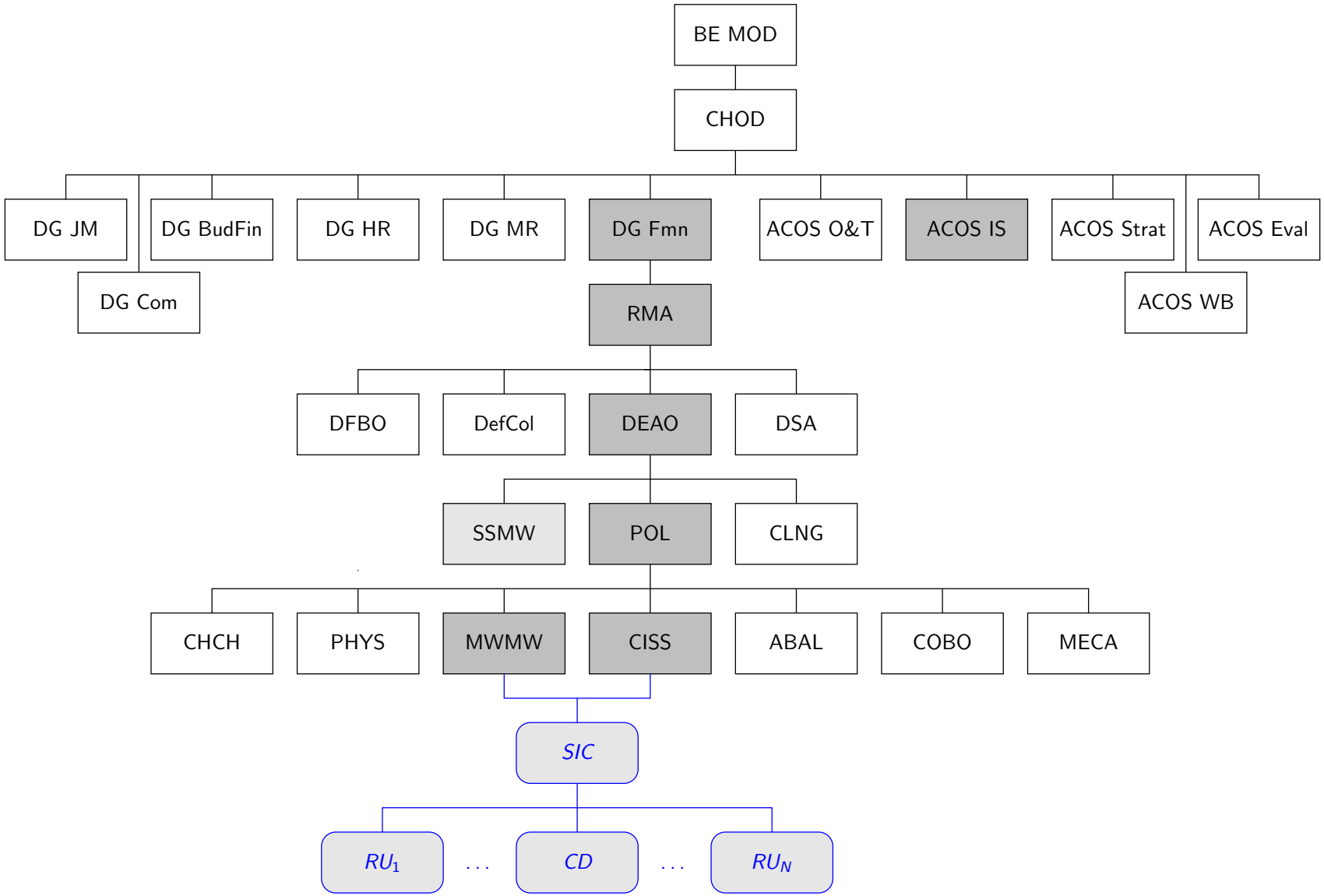
Cyber awareness

prof dr ir Wim Mees

Royal Military Academy - Dept CISS
Brussels, Belgium

December 2nd, 2014

who are we ?


BE MOD
CHOD
DG JM
DG BudFin
DG HR
DG MR
DG Fmn
ACOS O&T
ACOS IS
ACOS Strat
ACOS Eval
DG Com
RMA
ACOS WB
DFBO
DefCol
DEAO
DSA
SSMW
POL
CLNG
CHCH
PHYS
MWMW
CISS
ABAL
COBO
MECA
SIC
RU_1
...
CD
...
RU_N

outline

are we there yet ?

occupy the high ground

on foot

all throughout history,

(image credits: Pieter Brueghel the Elder)

occupy the high ground

on foot

all throughout history,

people have been fighting

(image credits: Pieter Brueghel the Elder and Fac-Man@flickr.com)

occupy the high ground

ground vehicles

ground mobility was invented,

(image credits: Elwood Haynes Museum)

occupy the high ground

ground vehicles

ground mobility was invented,

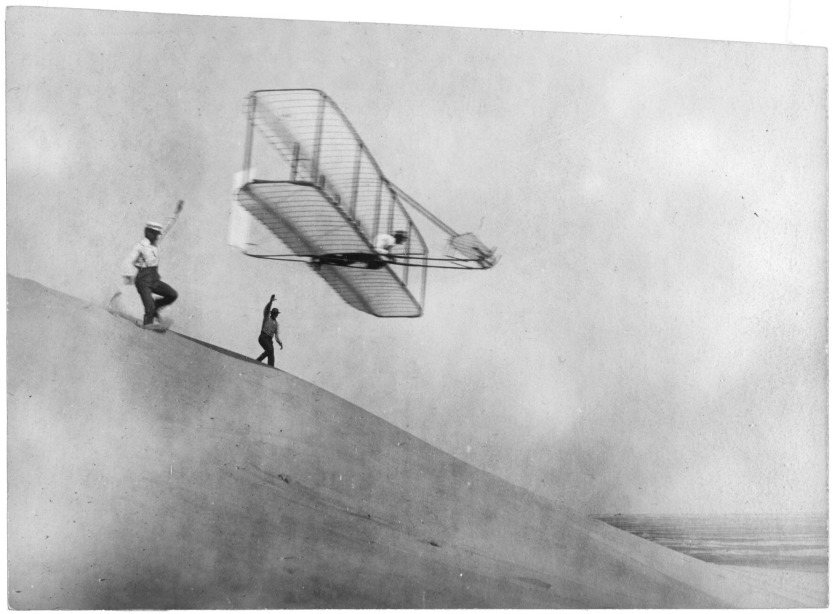
the first tank soon followed

(image credits: Elwood Haynes Museum and Imperial War Museum)

occupy the high ground

airspace

man conquered the air,

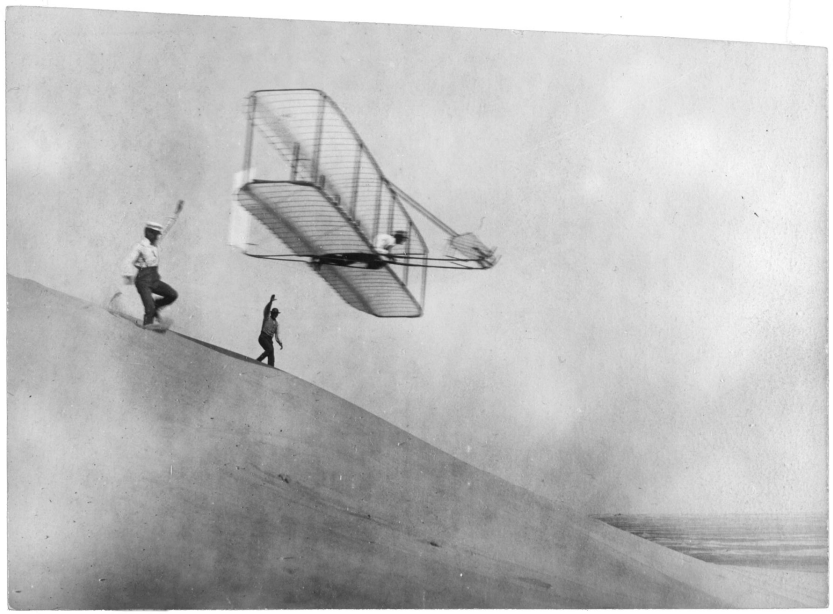


(image credits: Library of Congress)

occupy the high ground

airspace

man conquered the air,



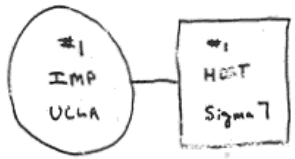
and used it to fight

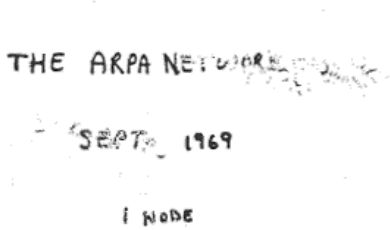
(image credits: Library of Congress and Wings Over The Rockies Air and Space Museum)

occupy the high ground

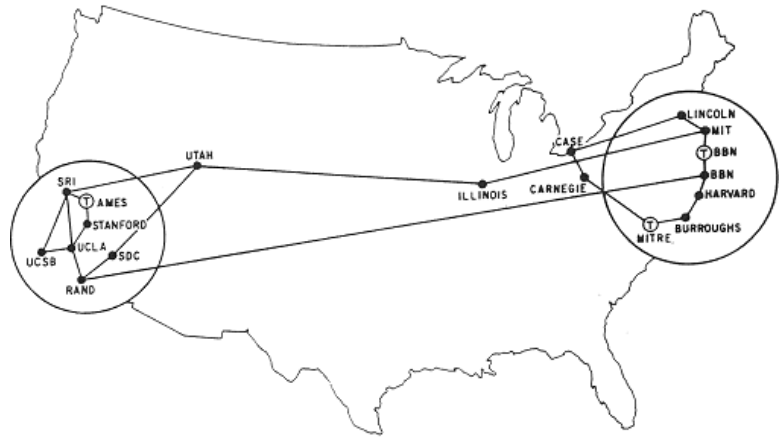
cyberspace

October 1969



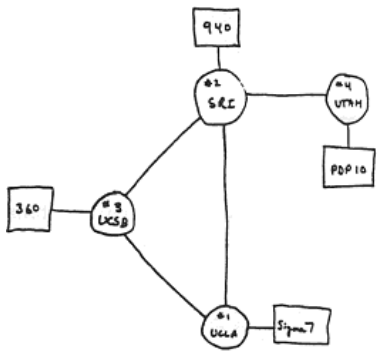


September 1971



MAP 4 September 1971

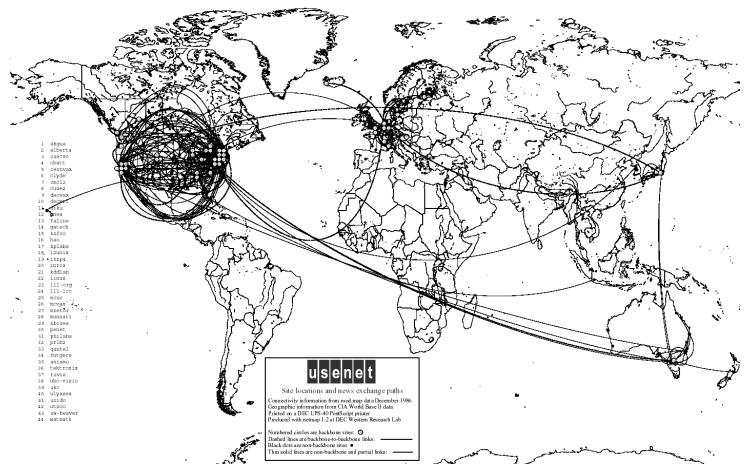
December 1969



THE ARPA NETWORK

DEC 1969

December 1986

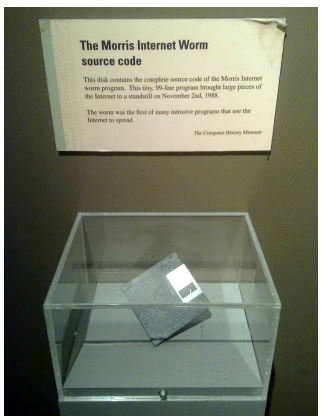


occupy the high ground

cyberspace

November 1988

Morris worm



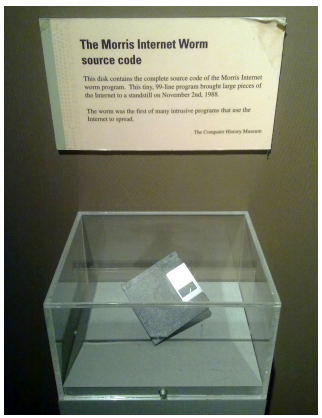
(image credits: Boston Museum of Science)

occupy the high ground

cyberspace

November 1988

Morris worm



March 1999

Melissa virus

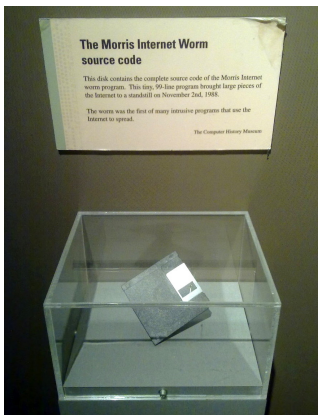
(image credits: Boston Museum of Science , sophos.com)

occupy the high ground

cyberspace

November 1988

Morris worm

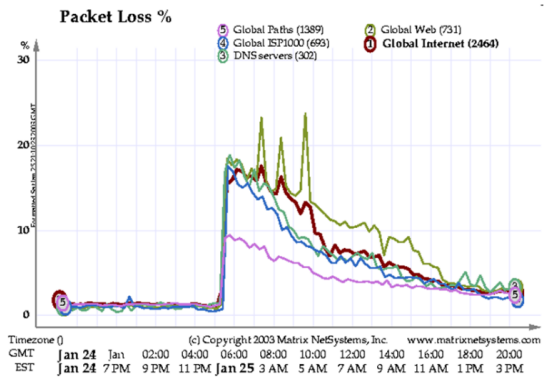


March 1999

Melissa virus

January 2003

SQL Slammer worm



(image credits: Boston Museum of Science , sophos.com and Matrix NetSystems)

occupy the high ground

cyberspace

occupy the high ground

cyberspace

Table 1
Evolution of Stuxnet versions

Version	Date	Description
0.500	November 3, 2005	C&C server registration
0.500	November 15, 2007	Submit date to a public scanning service
0.500	July 4, 2009	Infection stop date
1.001	June 22, 2009	Main binary compile timestamp
1.100	March 1, 2010	Main binary compile timestamp
1.101	April 14, 2010	Main binary compile timestamp
1.x	June 24, 2012	Infection stop date

Table 3
Evolution of Stuxnet replication

Replication Technique	0.500	1.001	1.100	1.101
Step 7 project files	X	X	X	X
USB through Step 7 project files	X			
USB through Autorun		X		
USB through CVE-2010-2568			X	X
Network shares		X	X	X
Windows Server RPC		X	X	X
Printer spooler		X	X	X
WinCC servers		X	X	X
Peer-to-peer updating through mailslots	X			
Peer-to-peer updating through RPC		X	X	X

Table 2
Evolution of Stuxnet exploits

Vulnerability	0.500	1.001	1.100	1.101	Description
CVE-2010-3888			X	X	Task scheduler EOP
CVE-2010-2743			X	X	LoadKeyboardLayout EOP
CVE-2010-2729		X	X	X	Print spooler RCE
CVE-2008-4250		X	X	X	Windows Server Service RPC RCE
CVE-2012-3015	X	X	X	X	Step 7 Insecure Library Loading
CVE-2010-2772		X	X	X	WinCC default password
CVE-2010-2568			X	X	Shortcut .lnk RCE
MS09-025		X			NtUserRegisterClassExWow/NtUserMessageCall EOP

(source: Stuxnet 0.5: The Missing Link, Symantec, 26feb13)

occupy the high ground

what's next ?

- Duqu
- Flame(r)/Skywiper
- ...

(Pandora opening her box, James Gillray, 1756-1815)

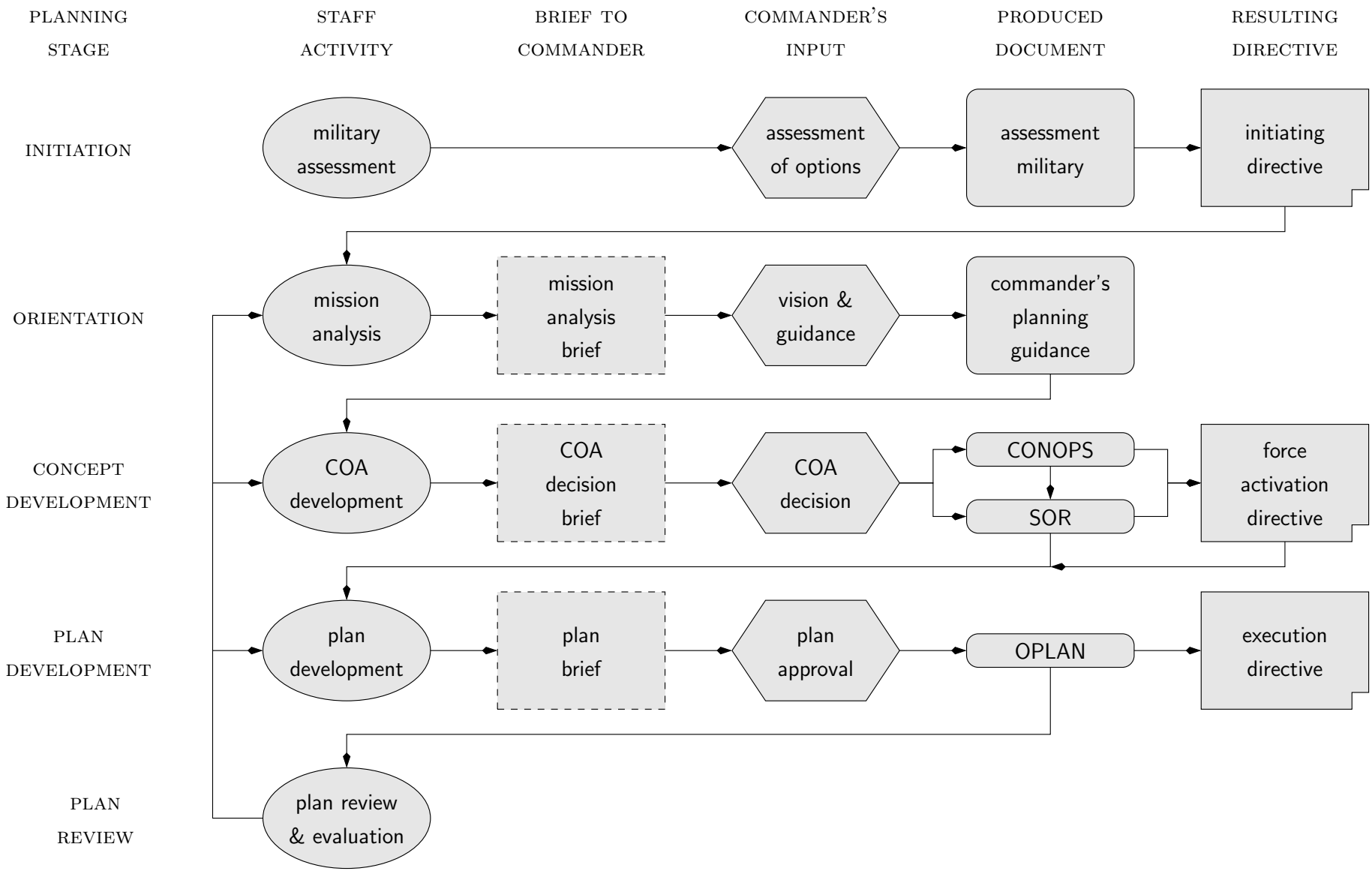
occupy the high ground

our objective:
coordinated command & control (C2) in a
combined joint task force (CJTF)

some additional challenges:

- *federated* mission networks
  (coalition partners bring in their own networks
  $\rightarrow$ integration, trust, security, ...)
- *converged* mobile tactical networks
  (data, voice, video combined with mobility, tactical data radios, ...)
- *disadvantaged* networks
  (low-bandwidth, high-latency, intermittent links, ...)

operational planning process (OPP)



outline

are we there yet ?

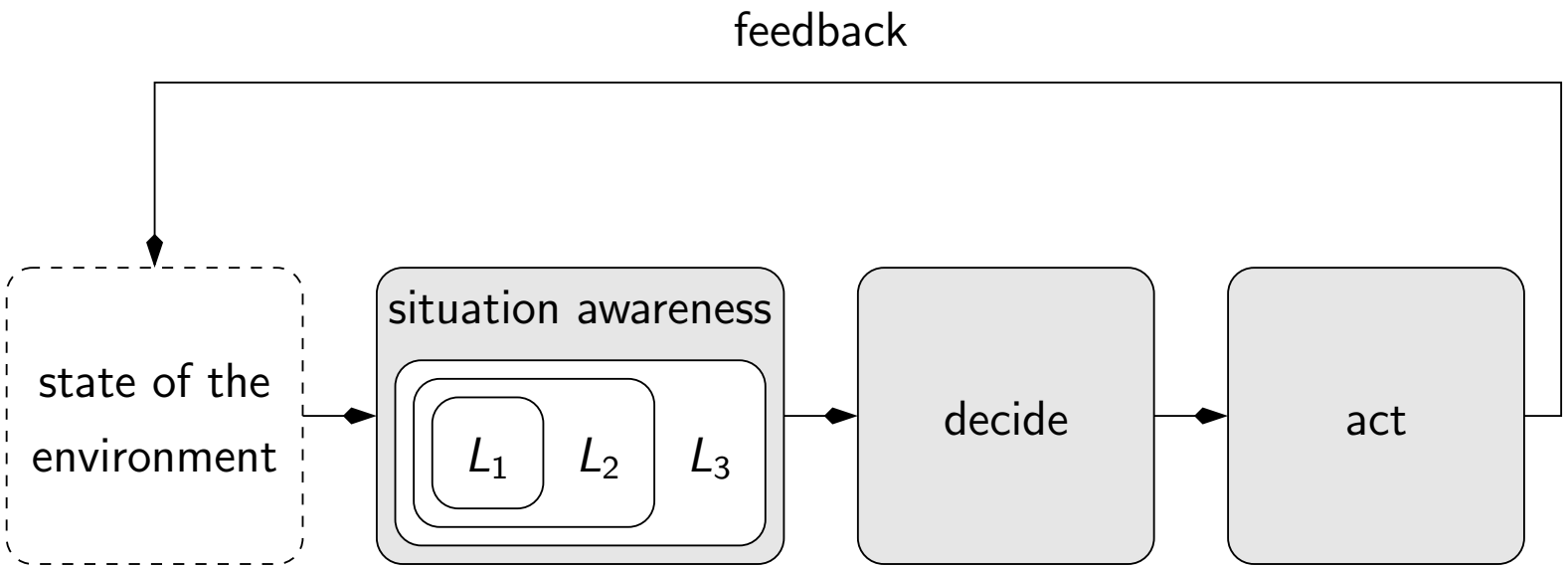
situation awareness (SA)

The formal definition of SA is

the perception of the elements in the environment
within a volume of time and space,
the comprehension of their meaning,
and the projection of their status in the near future.

(Endsley, 1988)

situation awareness (SA)



model of situation awareness in dynamic decision making (Endsley, 1995)

situation awareness (SA)

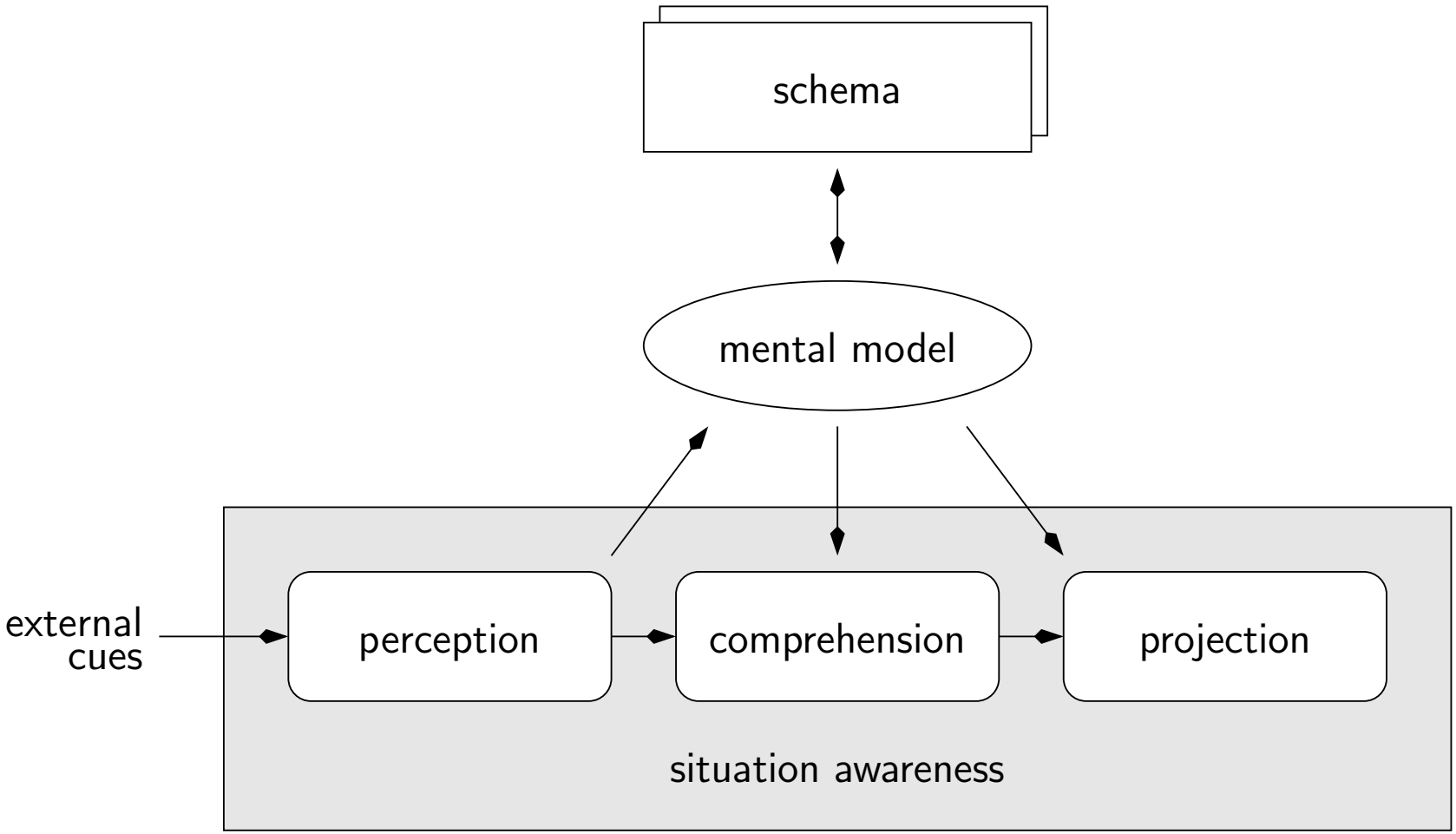
level 1: *perception* of the elements in the environment

level 2: *comprehension* of the current situation

level 3: *projection* of future status

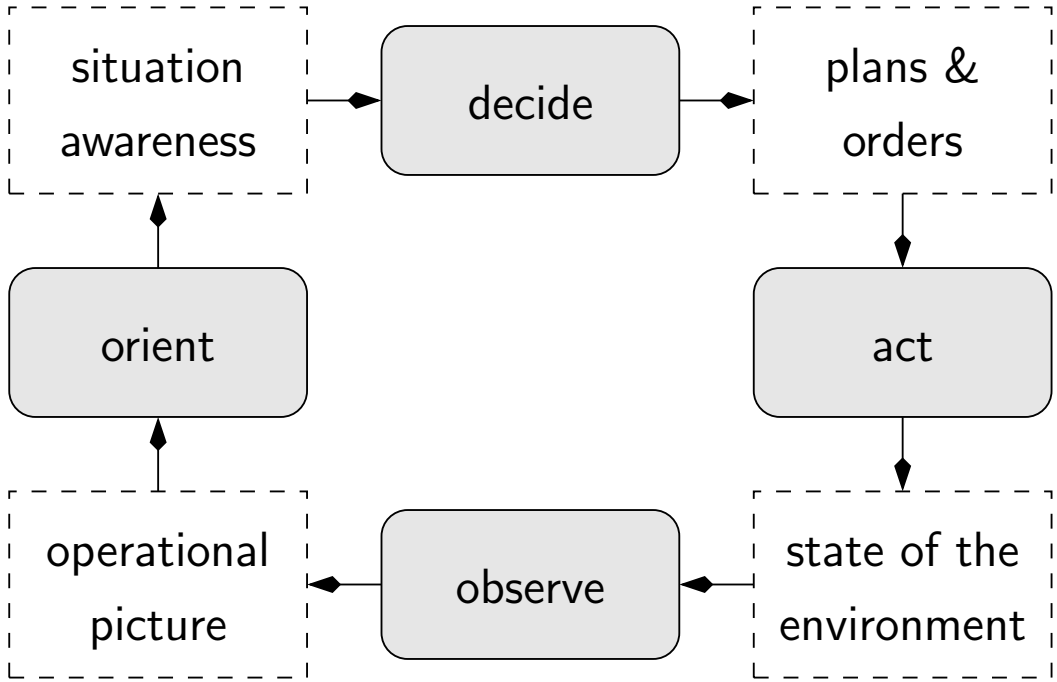
(Endsley, 1995)

situation awareness (SA)



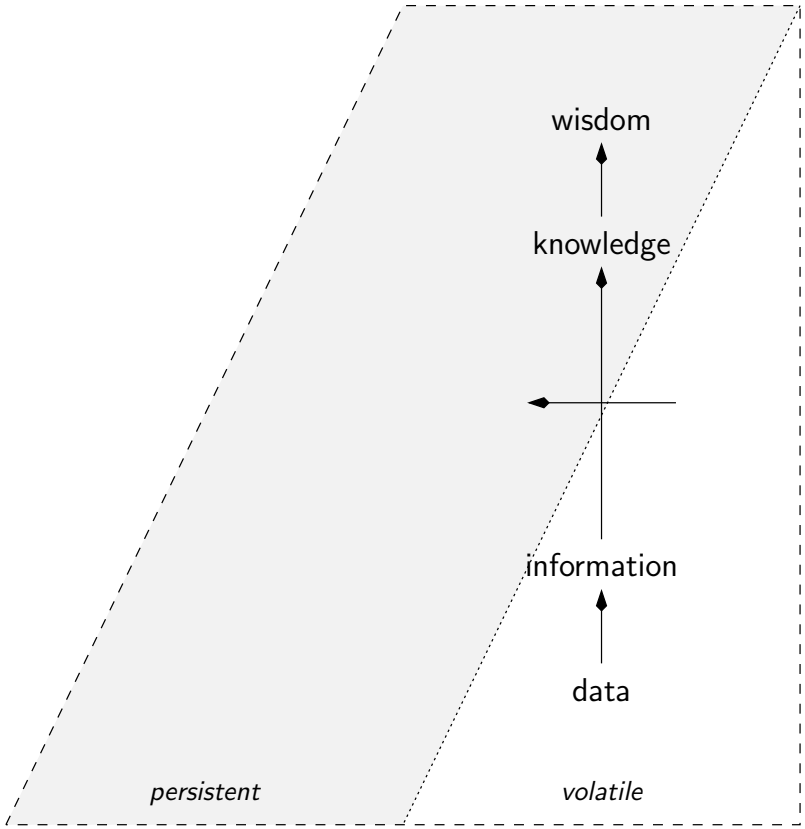
(Jones & Endsley, 2000)

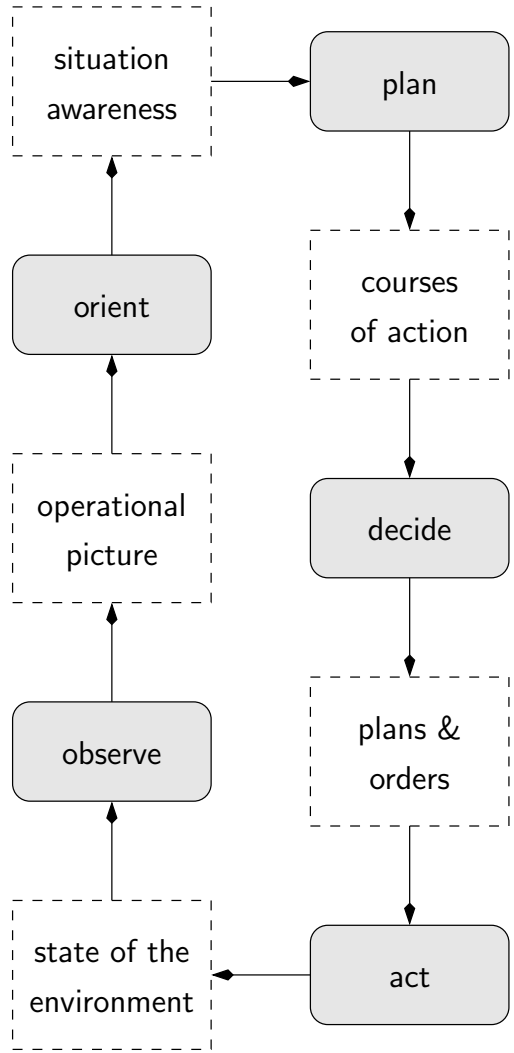
situation awareness (SA)



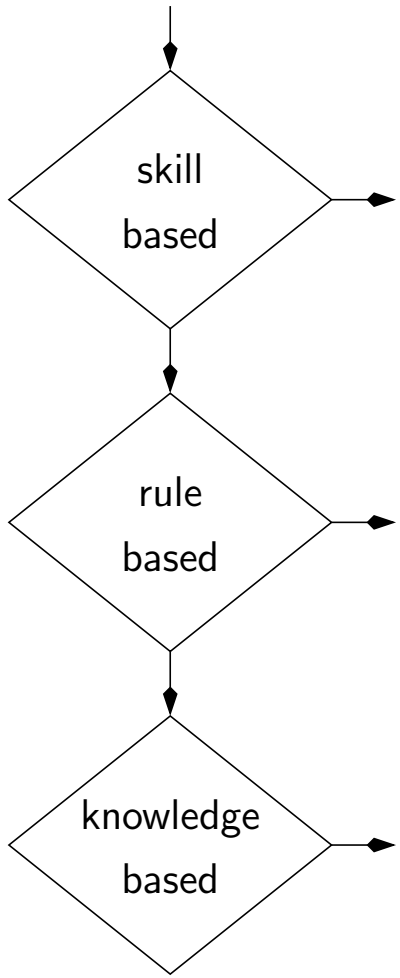
OODA loop
(Boyd, 1987)

situation awareness (SA)





situation awareness (SA)



"without thinking"
(fast)

match system state to a known task
(limited congnitive effort $\rightarrow$ still quite fast)

requires effort and time
(slow)

(Rasmussen, 1983)

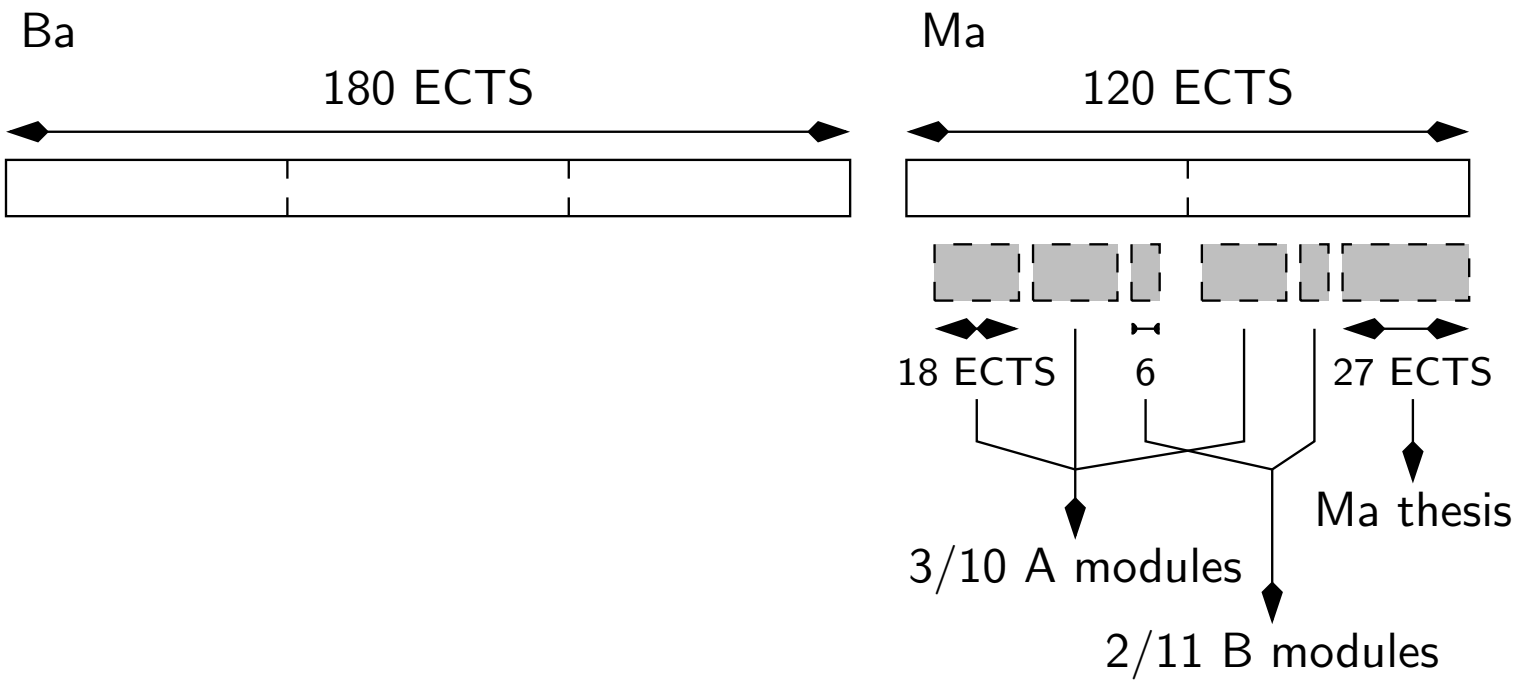
outline

are we there yet ?

education

current situation

POL



education

current situation

POL: A modules

- A1: applied fluid dynamics
- A2: applied mechanical systems
- A3: military and civil engineering
- A4: material sciences
- A5: ballistics
- A6: weapon systems
- A7: global monitoring for security
- A8: communication systems
- A9: **information systems**
- A10: *naval sciences*

education

current situation

POL: module A9

- TE013: telecommunication networks (6 ECTS)
- IN005: operating systems (3 ECTS)
- IN013: distributed systems (3 ECTS)
- IN012: **information security** (6 ECTS)

education

current situation

POL: B modules

- B1: global navigation systems for civil and military applications
- B2: **cyber security**
- B3: helicopter technology
- B4: mechanical design
- B5: complements in finite elements and numerical modelling
- B6: intervention engineering
- B7: forensic sciences
- B8: non conventional weapons
- B9: naval sciences I
- B10: aeronautical sciences
- B11: naval sciences II

education

current situation

POL: module B2

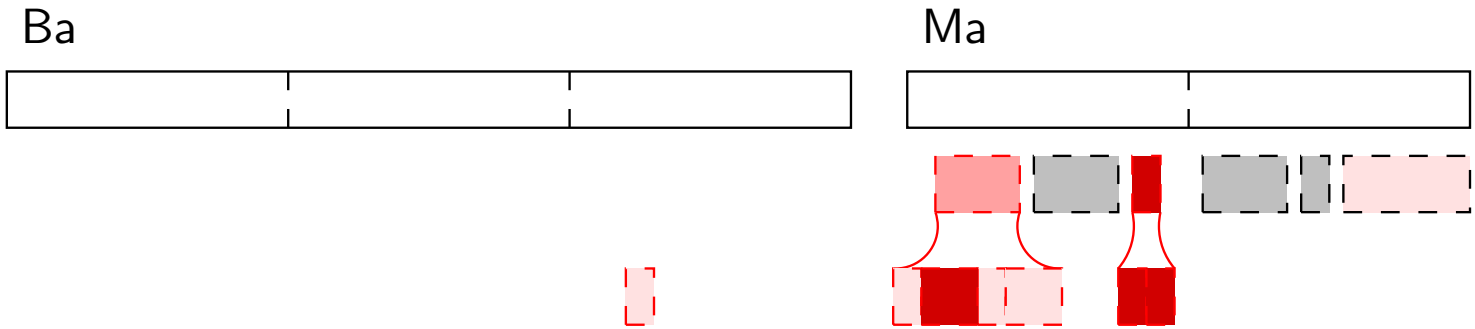
IN014: computer security incident response (3 ECTS)

MM011: cryptography (3 ECTS)

education

current situation

POL optimal cyber “specialist” path



outline

are we there yet ?

the research pole

with its research units

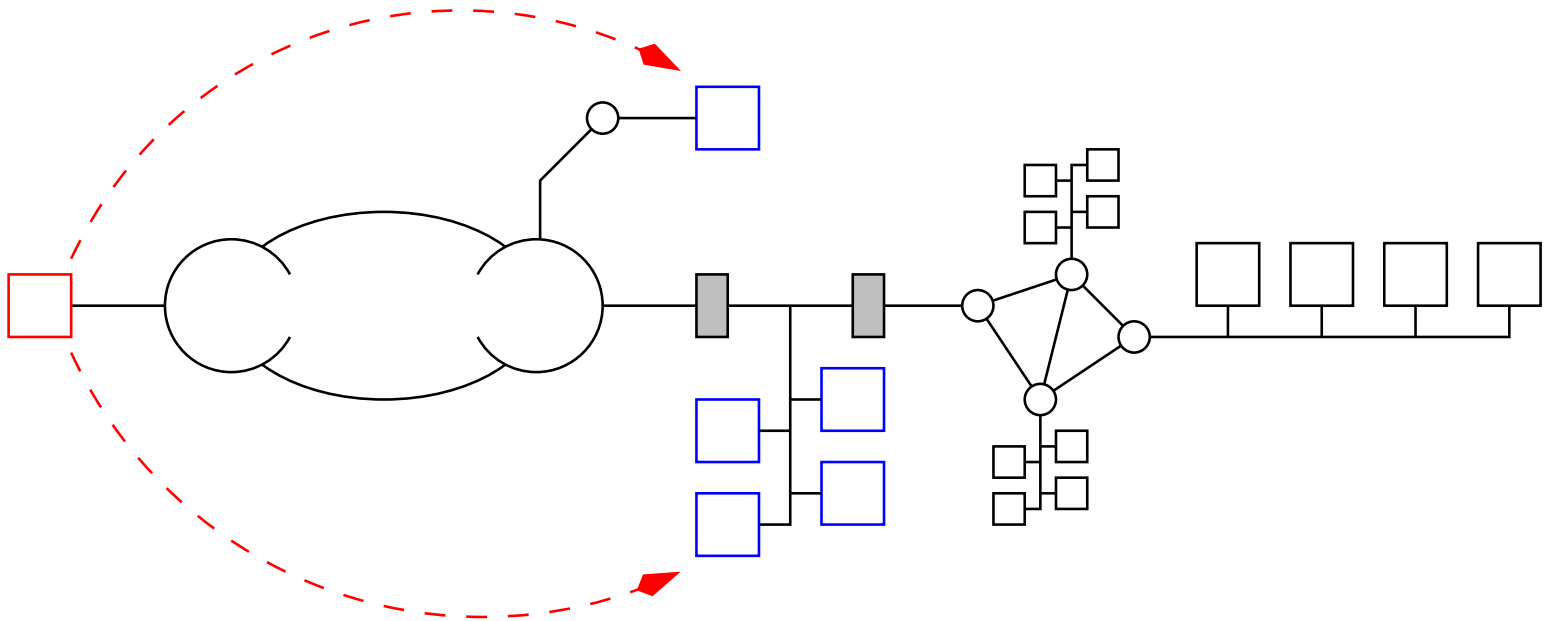
signal & image centre

- image processing
- radar signal processing
- VIPER
- near field electromagnetics
- terahertz
- RCS and IR signatures
- LEMA
- hyperspectral imaging
- audio signal processing
- optical fibers
- radio networks
- geodesy and GNSS
- **cyberdefense**

the collaboration between inter-department multidisciplinary research units leads to interdisciplinary cross-fertilization

old threats

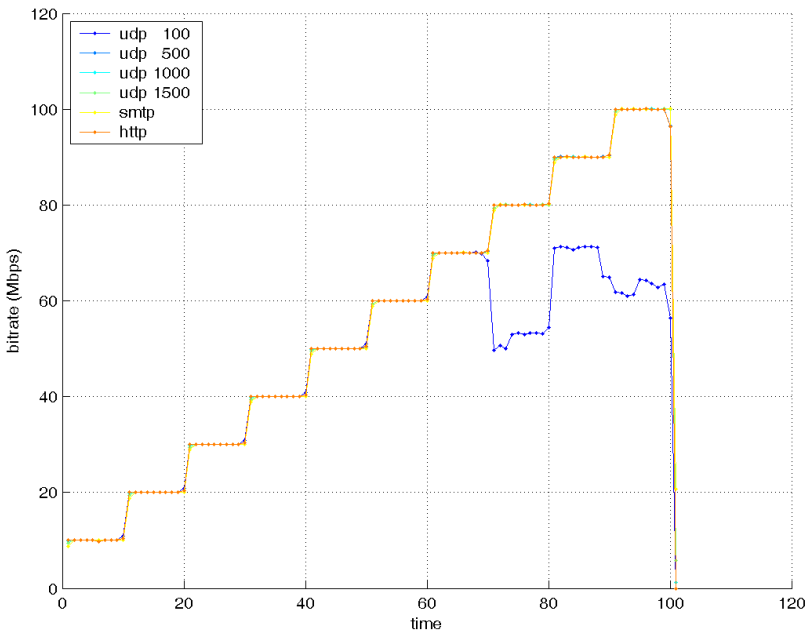
Internet facing services as a target



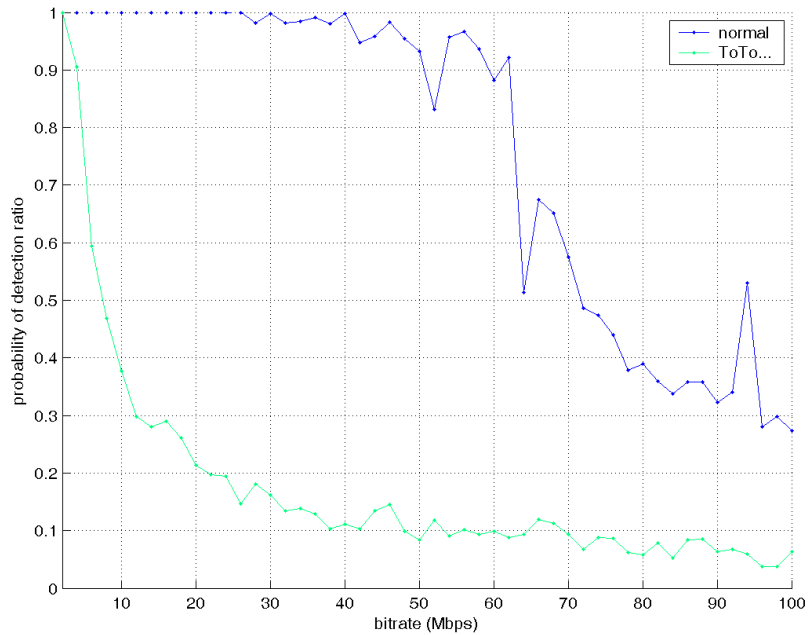
old threats

RMA research on NIDS evasion

packet generator calibration

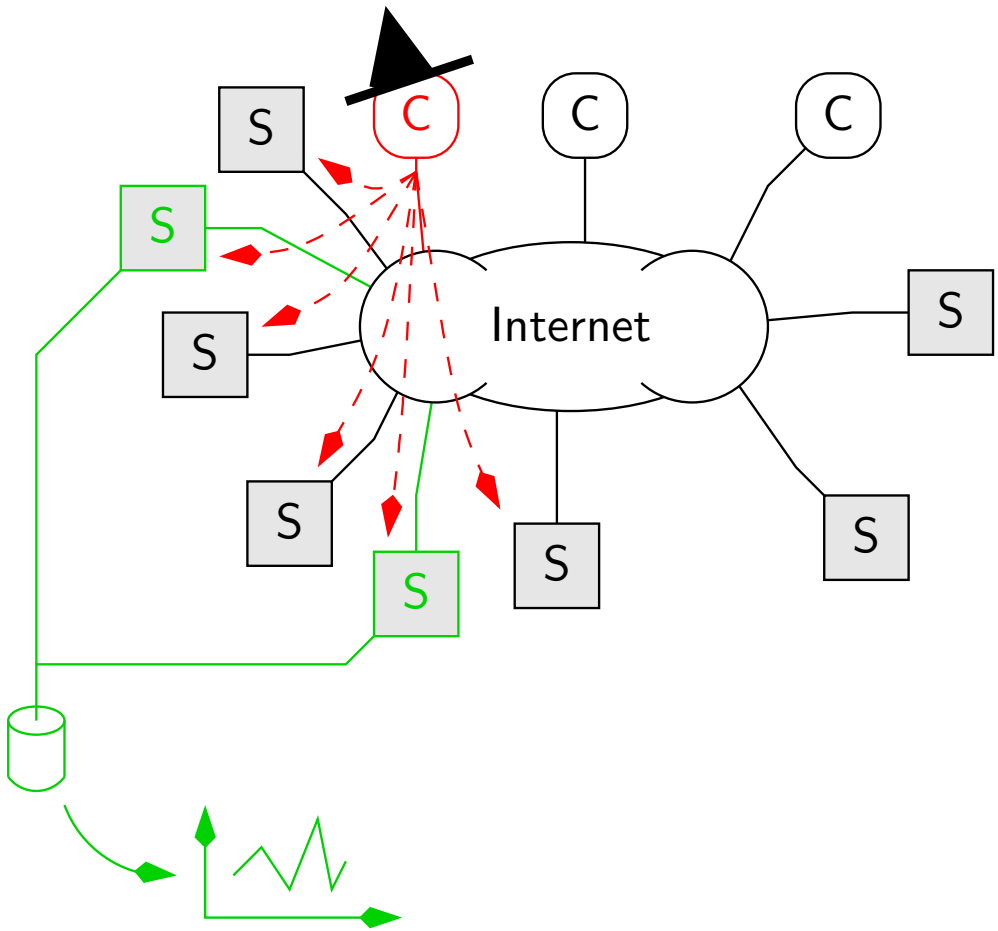


NIDS evasion using PCRE loading



old threats

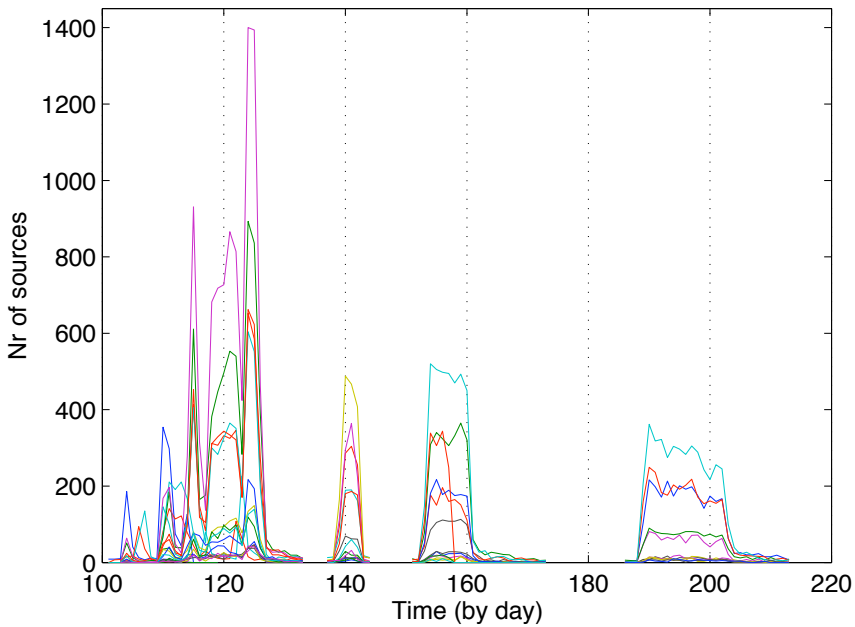
RMA research on honeynets



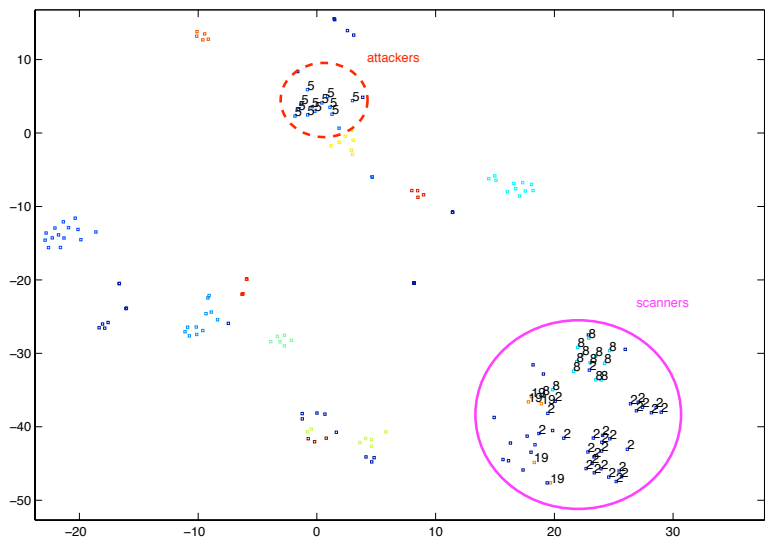
old threats

RMA research on honeynets

time series for zombie army ZA10

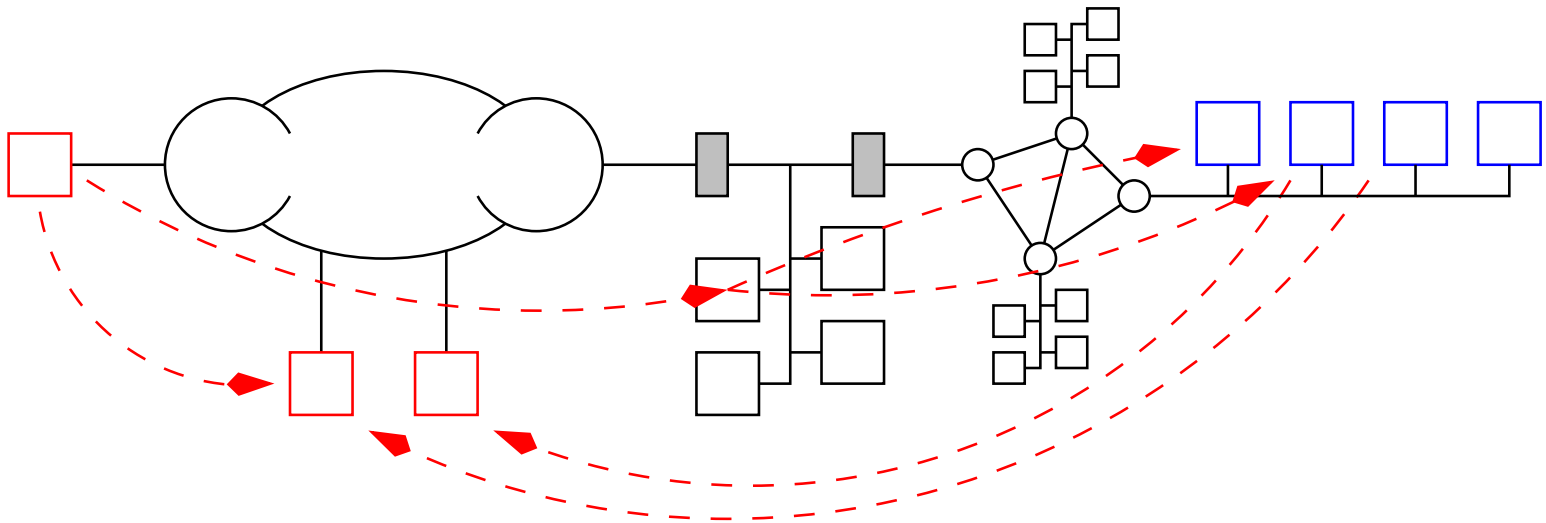


origin subnets ZA10 & ZA11



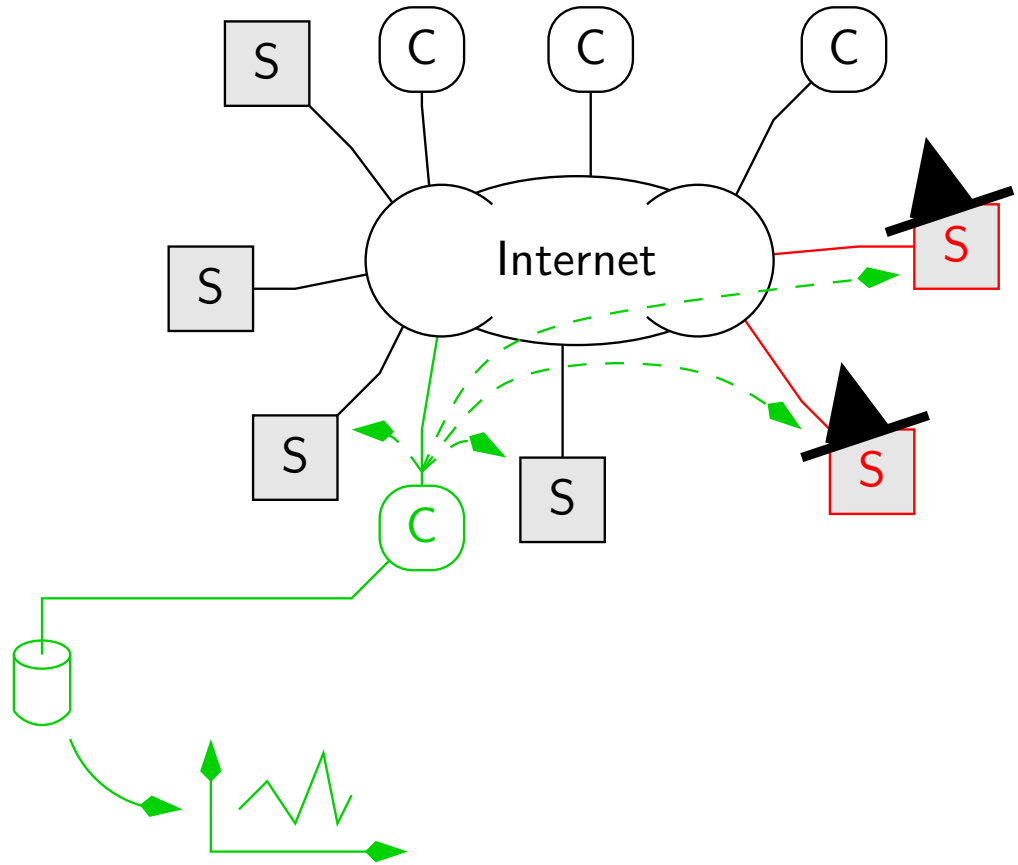
recent threats

client software as a target



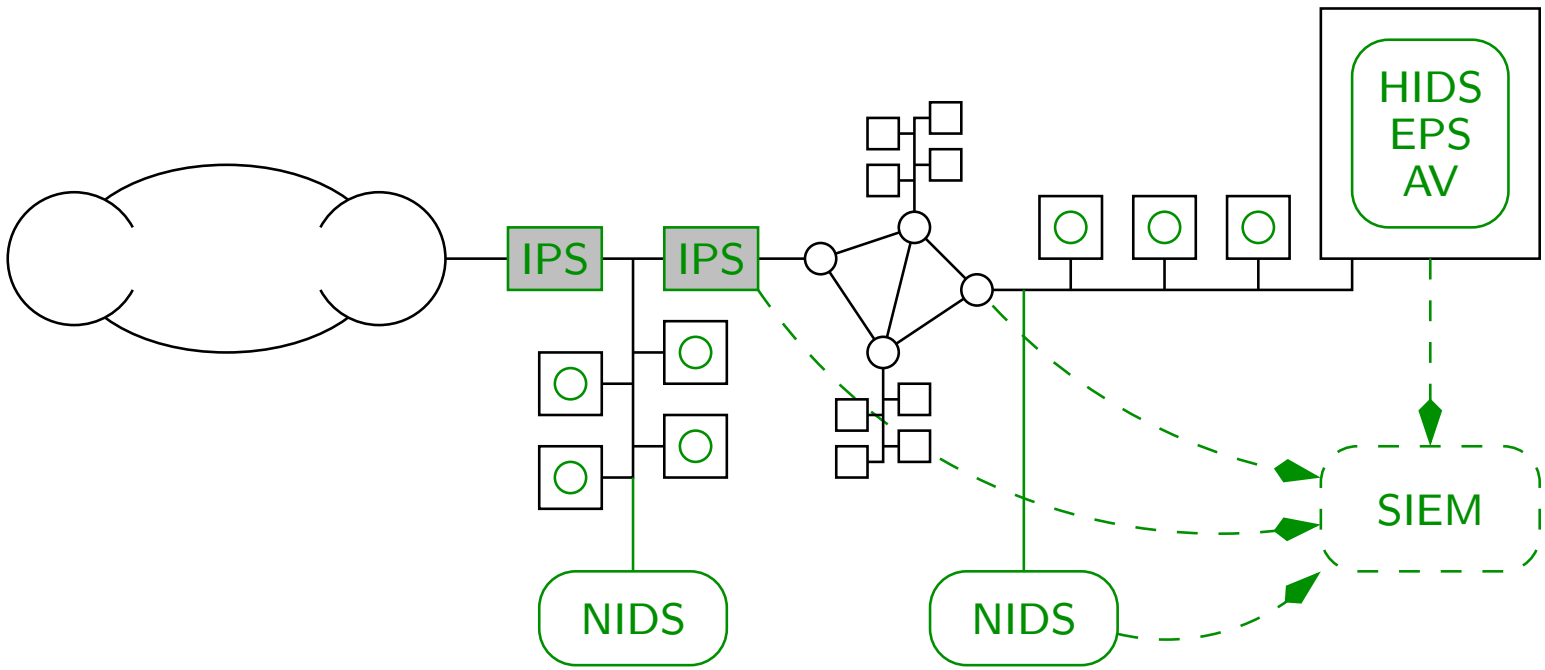
recent threats

RMA research on client honeypots



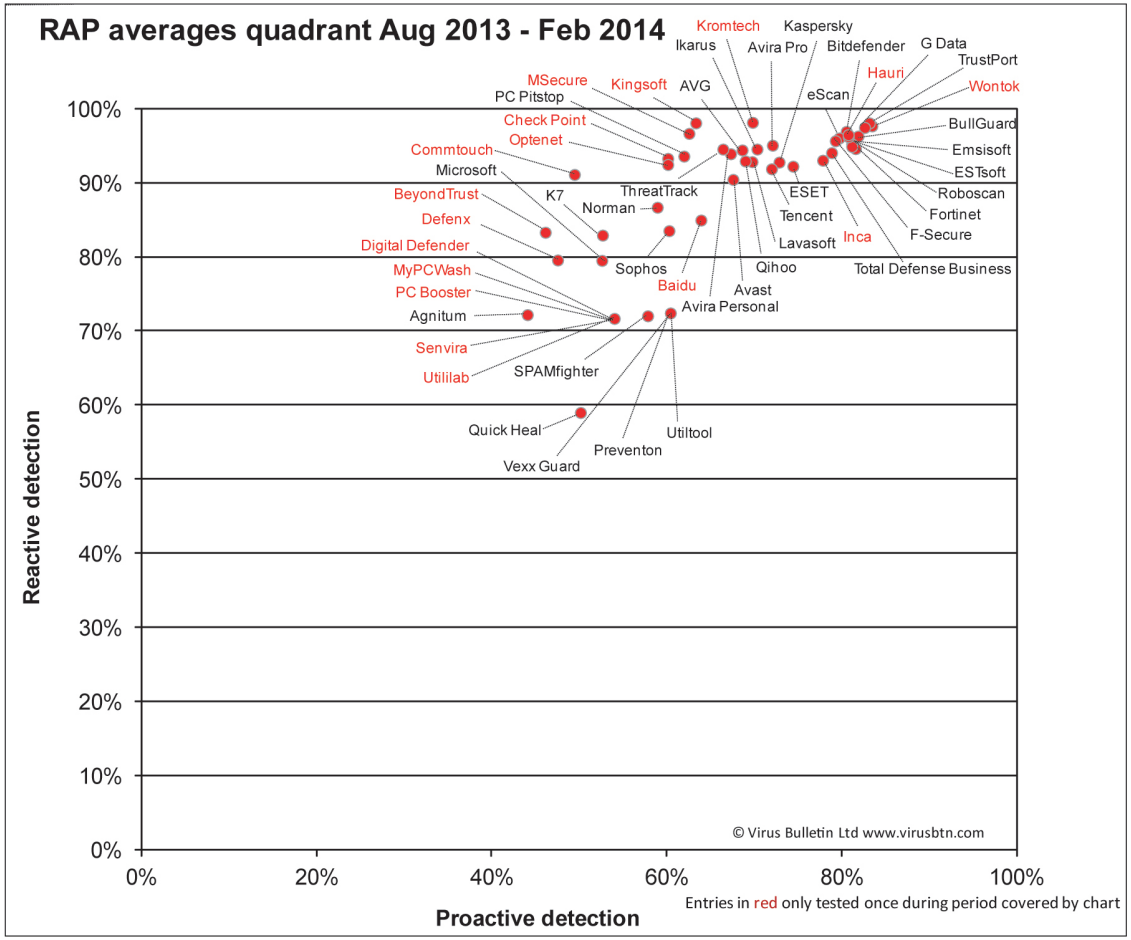
current COTS situation

"holistic" solution



current COTS situation

HIDS / EPS / AV



current COTS situation

SIEM

COTS vendors:

- problem: SIEMs suffer from *selection bias*
- solution: filter late/not

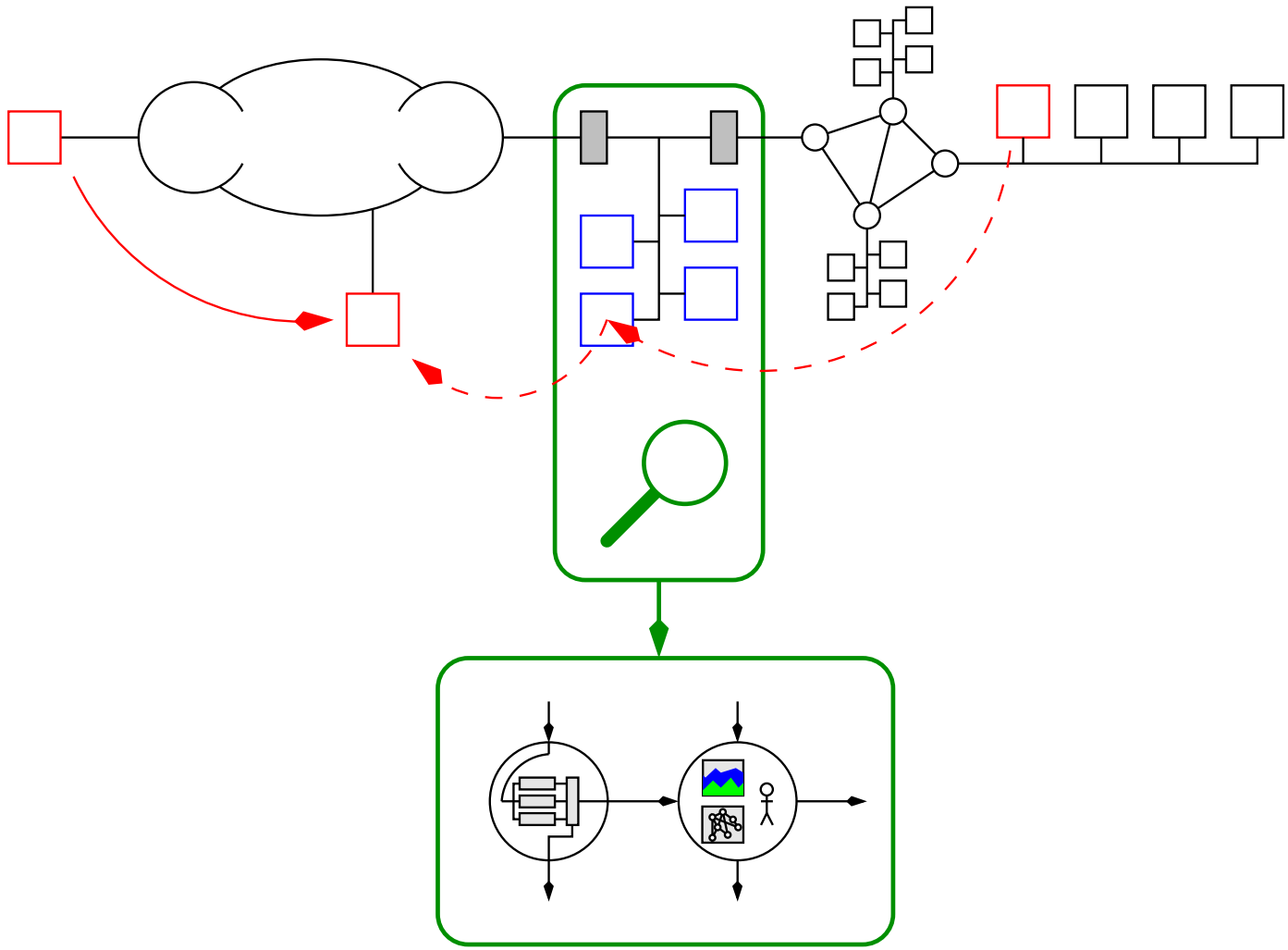
next:

- problem: data volume
- solution: data reduction $\rightarrow$ meta-data

detection:

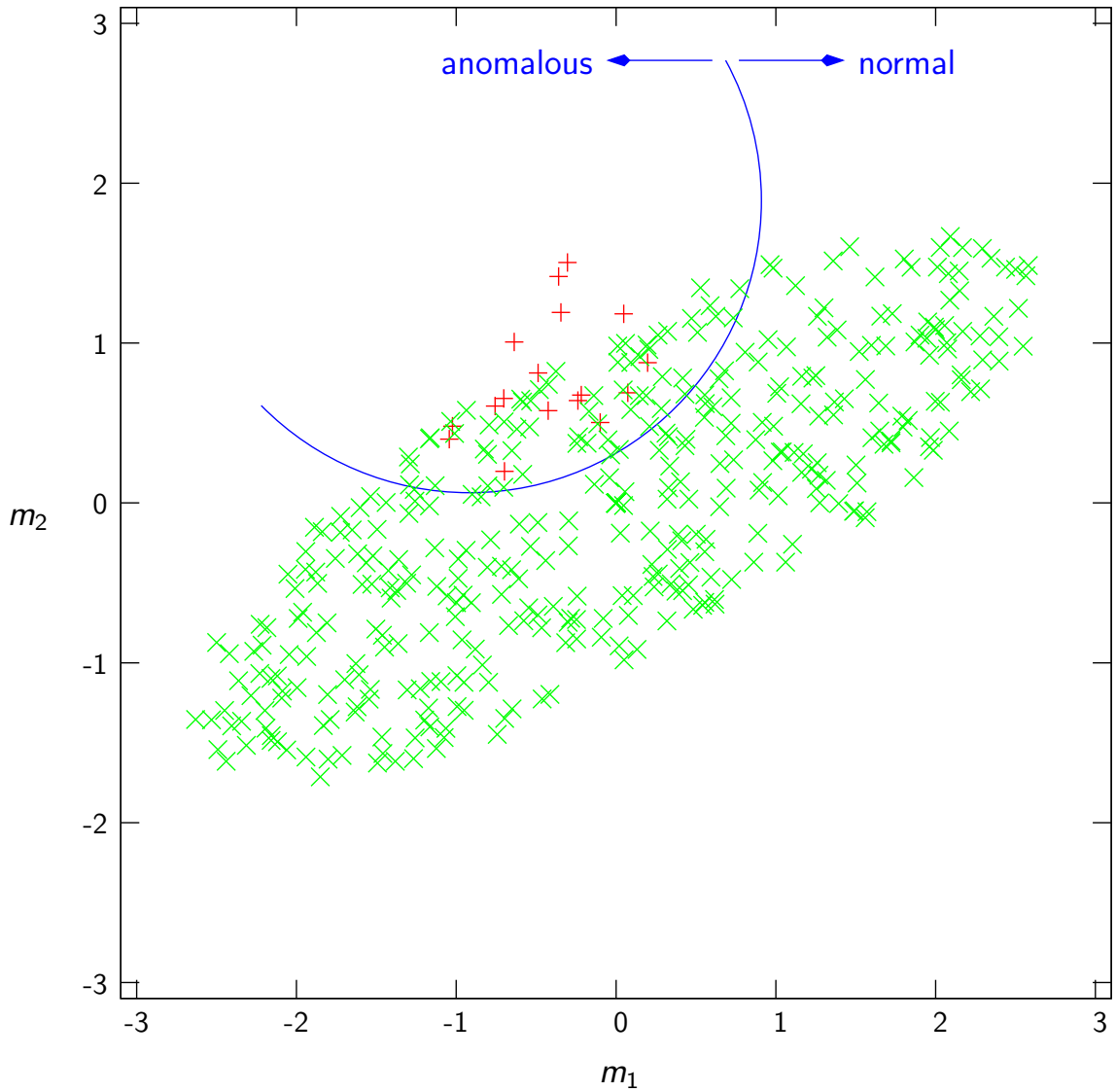
- rules: again selection bias ...
- *"security analytics"*: no info on what/how

our solution



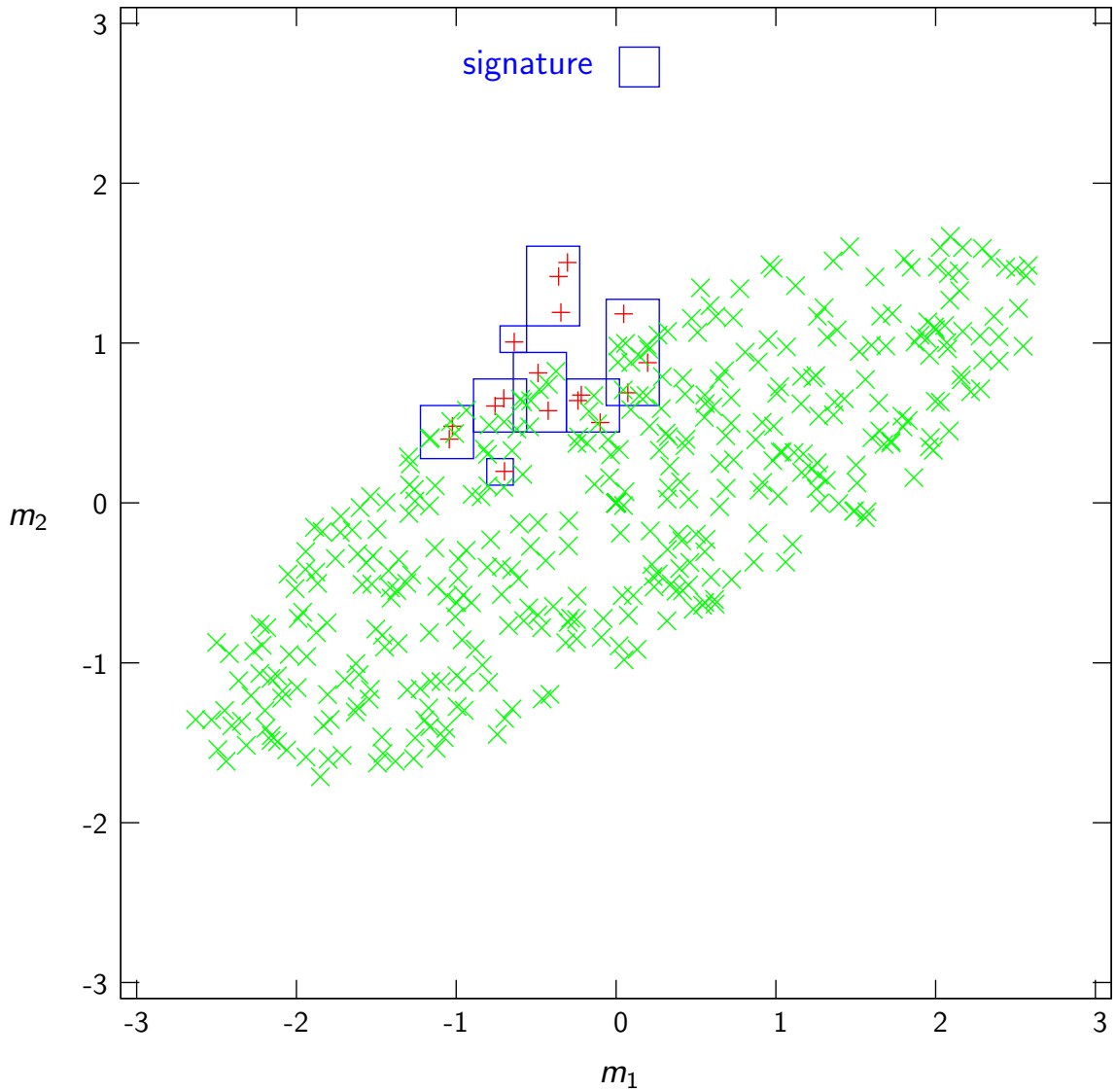
intrusion detection

anomaly-based detection



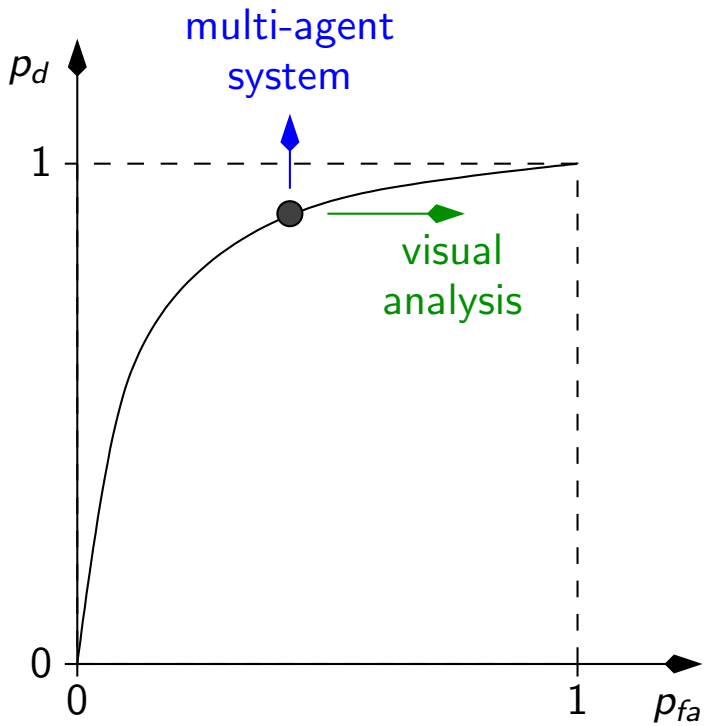
intrusion detection

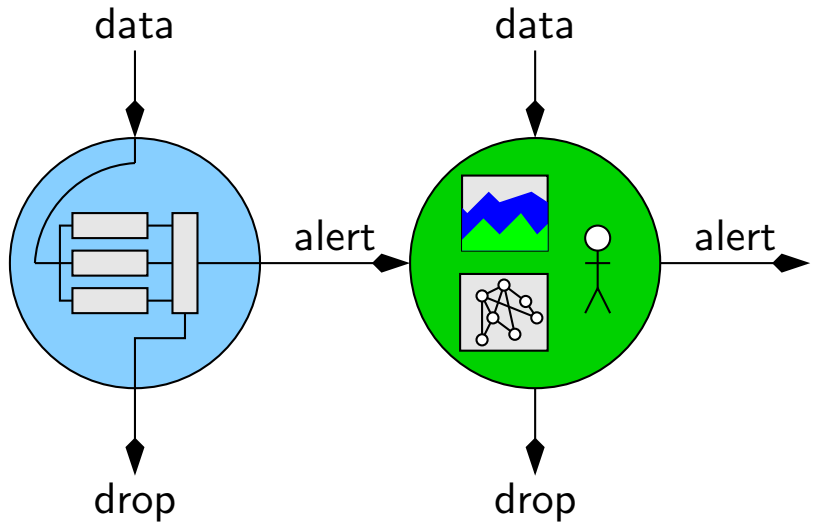
signature-based detection



our solution

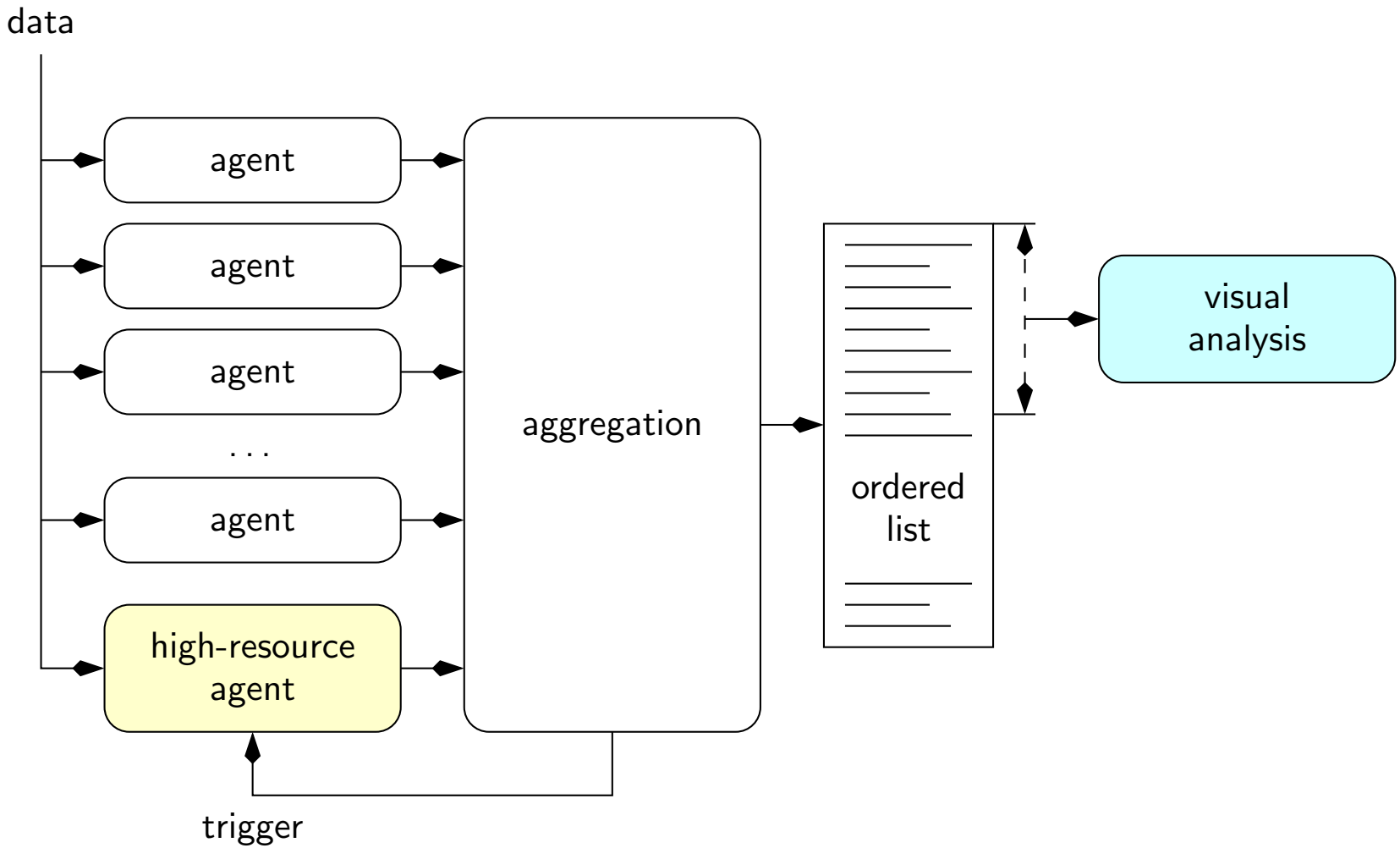
bring the human into the loop





multi-agent system

high-level design of the detection system



questions or comments ?