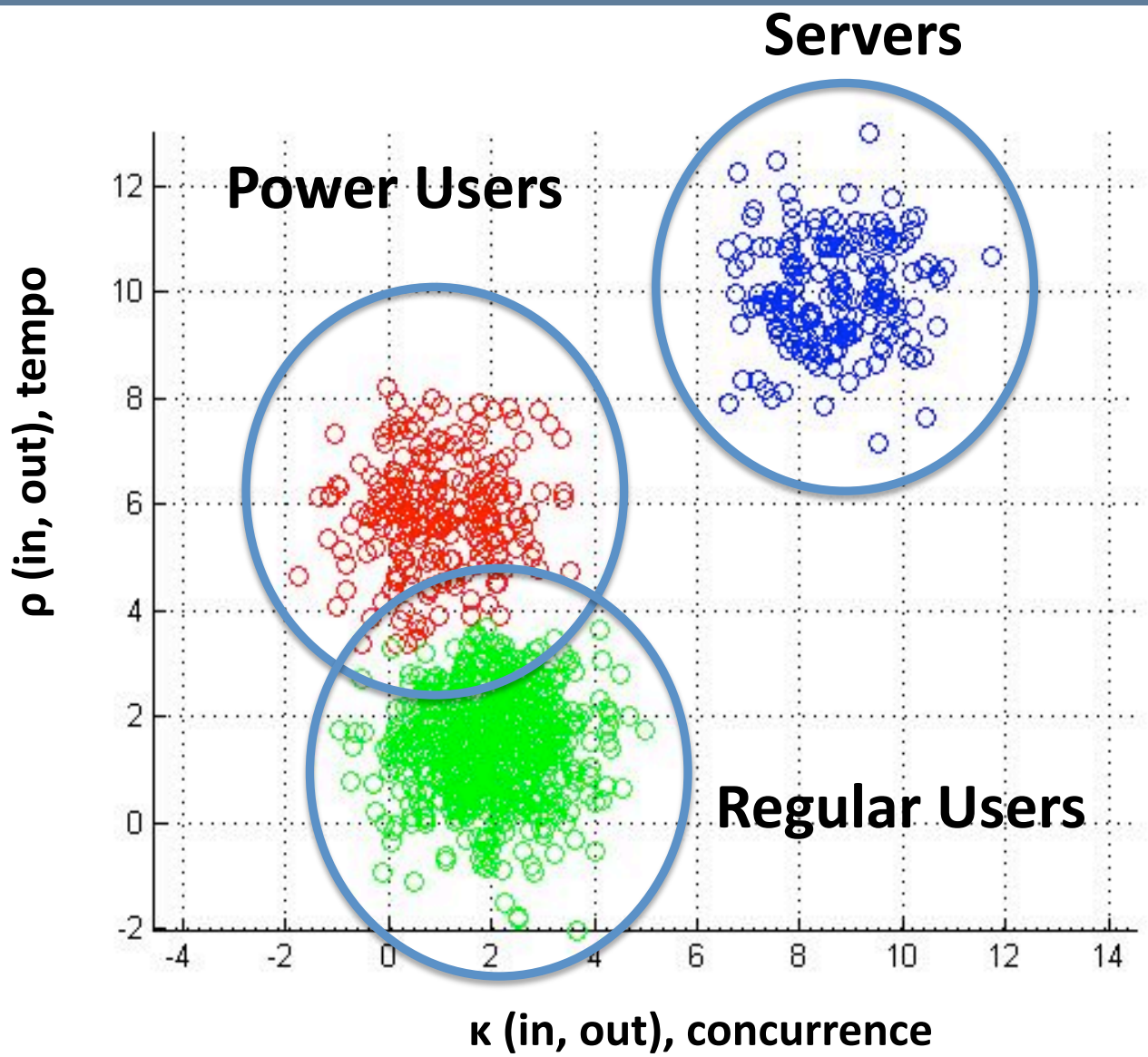
TCP/IP measurements

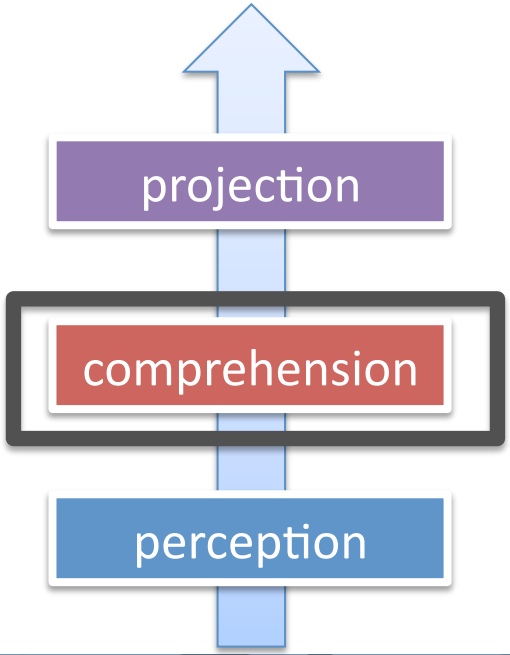
σ segment, τ type

- **κ (in, out), concurrence**
- **ρ (in, out), tempo**
- ψ (in, out), speed
- υ (in, out), volume

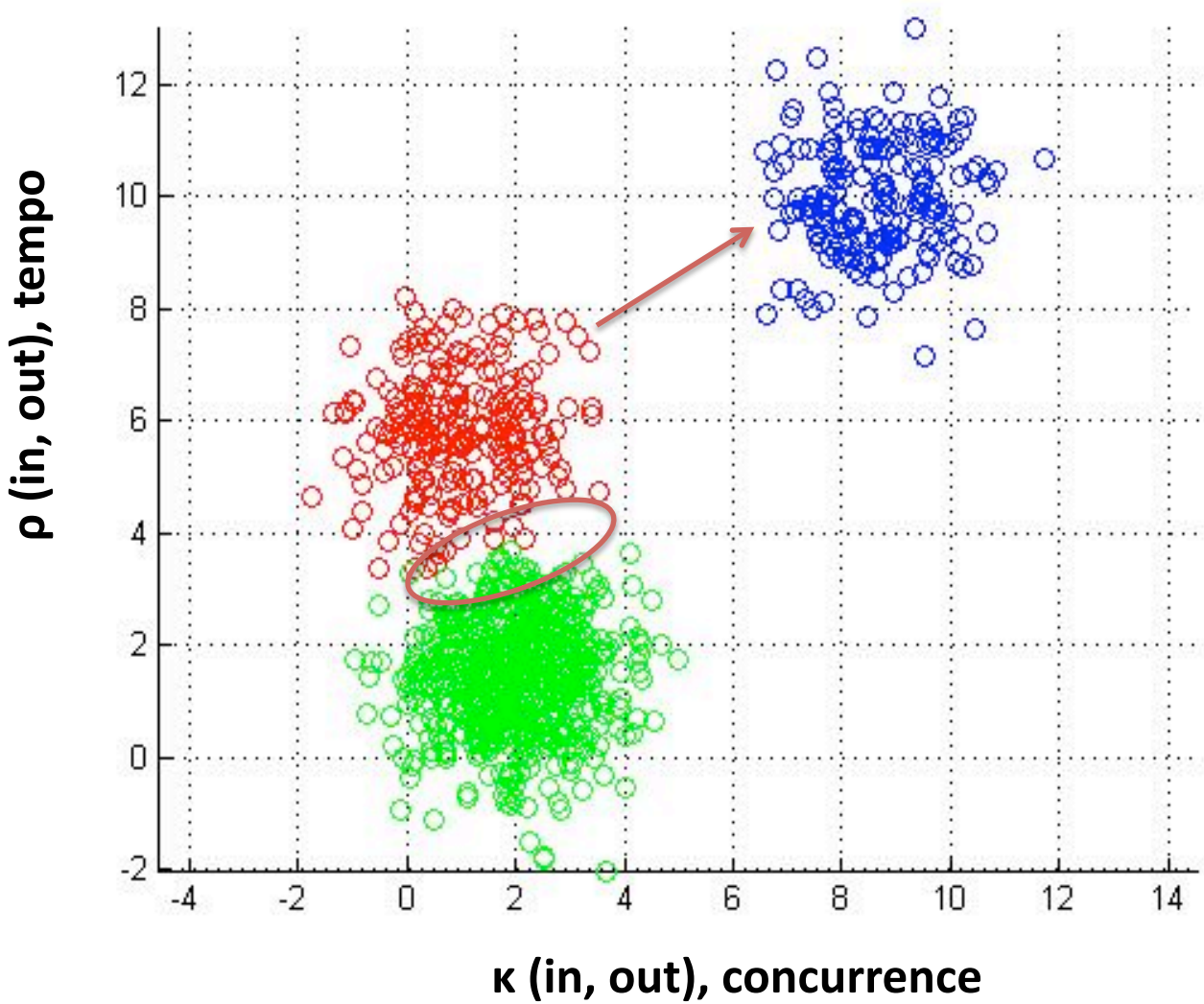


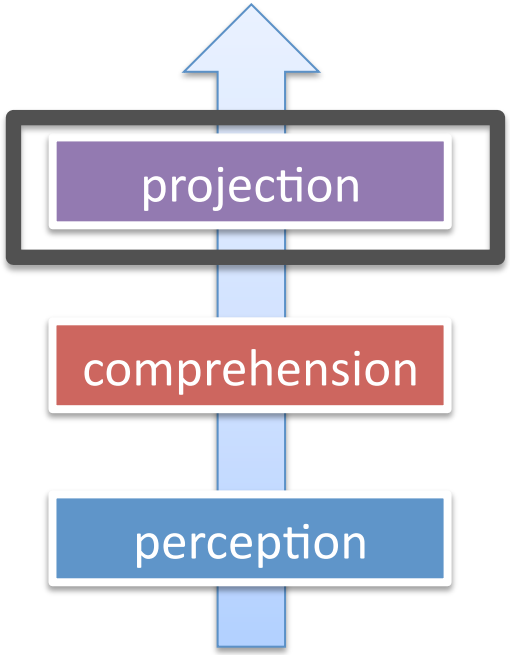
Comprehension



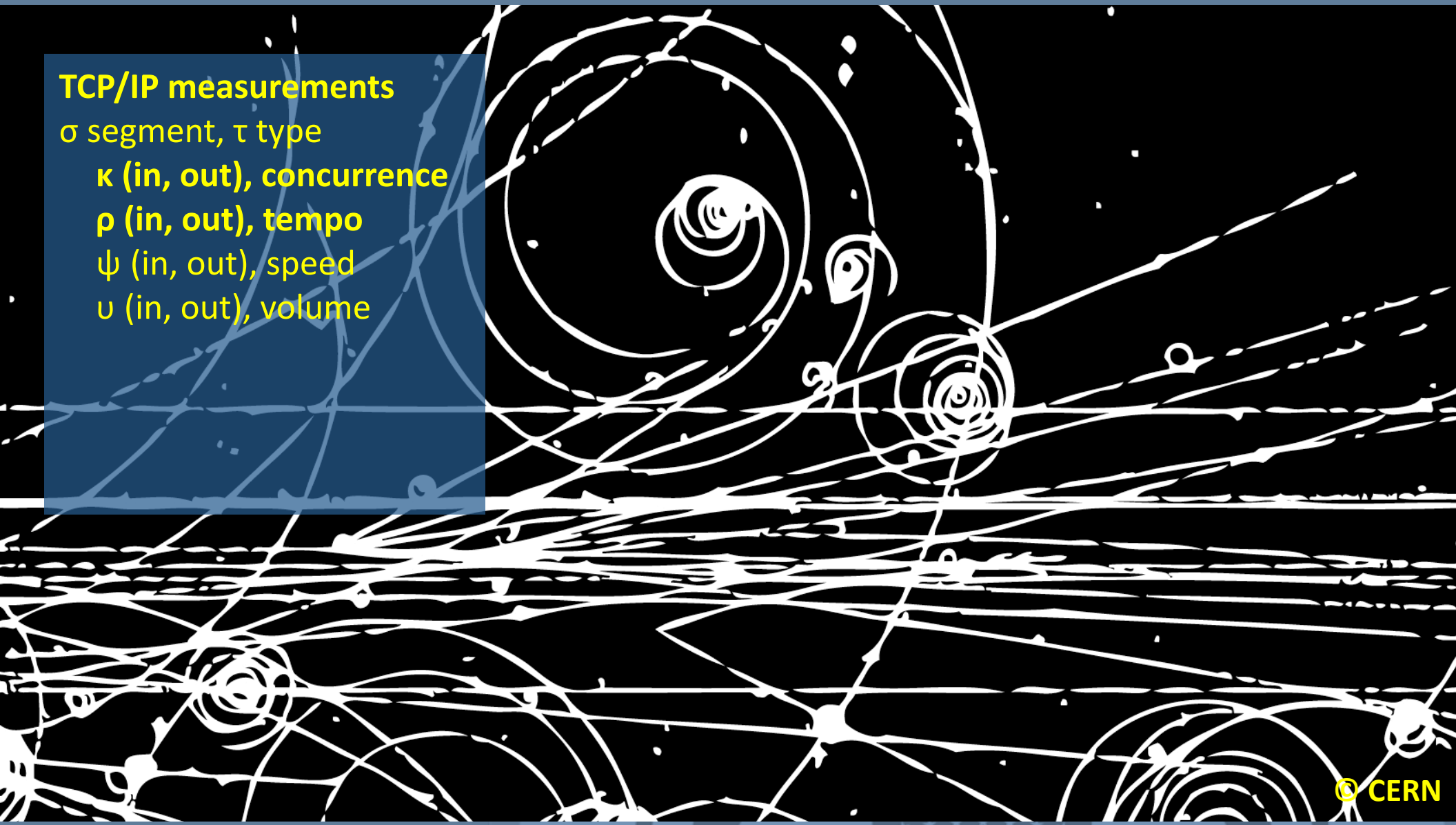


Projection


ρ (in, out), tempo
κ (in, out), concurrence
12
10
8
6
4
2
0
-2
-4
-2
0
2
4
6
8
10
12
14


projection
comprehension
perception

What are the phenomena?

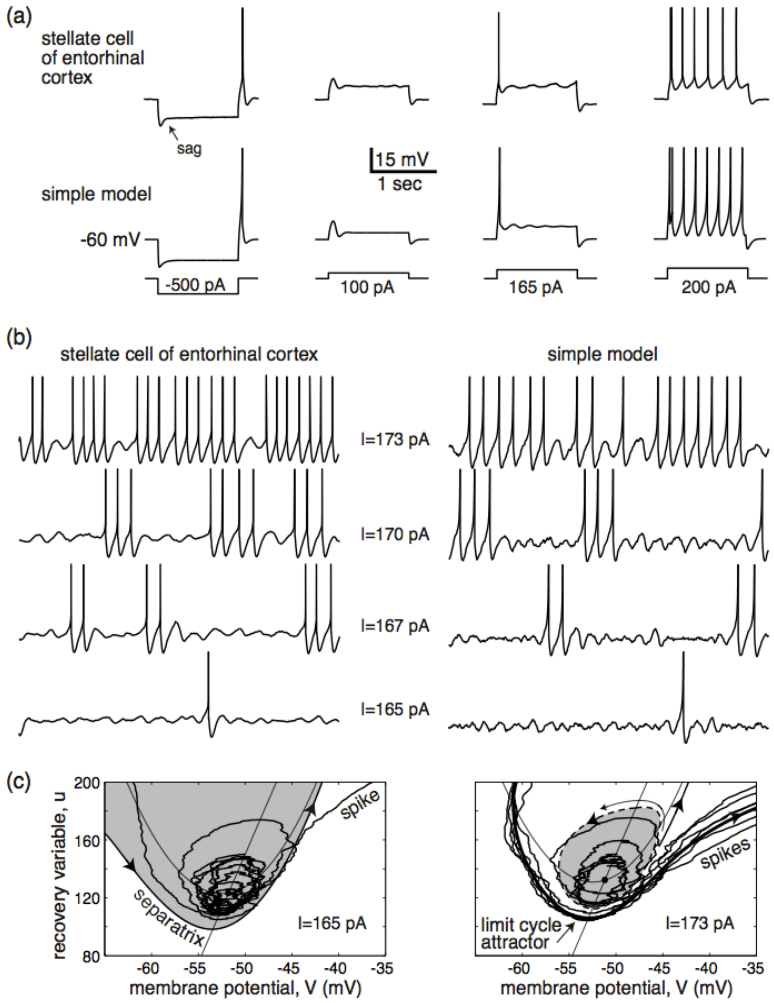


TCP/IP measurements

σ segment, τ type

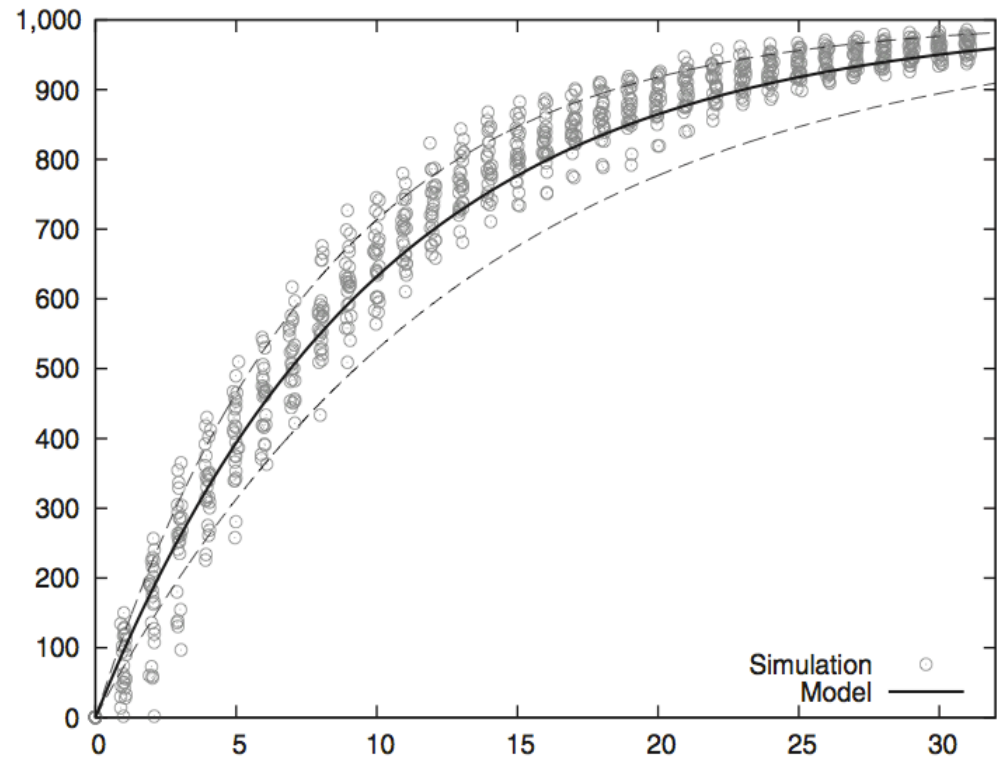
- **κ (in, out), concurrence**
- **ρ (in, out), tempo**
- ψ (in, out), speed
- υ (in, out), volume

What are the functions and methods?



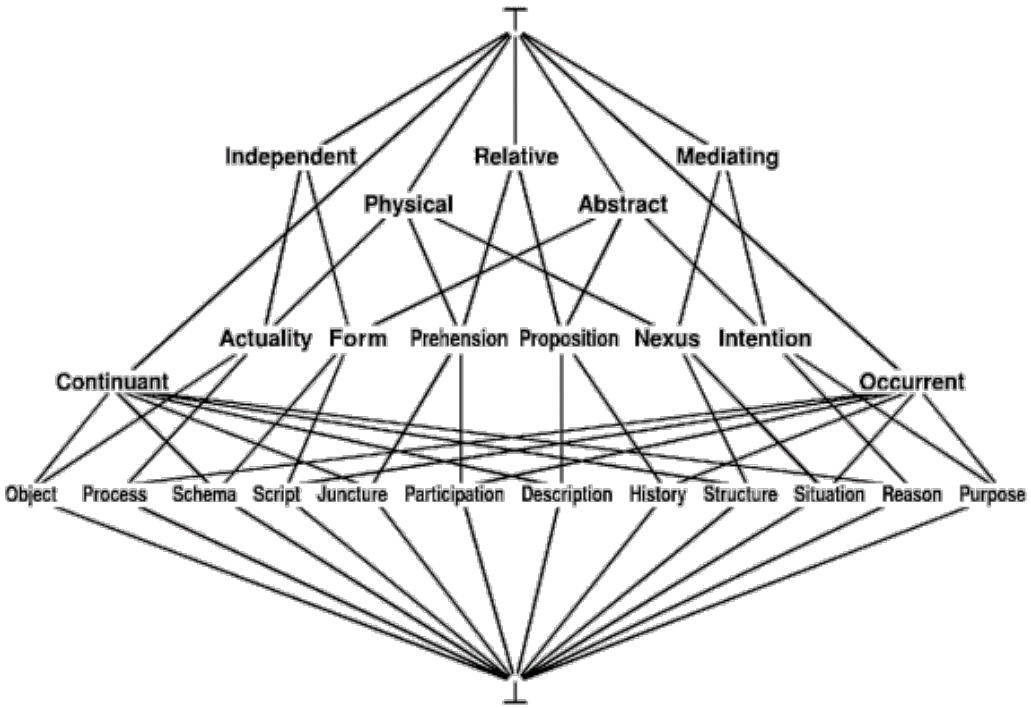
[Izhikevich, 2007]

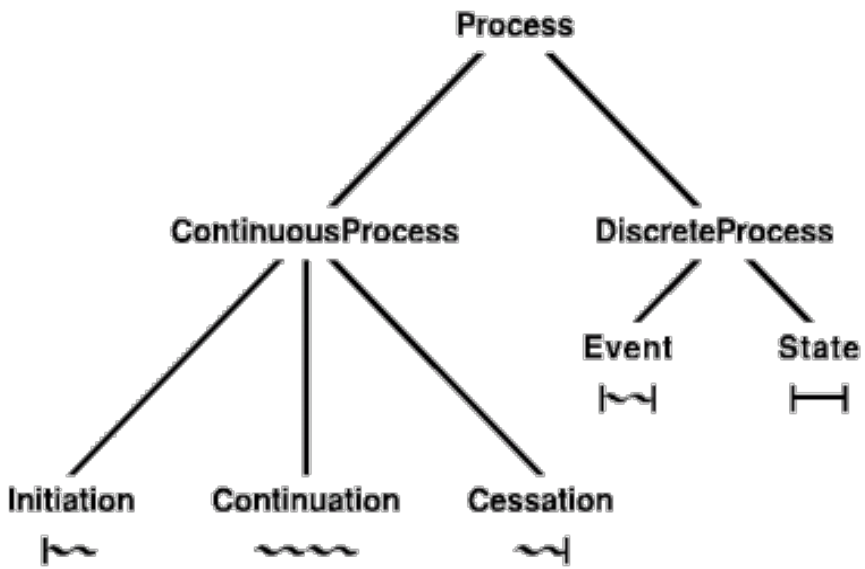
$$E[r(m)] = c_1 \int_0^n m\, p(m)\, \mathrm{d}m + c_1 \int_n^\infty n\, p(m)\, \mathrm{d}m - c_0 n \int_0^\infty p(m)\, \mathrm{d}m$$
$$= c_1 \int_0^n m\, p(m)\, \mathrm{d}m + c_1 n \left(1 - \int_0^n p(m)\, \mathrm{d}m\right) - c_0 n$$



[Janert, 2011]

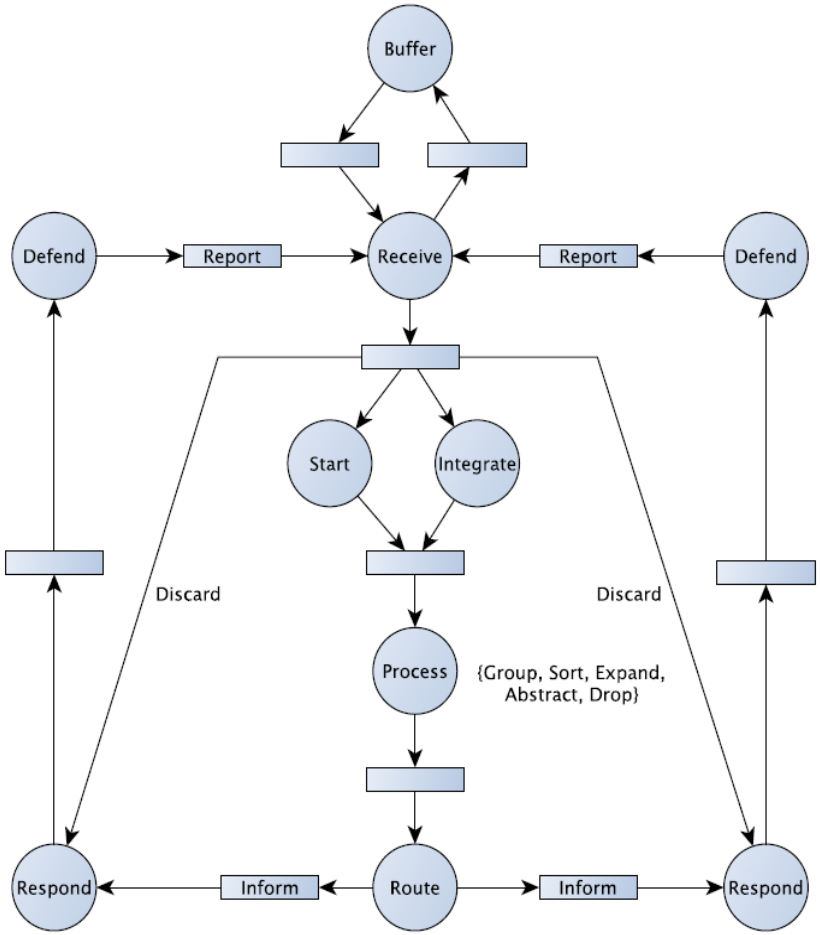
What are we talking about?

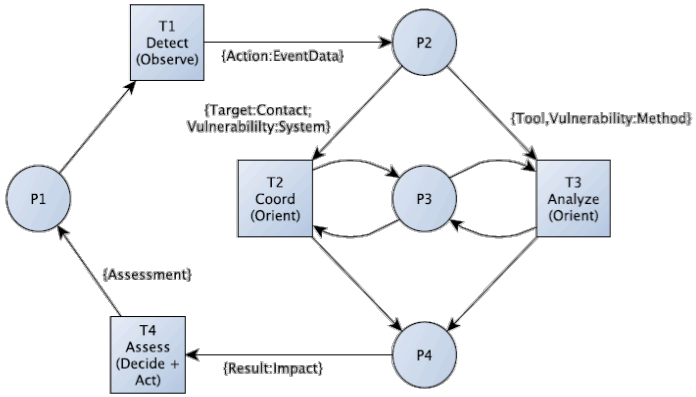




[Sowa, 1999]

How are we managing it?



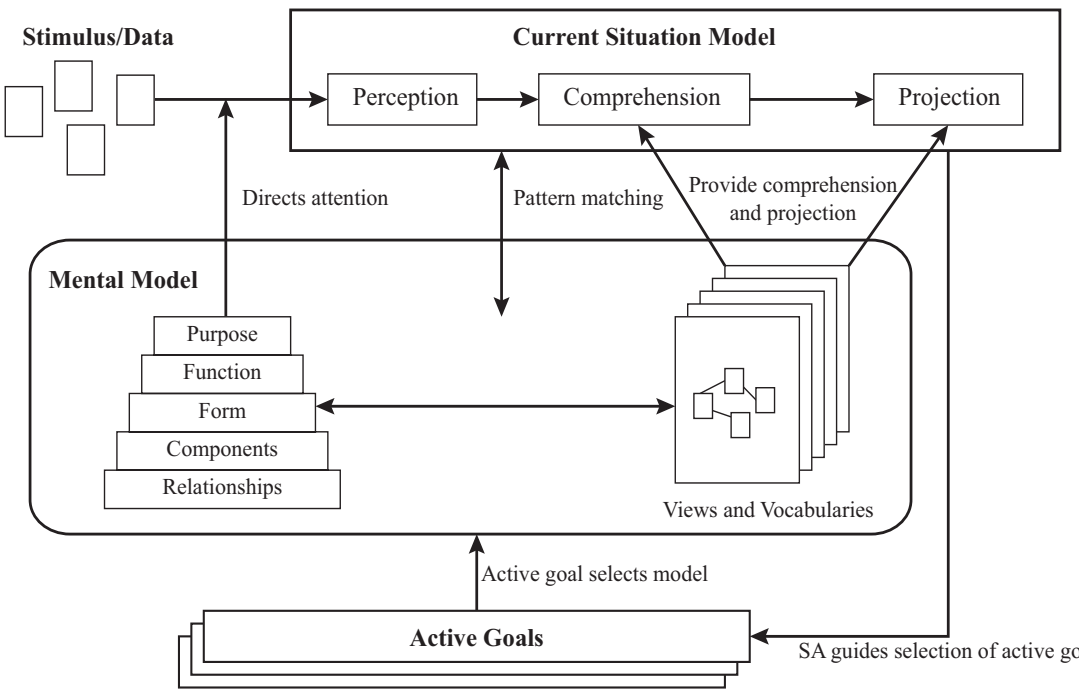


$defender$ = new $Contact$
$analyst$ = new $Contact$
$handler$ = new $Contact$
loop
  while $defender.detect(action) == false$ **do**
    $defender.continousMonitoring$ {P1}
  end while{T1}
  $handler \leftarrow defender.eventData$ {P2}
  $target = defender.eventData.System$
  $vulnerability[] = target.OperatingSystem$
  $vulnerability[] = target.Service$
  $vulnerability[] = target.Application$
  $tool = defender.eventData.Method$
  while $handler.resultKnown == false$ **do**
    $handler.coordinate(target, vulnerability)$ {T2}
    $analysis.analyze(tool, vulnerability)$ {T3}
  end while{P3}
  $impact = analysis.determine(result)$ {P4}
  $defender.assess(impact)$ {T4}
end loop

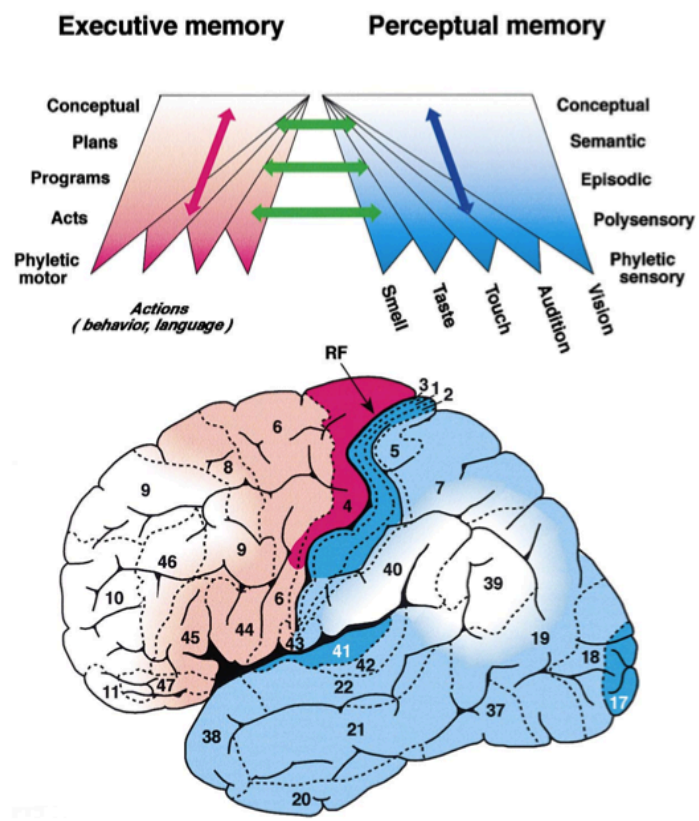
[Osorno, Millar, Rager. Unpublished notes]

How do we know what we're doing?

goals and actions



[Endsley, 2003]



[Fuster, 2011]

Word of warning from the IC

Tradecraft* implies a mysterious process learned only by the initiated and acquired only through elaborate rituals of professional indoctrination. It also implies that the methods and techniques of analysis are informal, idiosyncratic, unverifiable, and perhaps unexplainable.

*Rob Johnston, Analytics Culture in the US Intelligence Community, 2005 (*and other pseudoscientific jargon. Ed.)*

Part II: Building a model

The greatest risk of folk models is that they appear to make sense, even though statements and conclusions may not be falsifiable. They therefore may seem more plausible than articulated models since the latter require an understanding of the underlying mechanisms. *Dekker, Human Factors and Folk Models, 2004.*

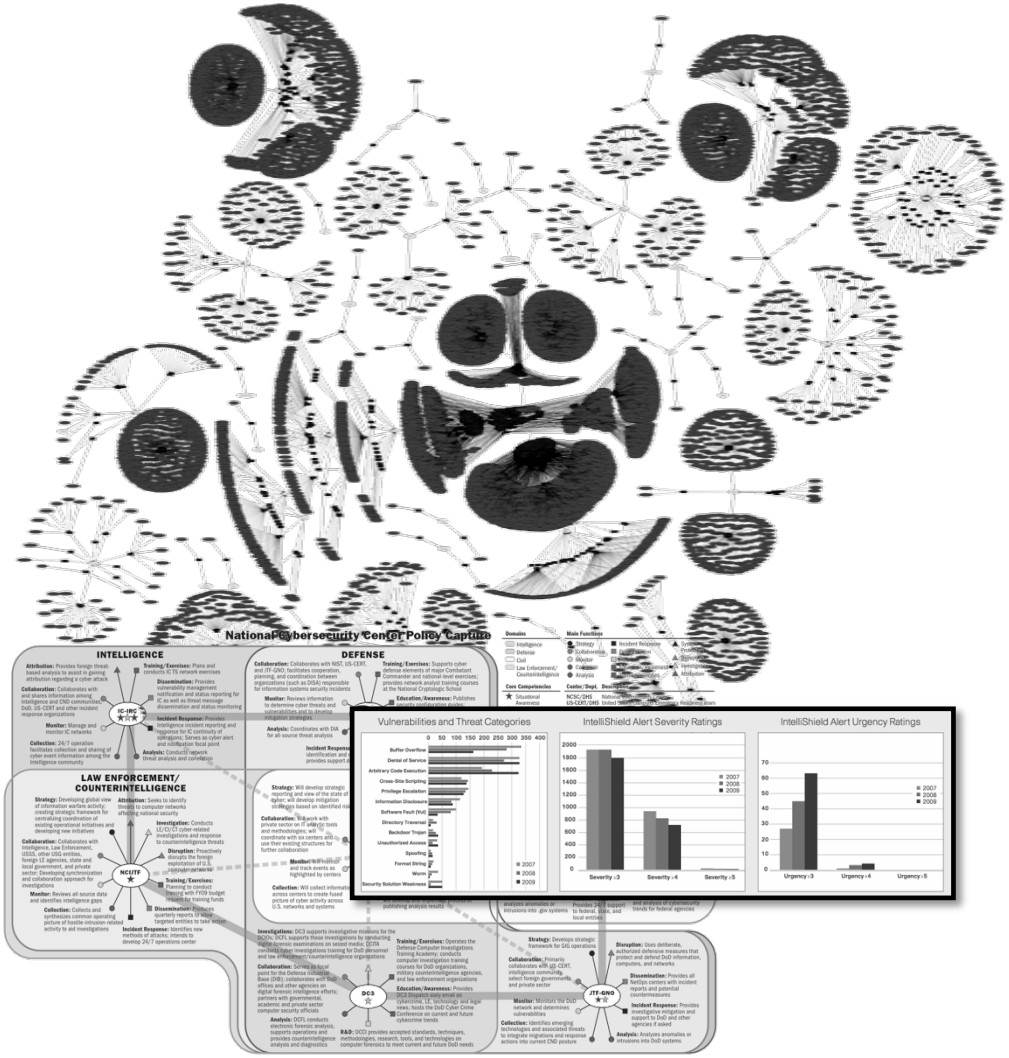
I'm going to cruise through this. If you want more information come and see us in **Presidential Chamber B**

What are we trying to do?

Inform the design of a domestic federal network defense cybersecurity incident handling system by creating a coordinated, distributed incident handling process.

US-CERT + NIST + JHU/APL

Scale & diversity



United States Government

1.9 million federal employees

1.25 million in federal civil sector

100+ department and agencies

208 thousand in largest dept

4 thousand in smallest dept

80.4% in IS/IT dependent work

354 million ft^2 in 8,600 buildings

2,758 access points (2008)

16,843 incident reports in 2008

206% increase from 2006

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

APL

Current incident handling processes

2004: **US National Institute of Standards and Tech.**

Background

1990: Lawrence Livermore National Labs

2004: US National Institute of Standards and Tech.

Current trends

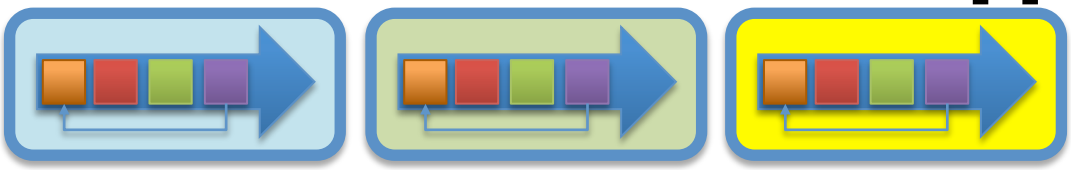
1990: Lawrence Livermore National Labs

2004: US National Institute of Standards and Tech.

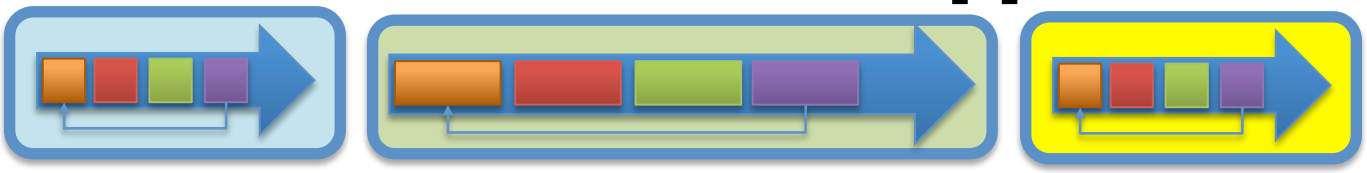
2009: Chairman of the Joint Chiefs of Staff

What about multiple incidents?

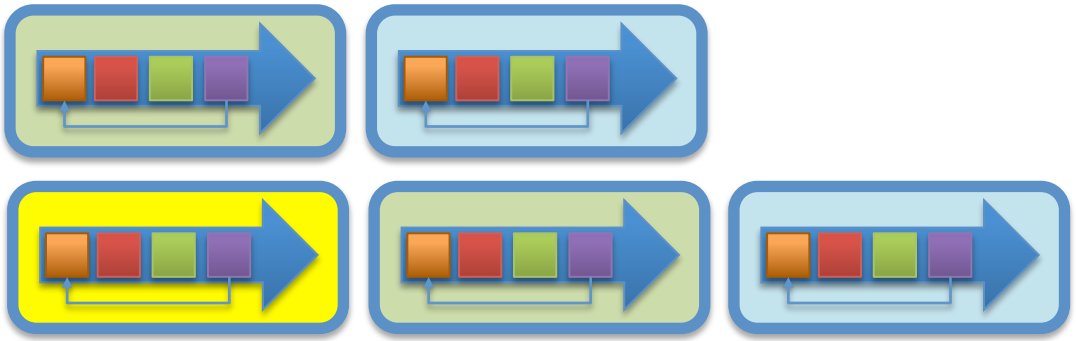
A: Serial constant time approach



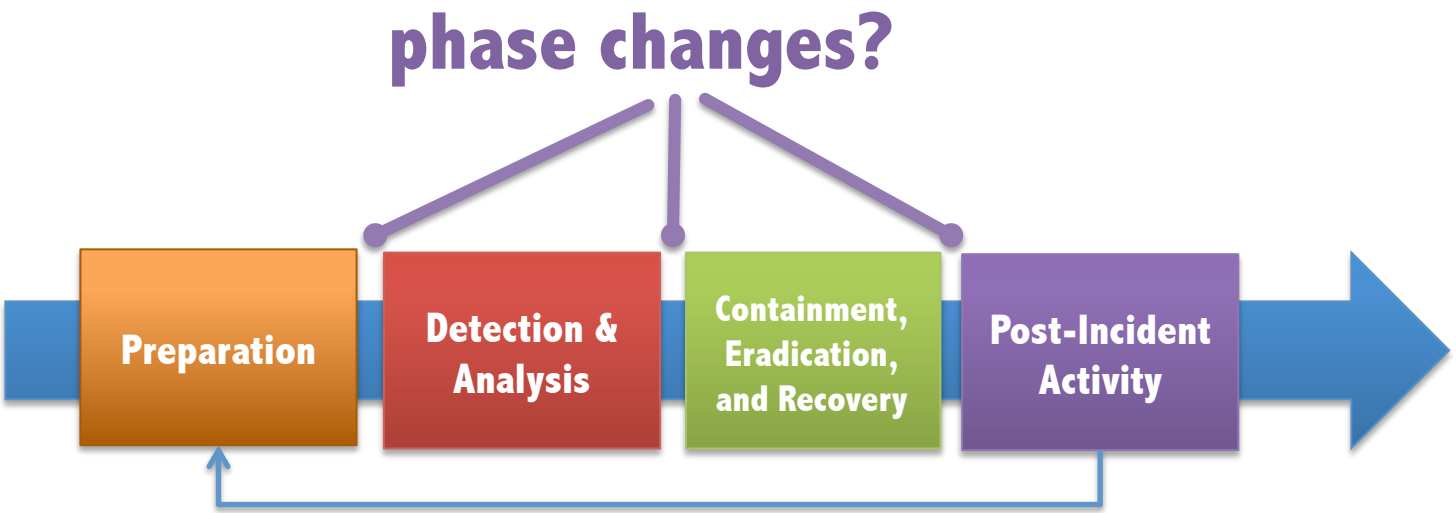
B: Serial variable time approach

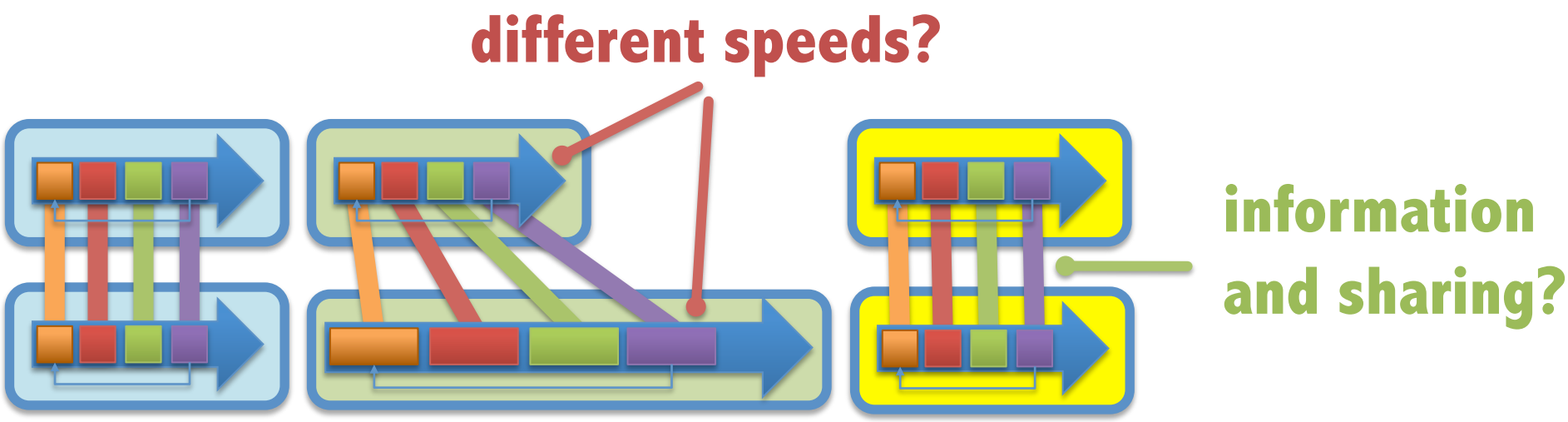


C: Pipeline approach

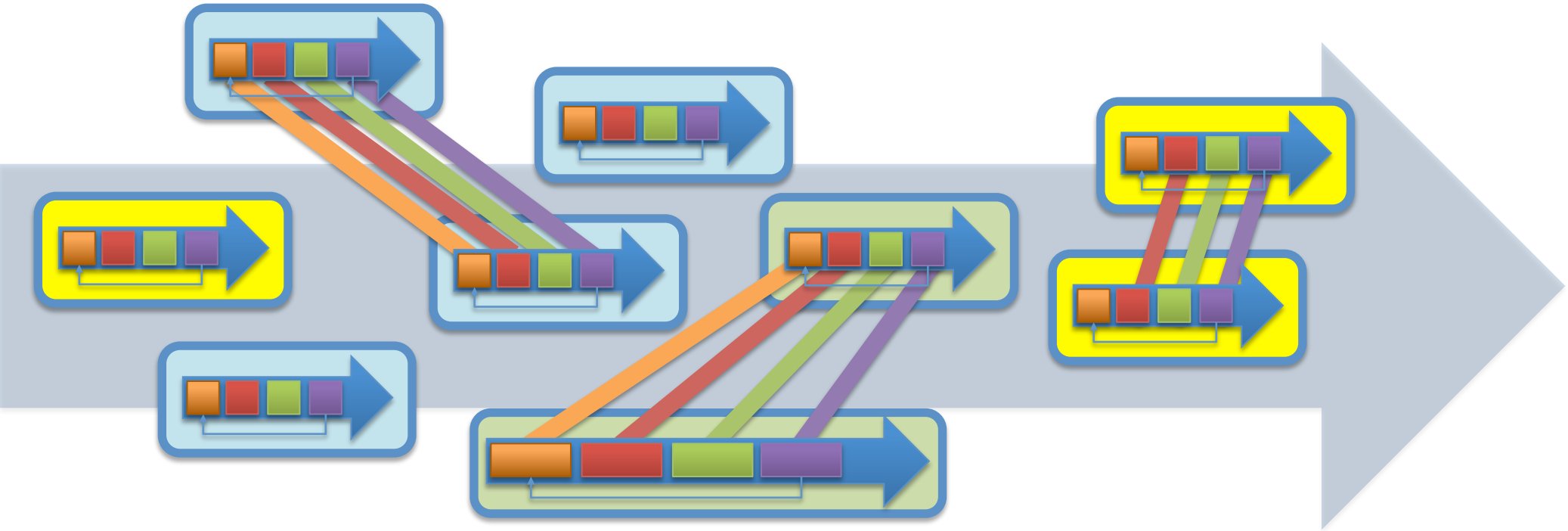


What about cross-cutting incidents?



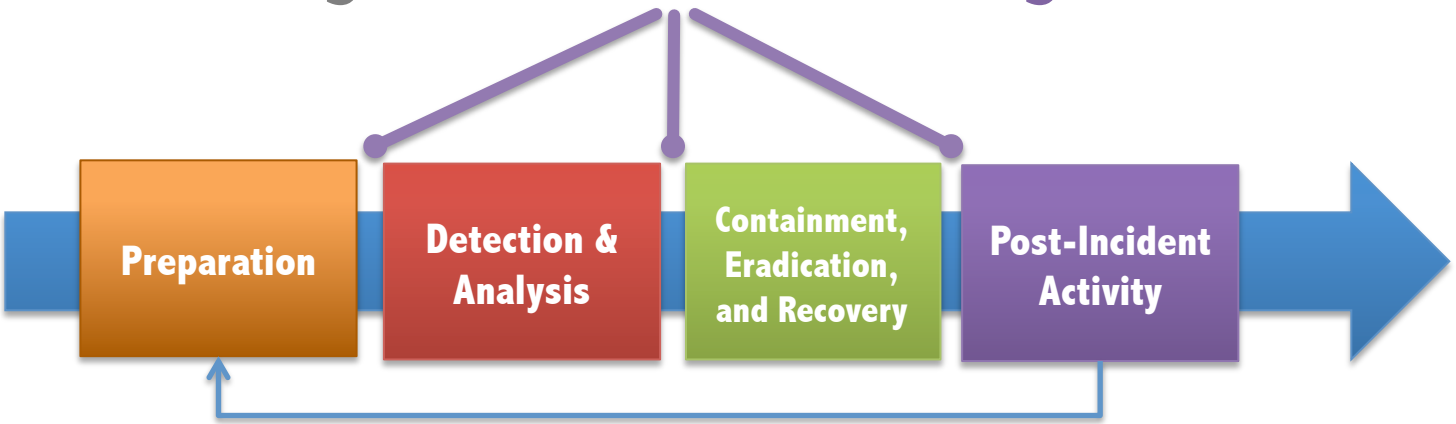


So how could we deal with it?

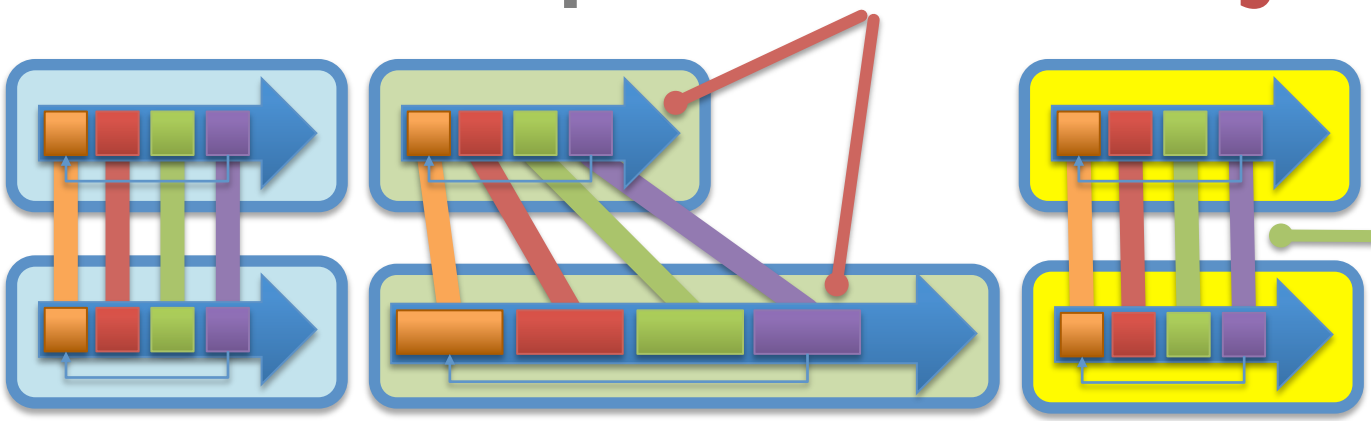


Three broad answers

phase changes? focus on handling activities not an incident



different speeds? reduce locking dependencies

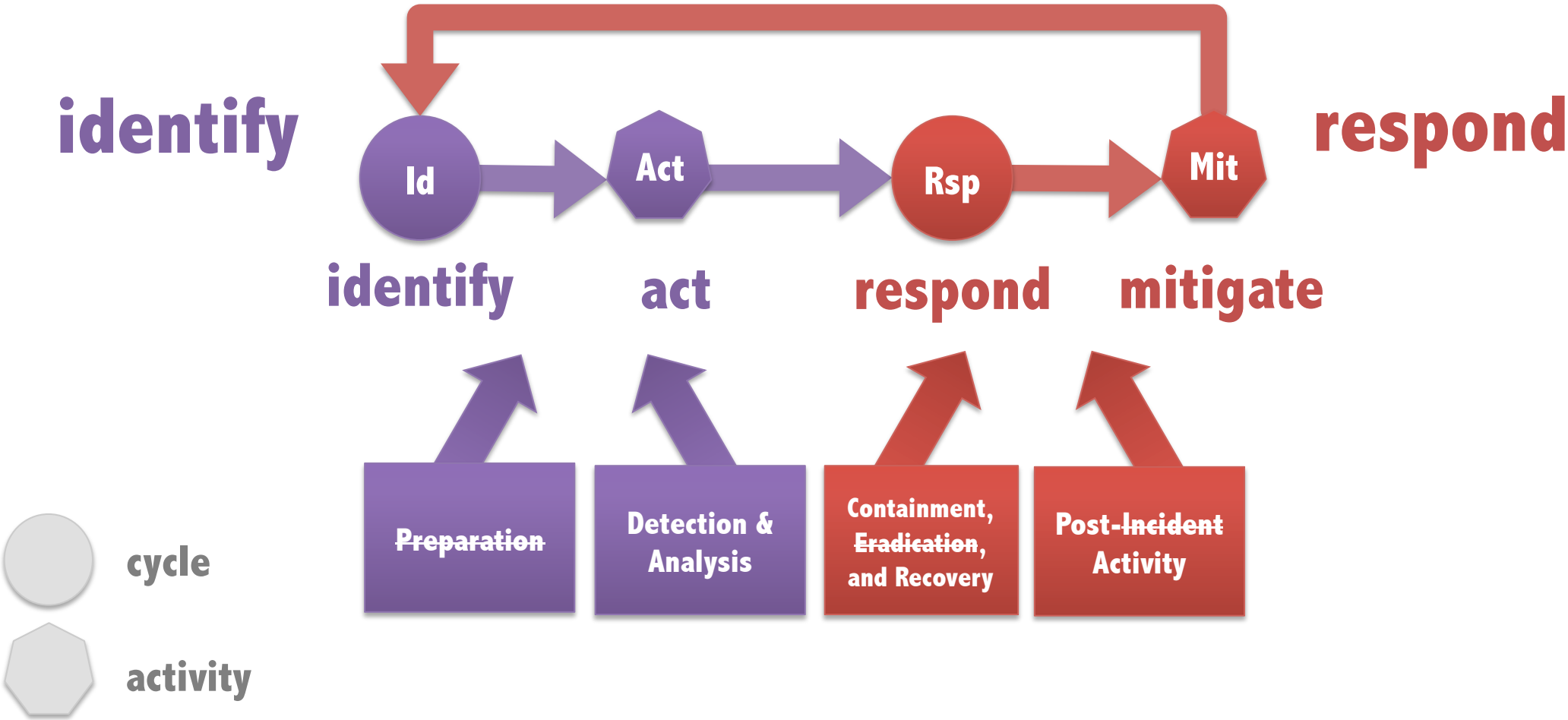


information and sharing?

standard data, common activities

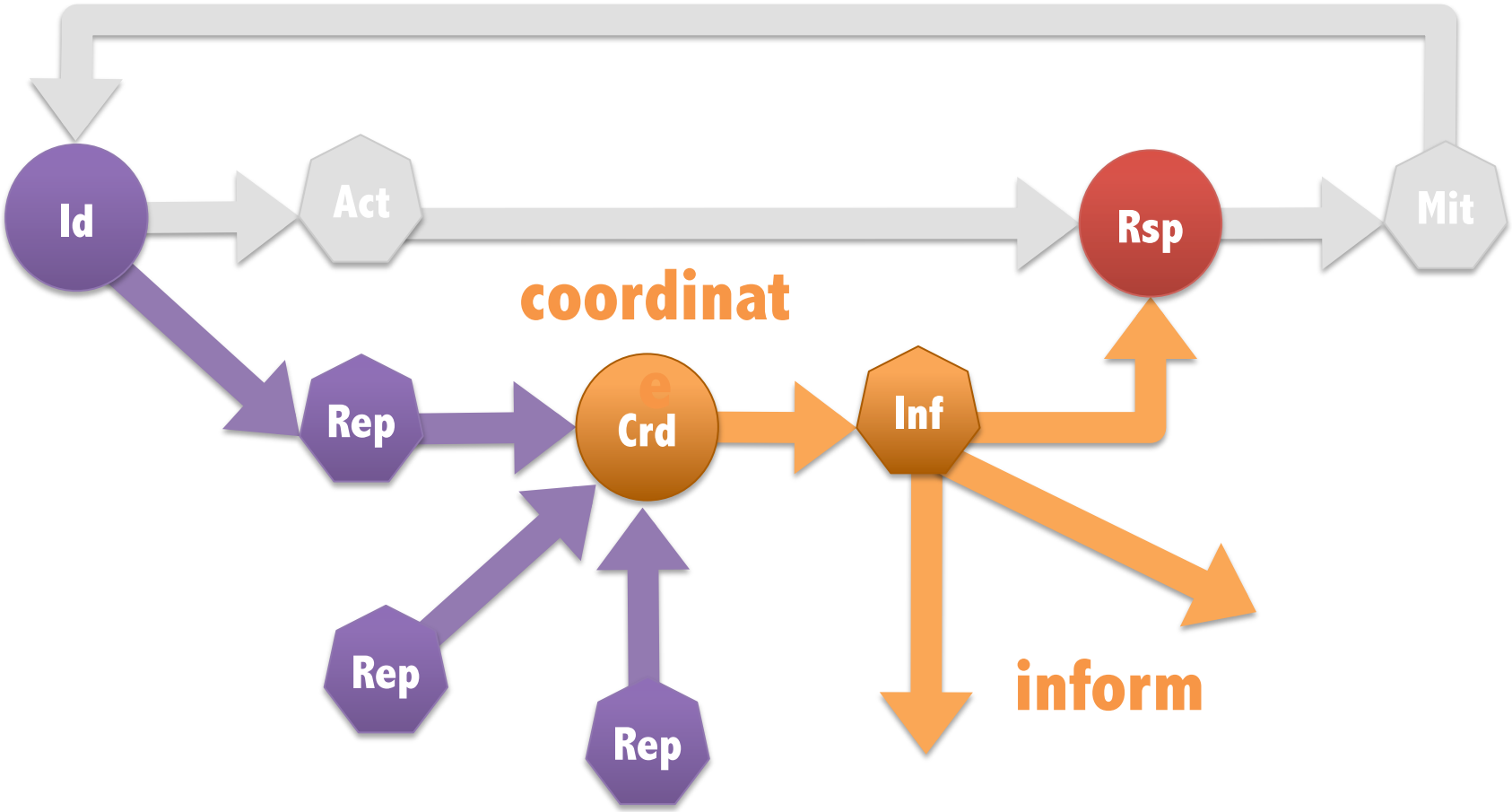
1. Focus on activities

phase changes? focus on handling activities not an incident

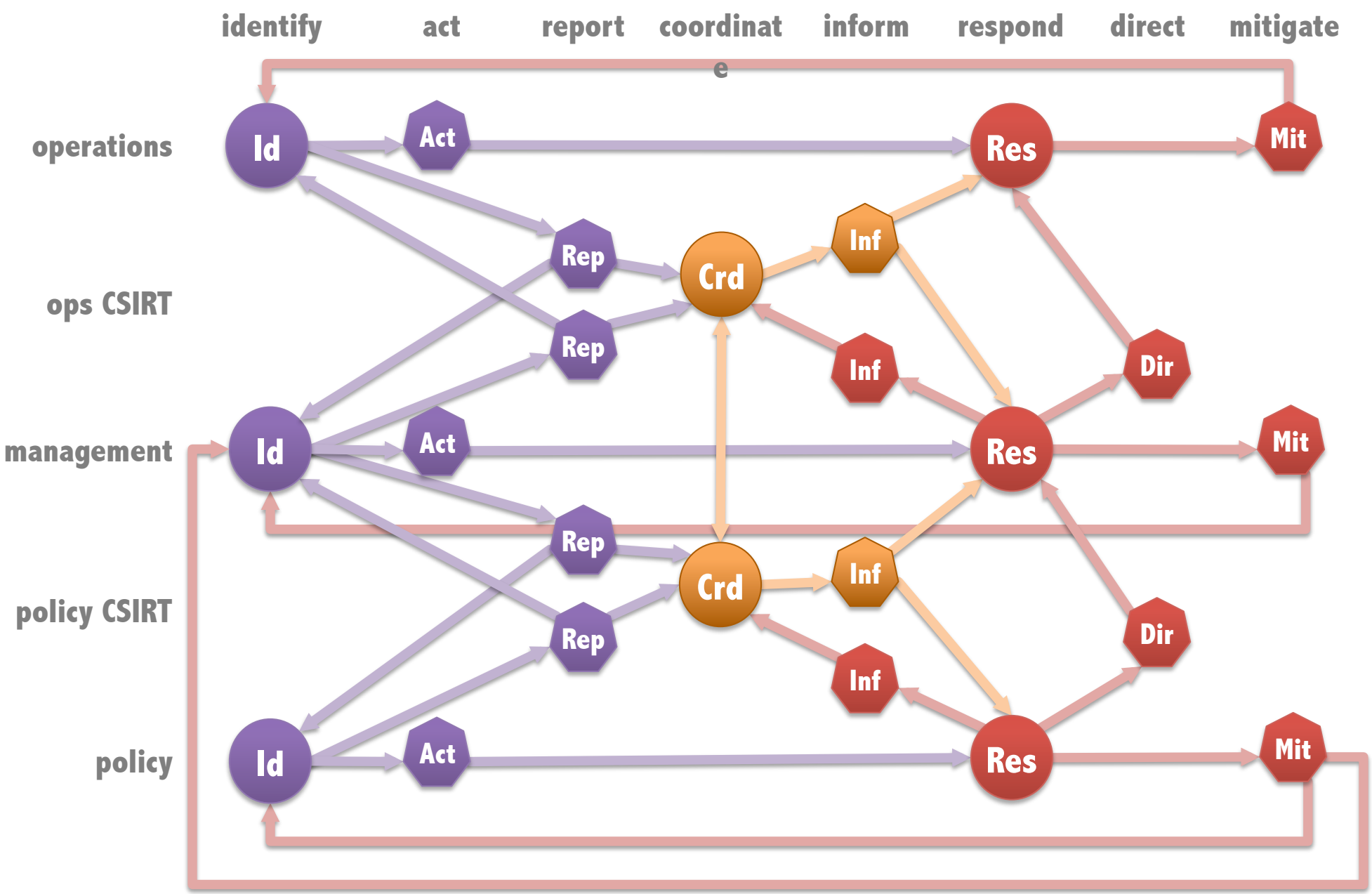


2. Reduce locking dependencies

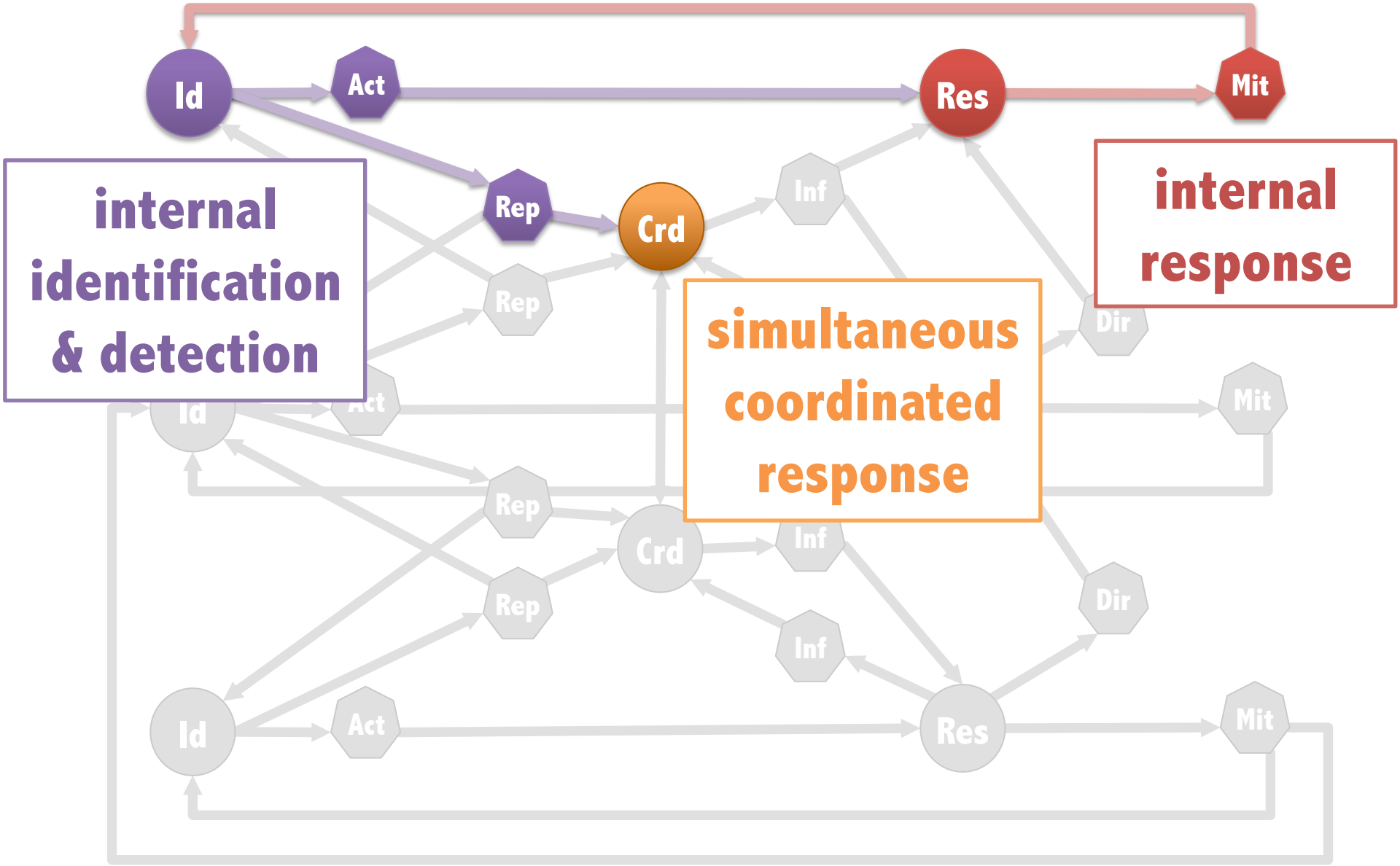
different speeds? **reduce locking dependencies**



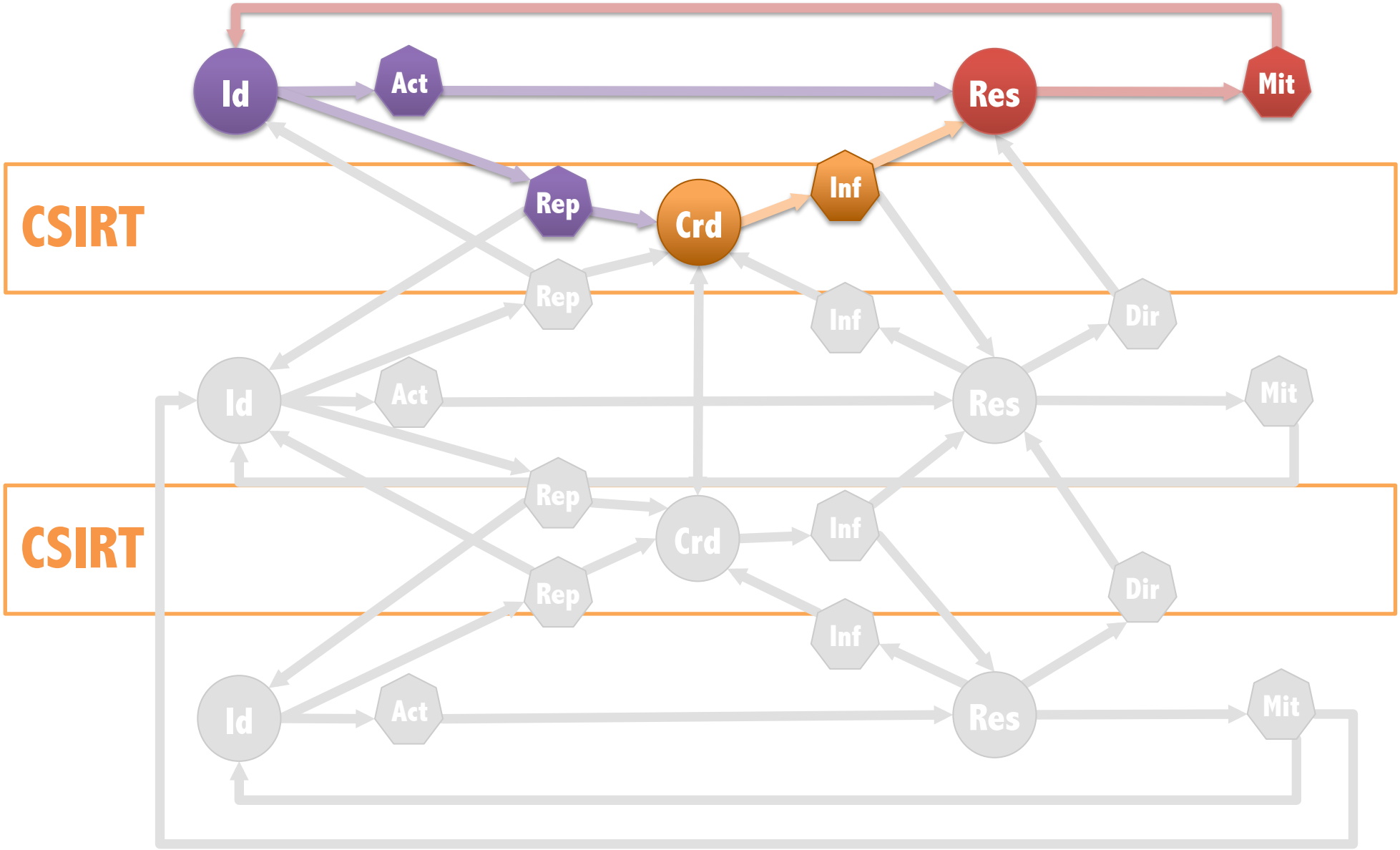
Which: allows for complex system



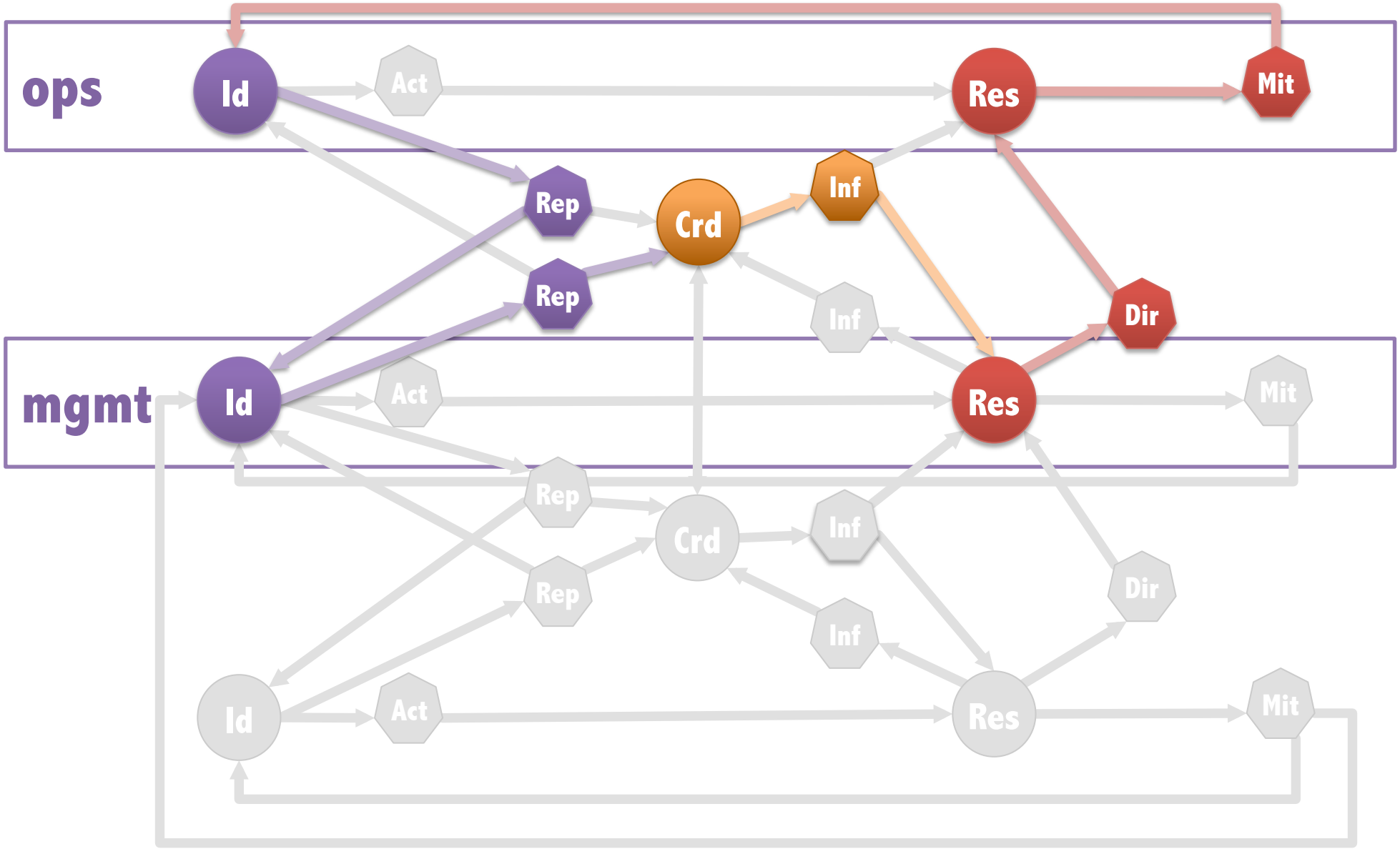
Allows for multiple, concurrent flows



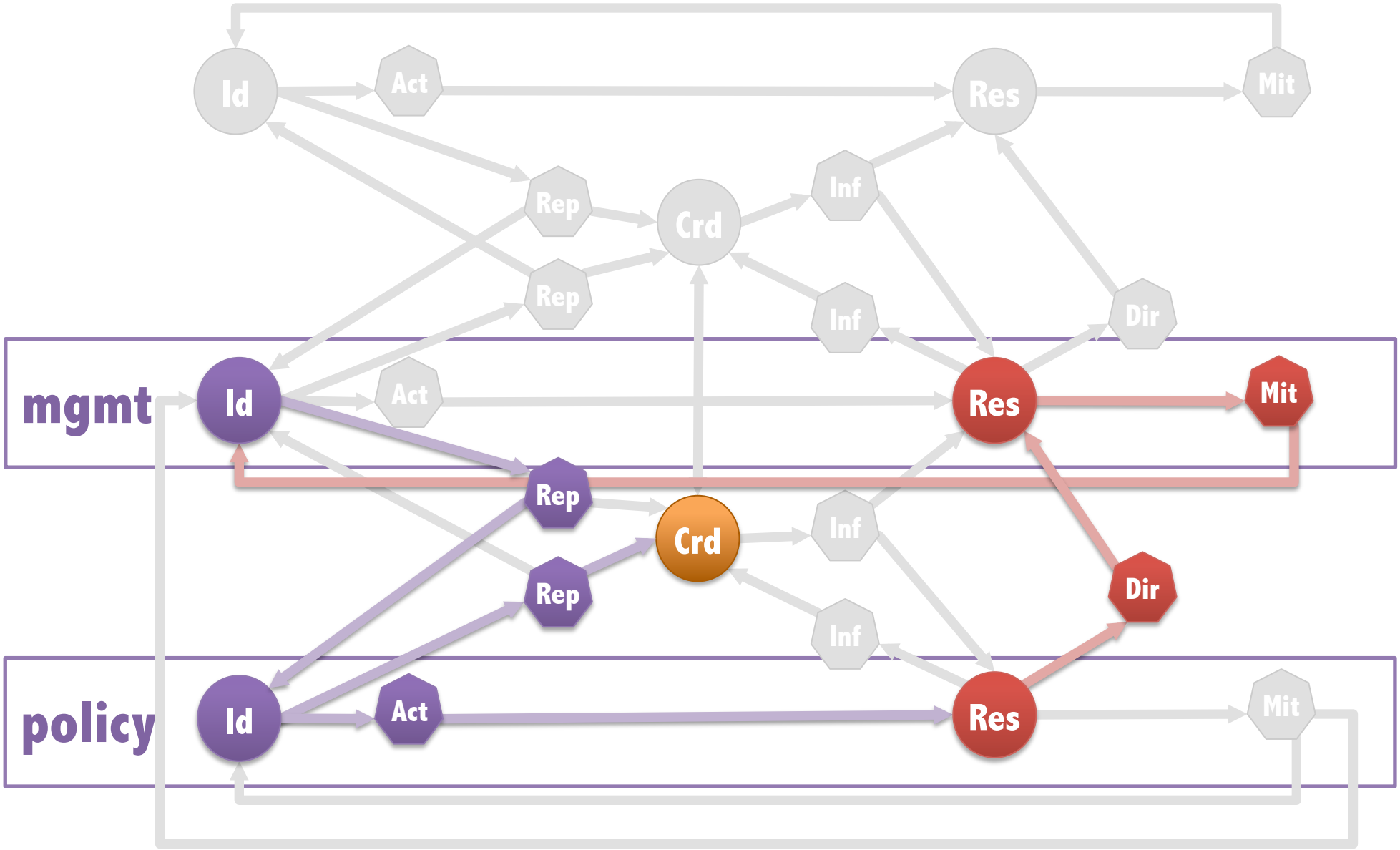
Accounts for role of CSIRT



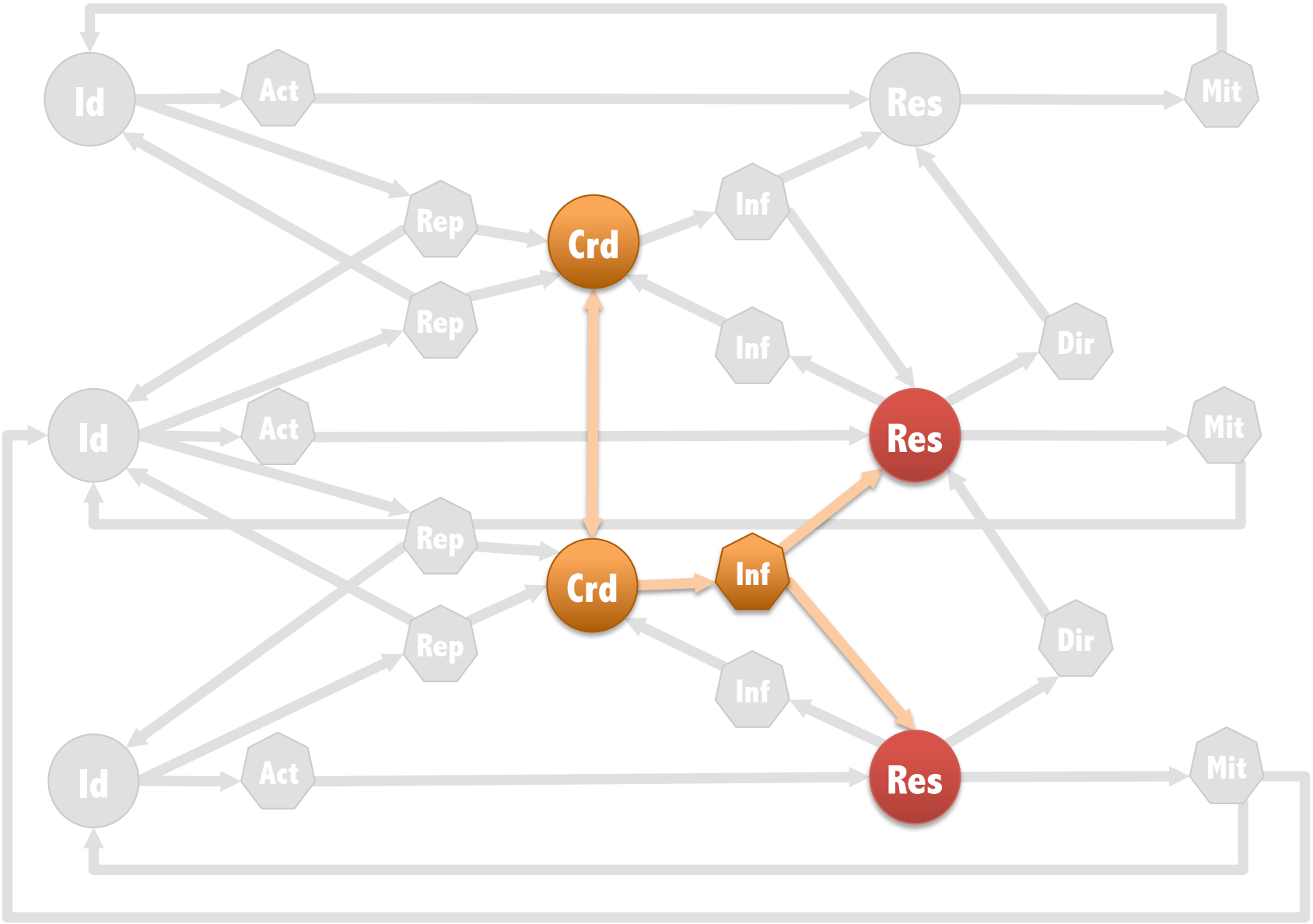
Allows for integration of management



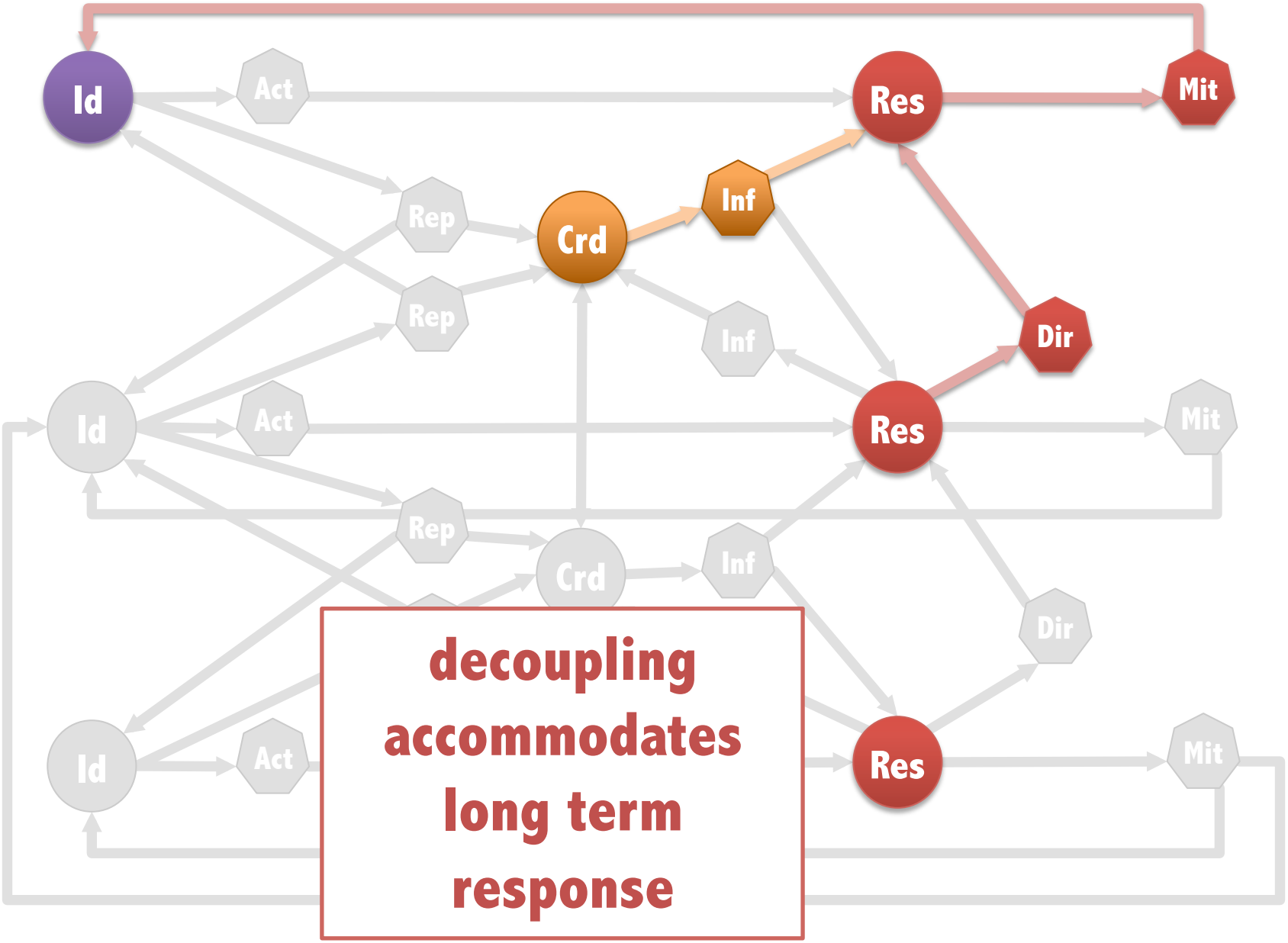
Allows for integration of policy



Uses CSIRTs to drive dissemination



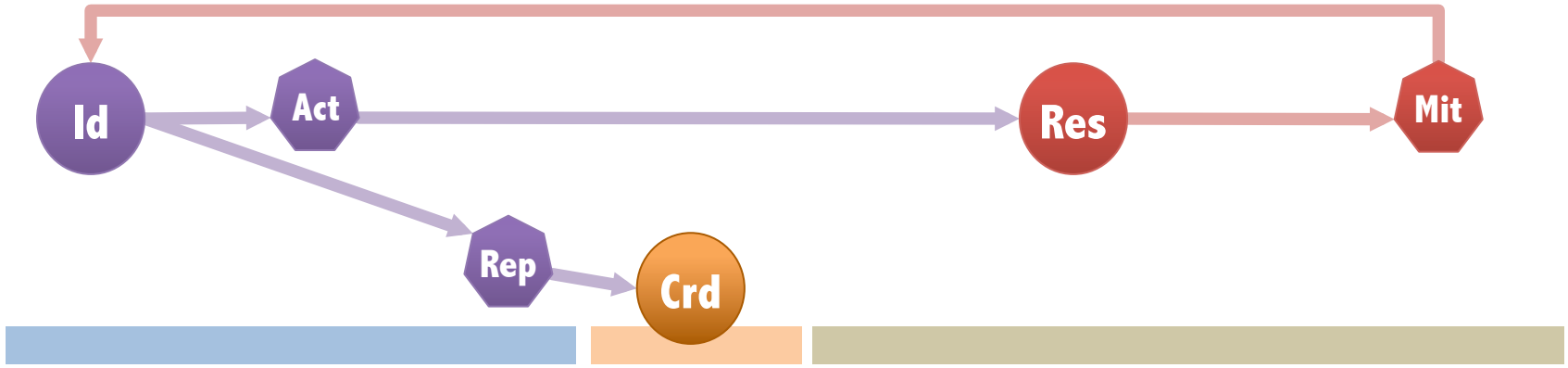
And accounts for long-term impact

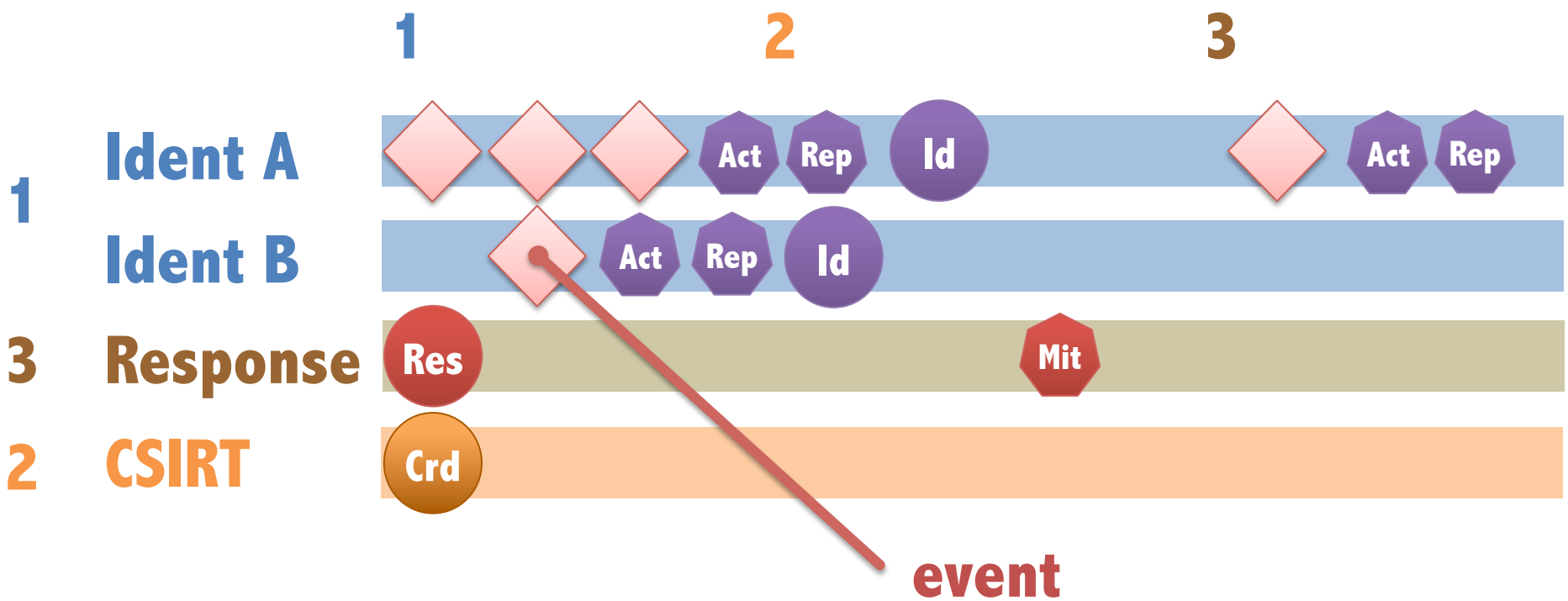


decoupling accommodates long term response

3a. Mapped to common activities

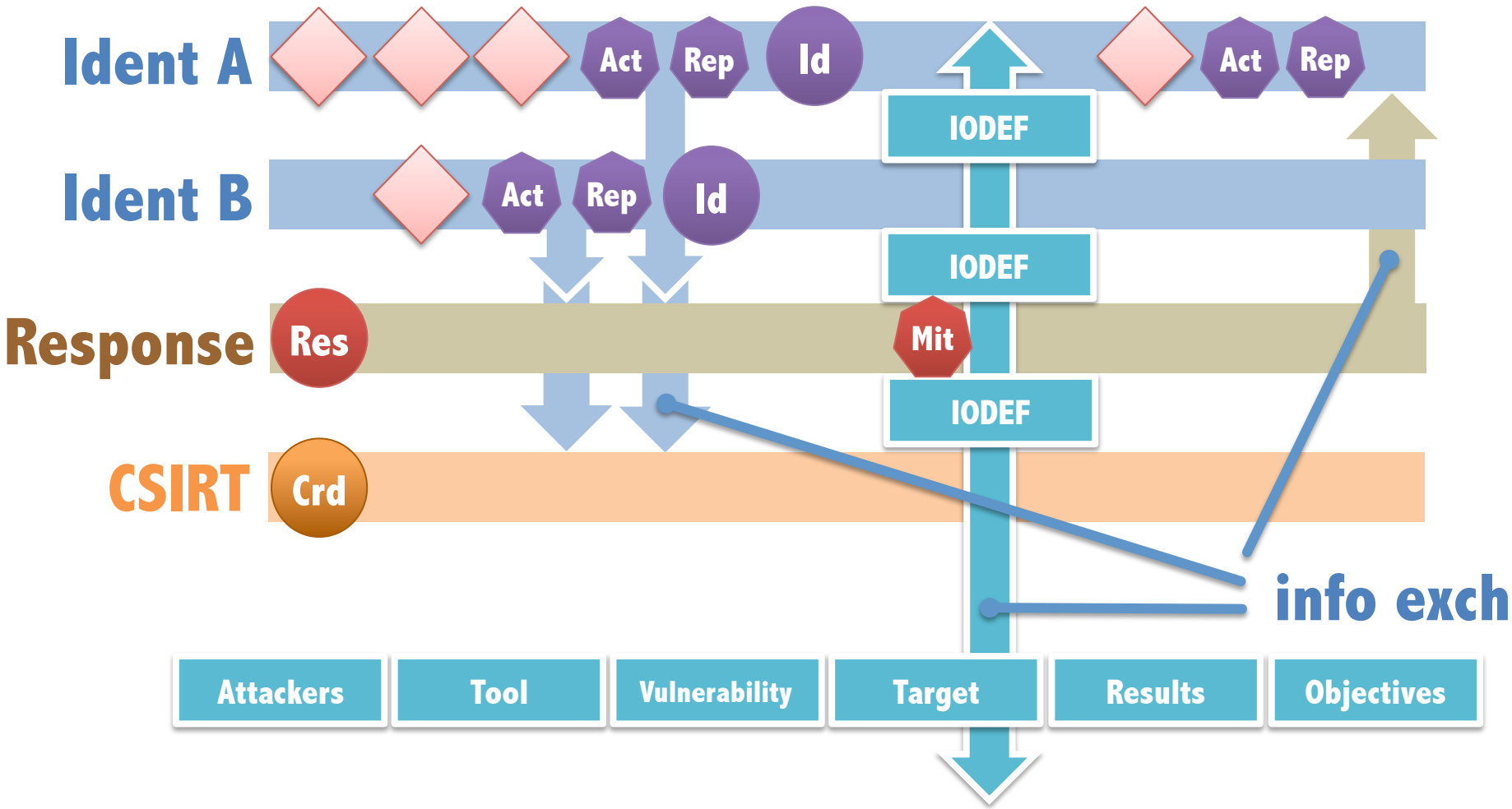
Information and sharing? standard data, common activities



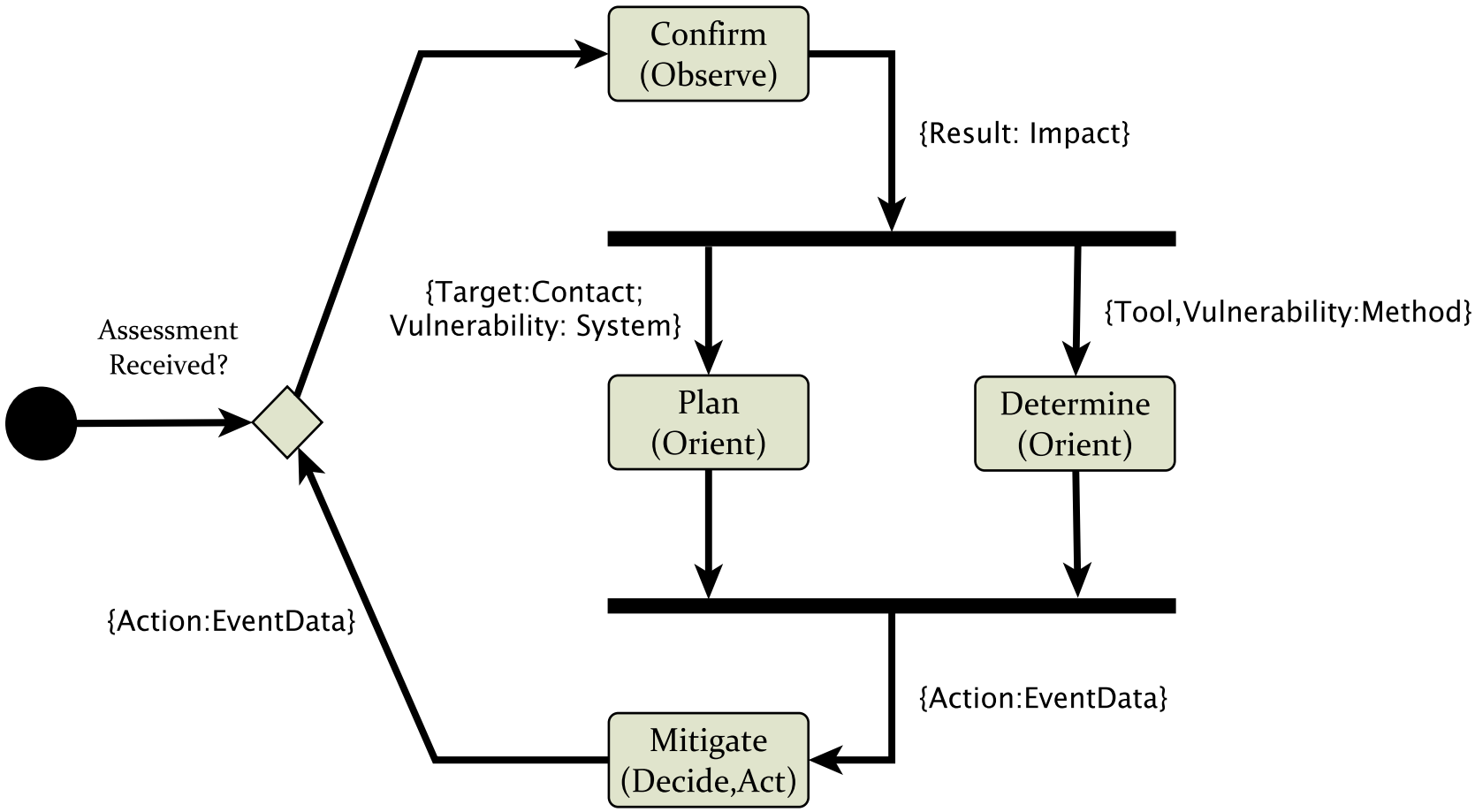


3b. Using standards to communicate

Information and sharing? standard data, common activities

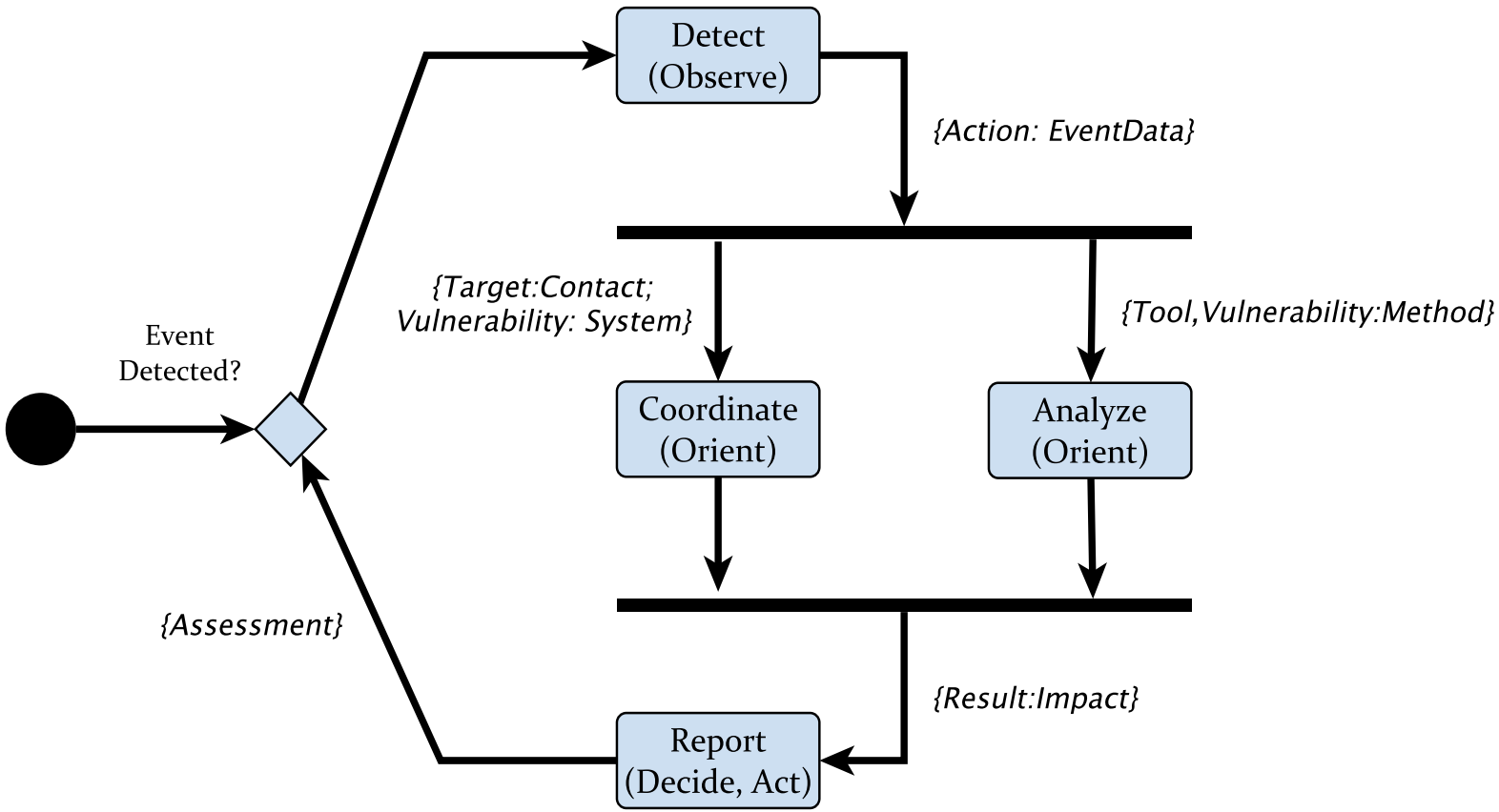


Identify



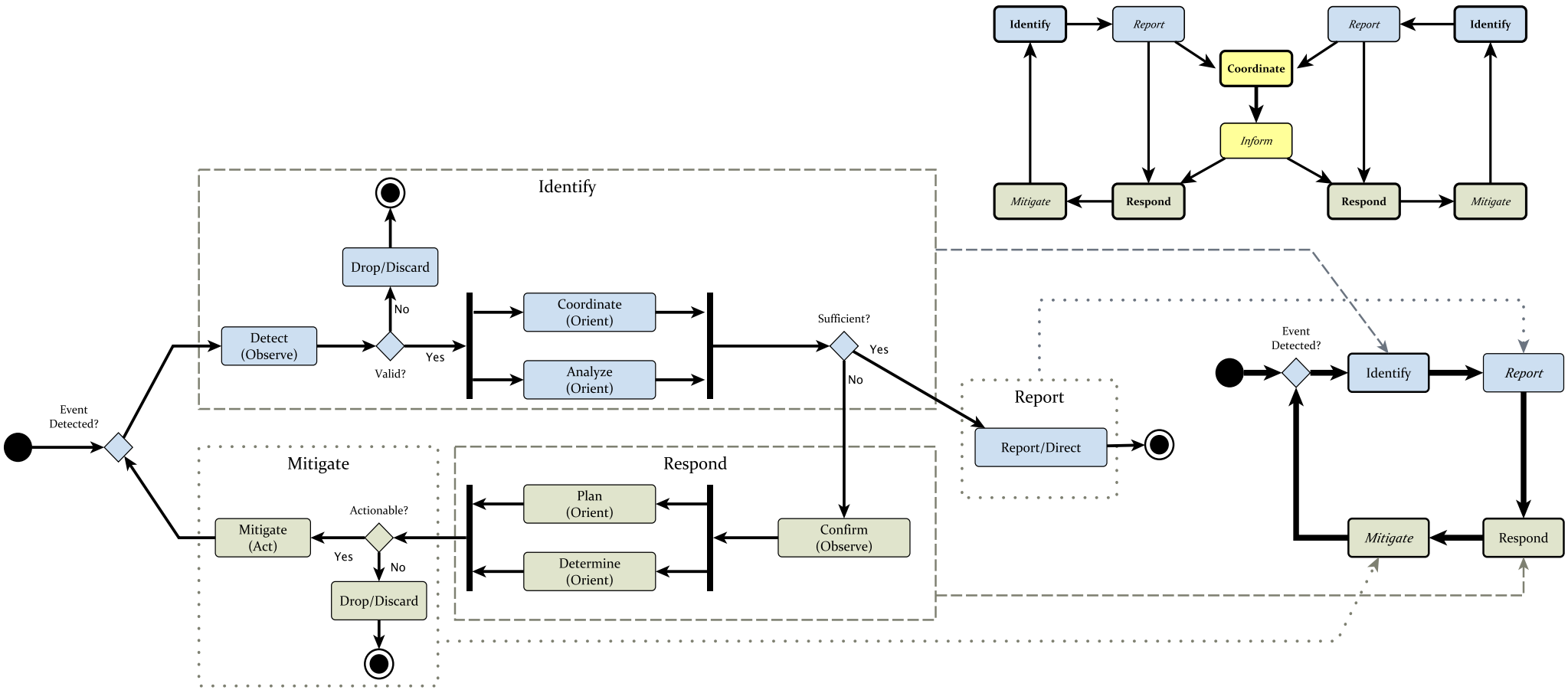
[Osorno, Millar, Rager. 2011]

Respond



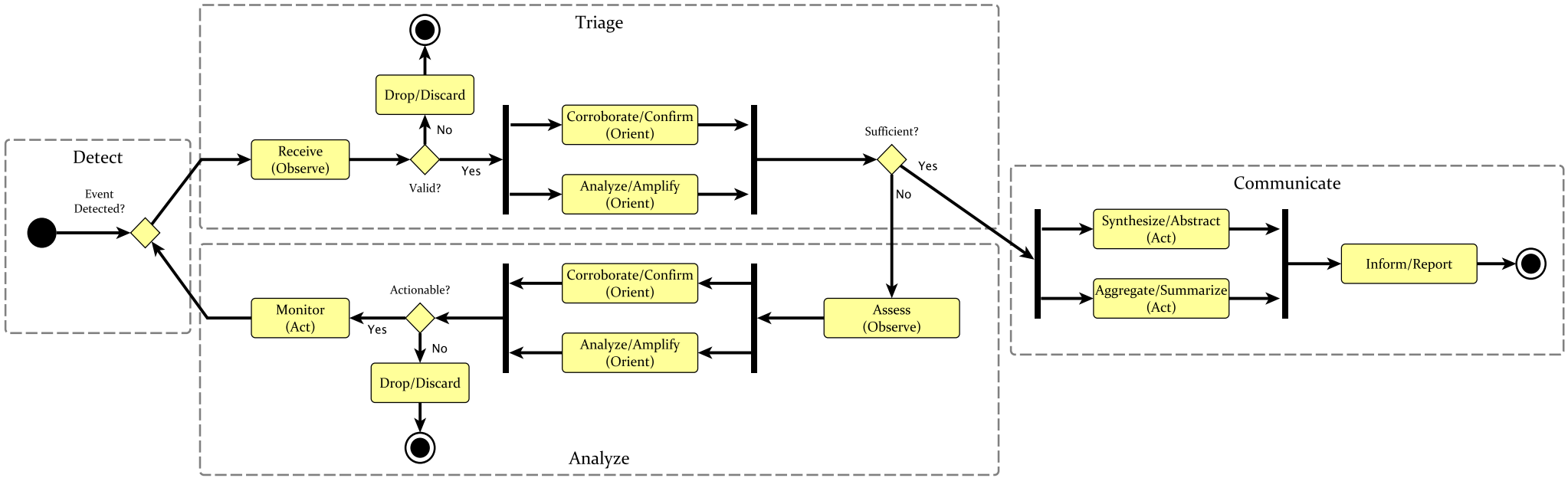
[Osorno, Millar, Rager. 2011]

Defend (identify + respond)



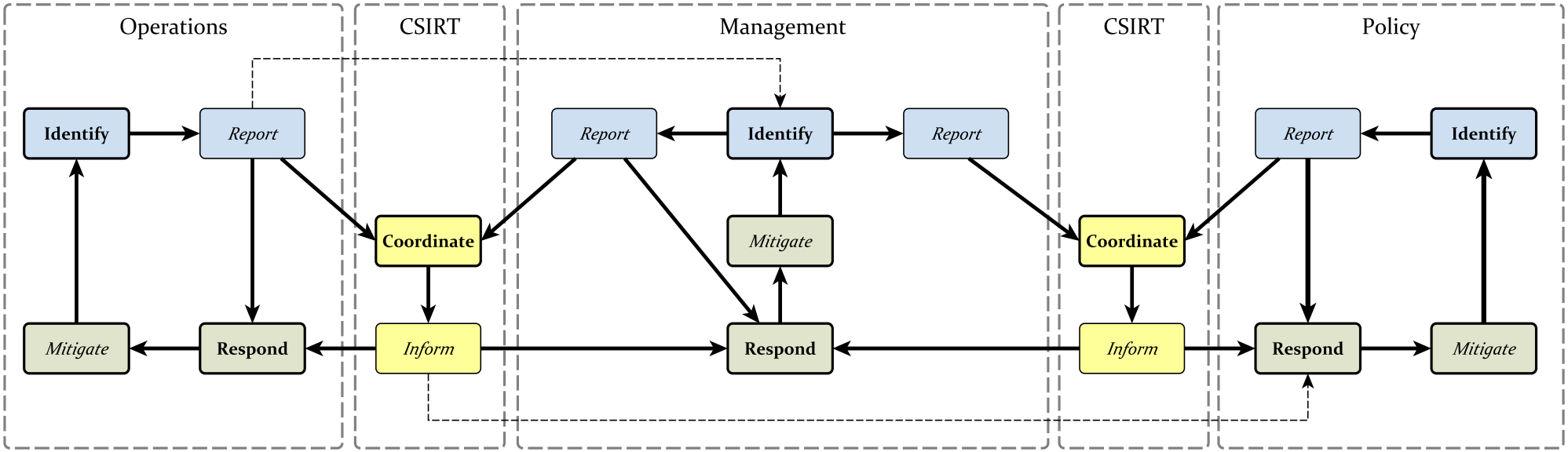
[Osorno, Millar, Rager. 2011]

Coordinate



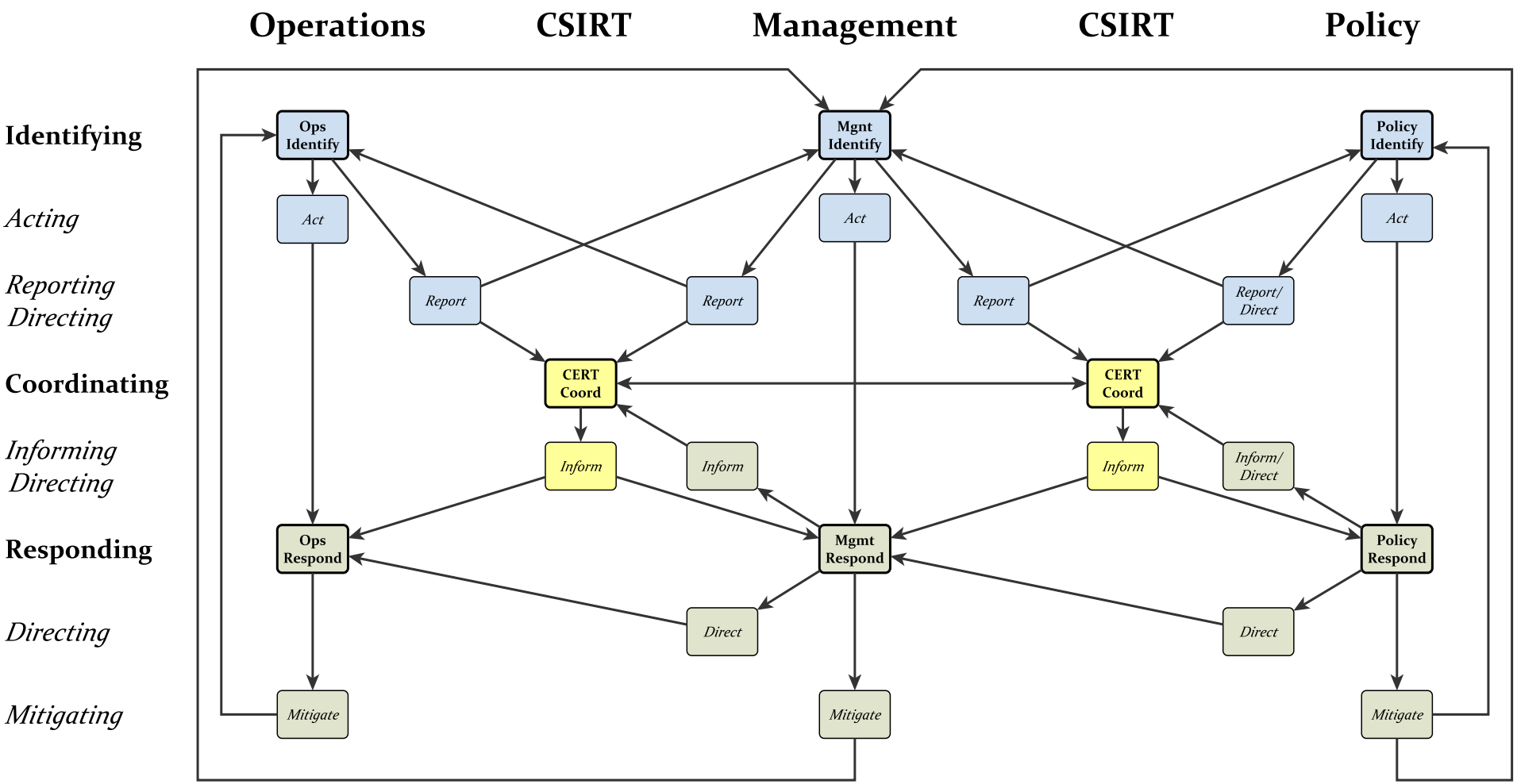
[Osorno, Millar, Rager. 2011]

Simplified coordination model



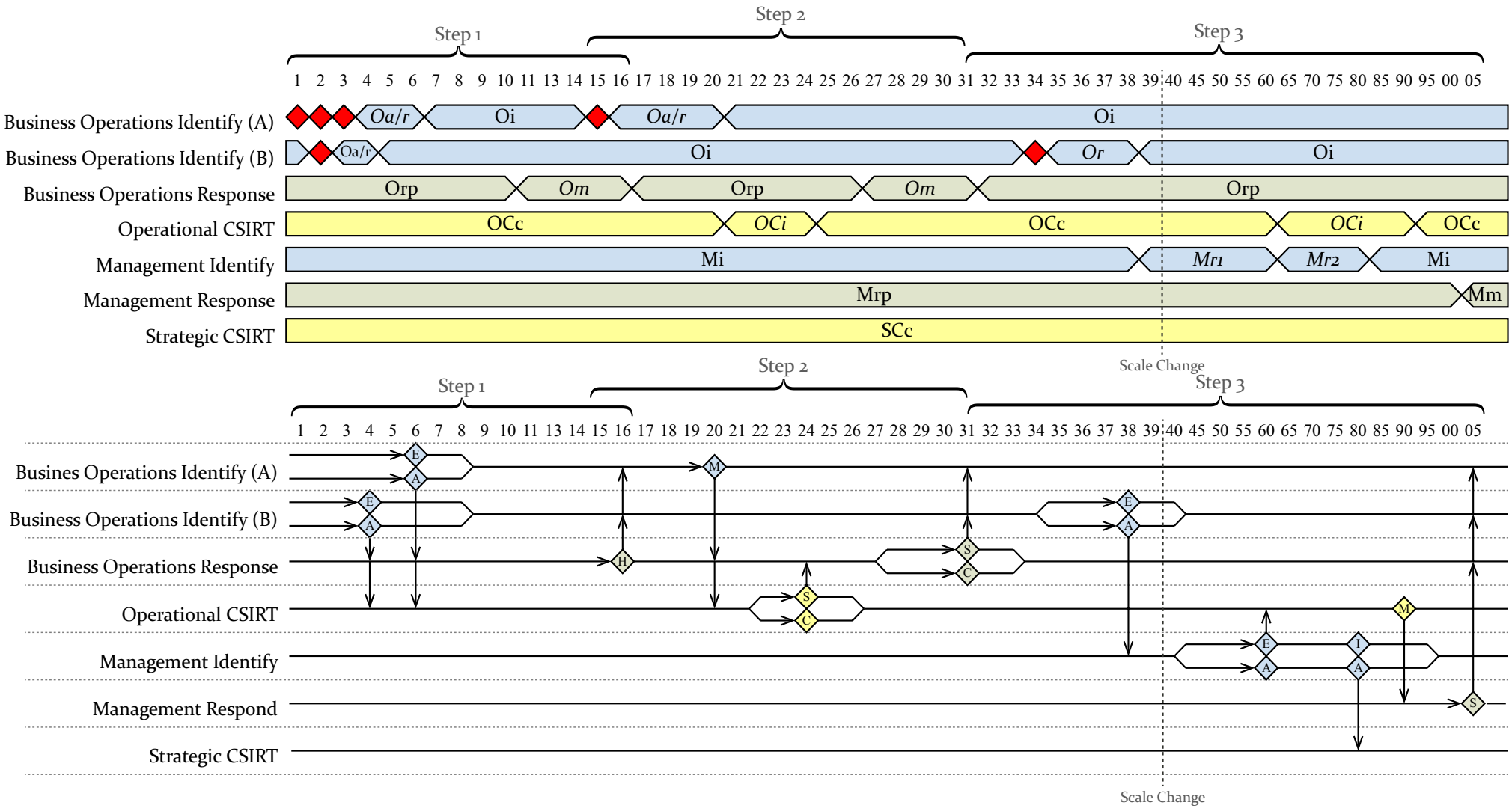
[Osorno, Millar, Rager. 2011]

Larger model



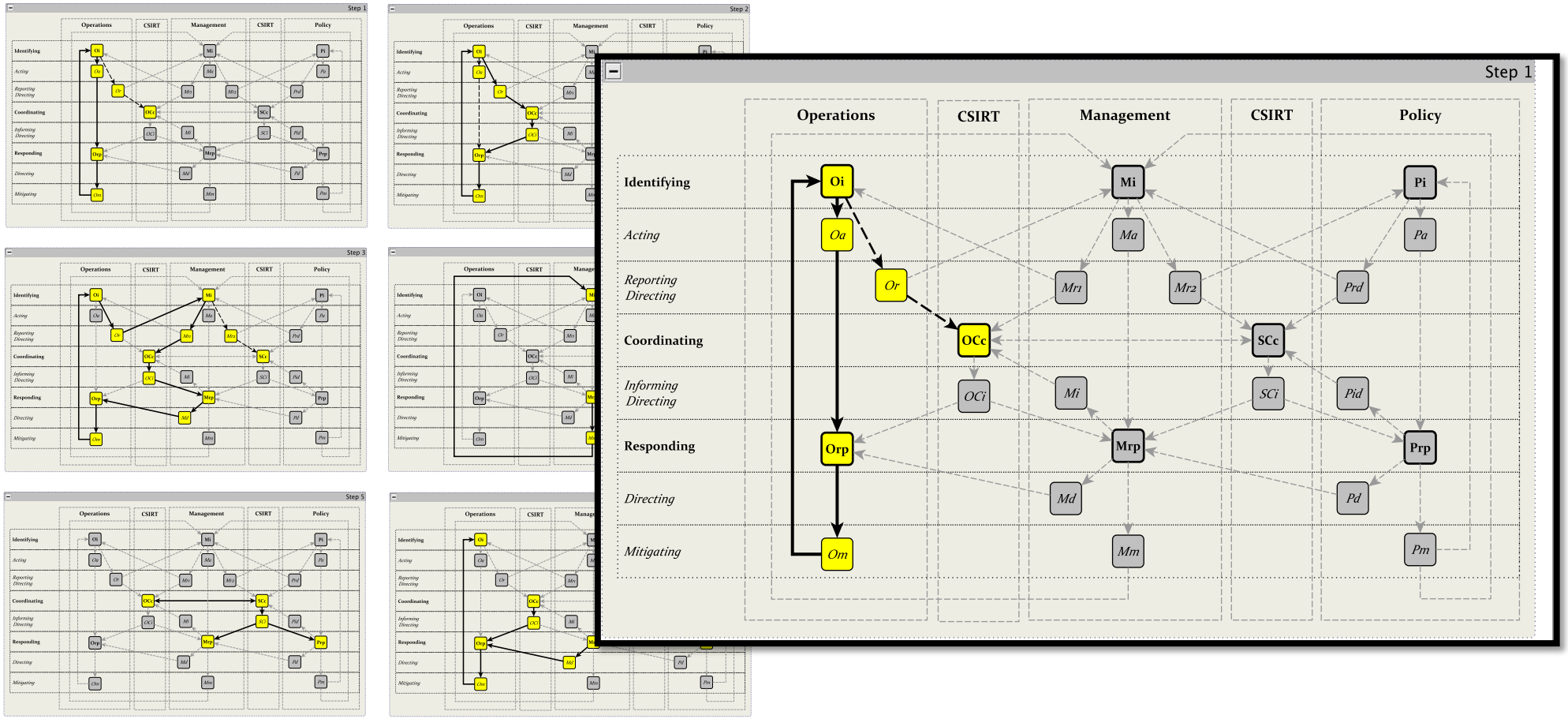
[Osorno, Millar, Rager. 2011]

Timing and state



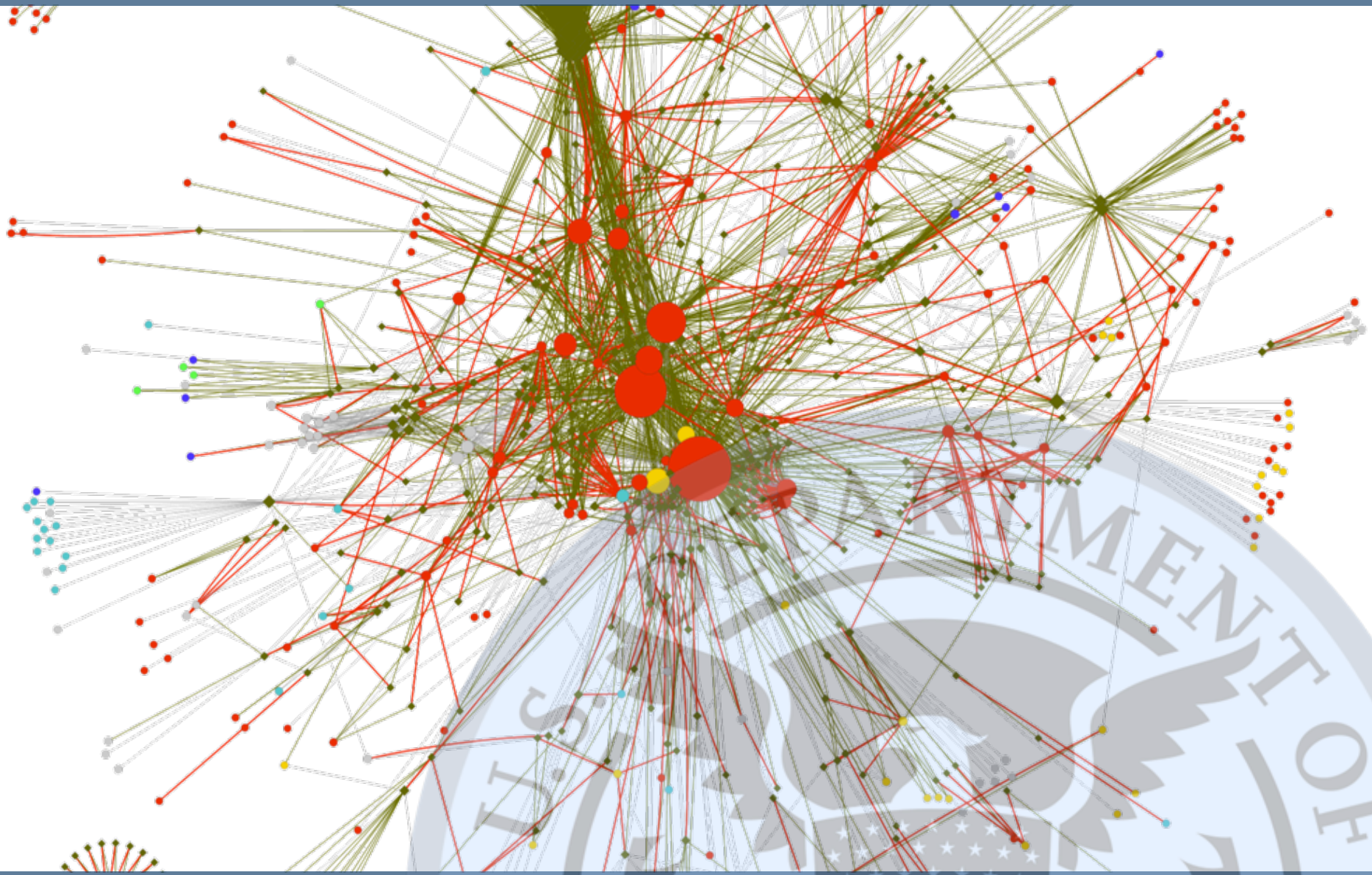
[Osorno, Millar, Rager. 2011]

Multi-phase scenario



[Osorno, Millar, Rager. 2011]

What's next: Exercise/Model Analysis



Part III: Etc

Every scientific construct is an abstraction and the vast majority are, and indeed must be, proposed post hoc – across all fields of science. The problem is rather that the value of the constructs hinges on their common-sense appeal rather than their substance. *Dekker, Human Factors and Folk Models, 2004.*

Build a system to count dangerous things that are ?x

1111 1111 0000 0000 0000 0000

0000 0000 0000 0000 1111 1111

1000 0000 0000 0000 0000 0000

0000 0011 0000 0001 0000 0000

0000 0000 0000 0000 0000 0000 0000 0000

0011 1111 1000 0000 0000 0000 0000 0000

0011 1111 1000 0000 0000 0000 0000 0000

0000 0000 0000 0000 0000 0000 0000 0000

01110010 01100101 01100100

01110010 01100101 01100001 01100100

It's just semantics…

1111 1111 0000 0000 0000 0000 #FF0000 ~ Red

0000 0000 0000 0000 1111 1111 Endian? Red? Blue?

1000 0000 0000 0000 0000 0000 Is 'maroon' red?

0000 0011 0000 0001 0000 0000 Is red R>G && R>B?

0000 0000 0000 0000 0000 0000 0000 0000 C

0011 1111 1000 0000 0000 0000 0000 0000 M

0011 1111 1000 0000 0000 0000 0000 0000 Y

0000 0000 0000 0000 0000 0000 0000 0000 K

01110010 01100101 01100100 'red'

01110010 01100101 01100001 01100100 'read'

Why?

Whether you {know|like} it or not you are probably part of National C2 and of ensuring the continuity of our Constitutional, democratic form of government. Your systems provide and defend essential, legally mandated services for the American people and we need to understand the state of these systems and their services.

Your point?

Let's stop talking sideways about information sharing and start engineering it. Let's stop using vague terms like 'analytics', 'malicious', and 'common operating picture' and define actual phenomena, hypotheses, supporting functions, semantics, and cognitive goals. It's time for science and engineering.

marcos.osorno@jhuapl.edu
(443) 778-9187

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

APL