

Analysis of a Cyber Defense Exercise using Exploratory Sequential Data Analysis

Dennis Andersson
Magdalena Granåsen
Jonas Hallberg

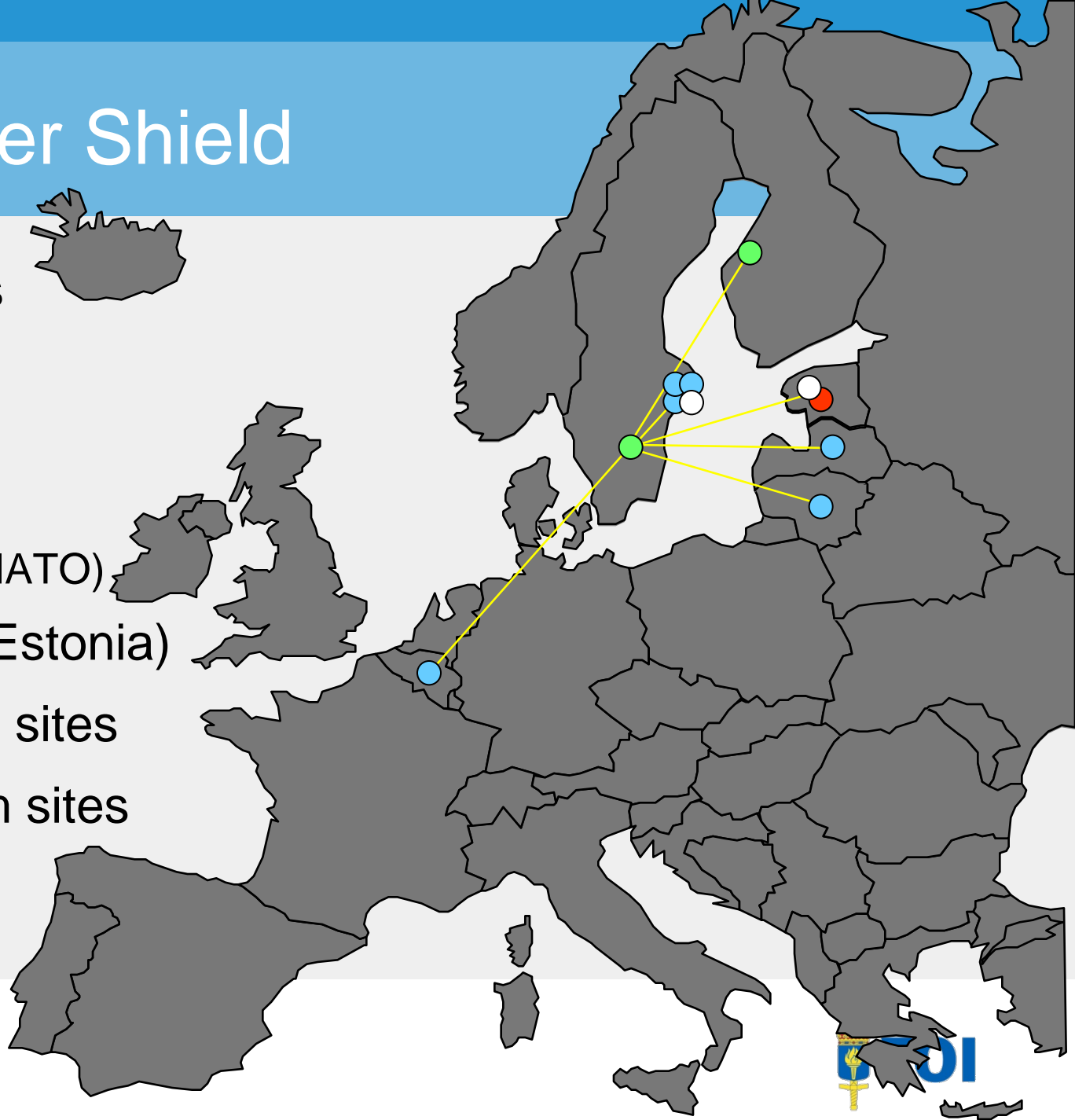


Baltic Cyber Shield

- Scenario-driven 2-day multinational CDX in 2010
 - Swedish side coordinated by MSB
- Motivated by cyber attacks on Estonia 2007
- Main objectives
 - Improve capability of conducting technical IT security exercises
 - Investigate how to study IT attacks and defence of critical infrastructure

Baltic Cyber Shield

- 6 blue teams
 - 3 Swedish
 - 1 Latvian
 - 1 Lithuanian
 - 1 Belgian (NATO)
- 1 red team (Estonia)
- 2 white team sites
- 2 green team sites



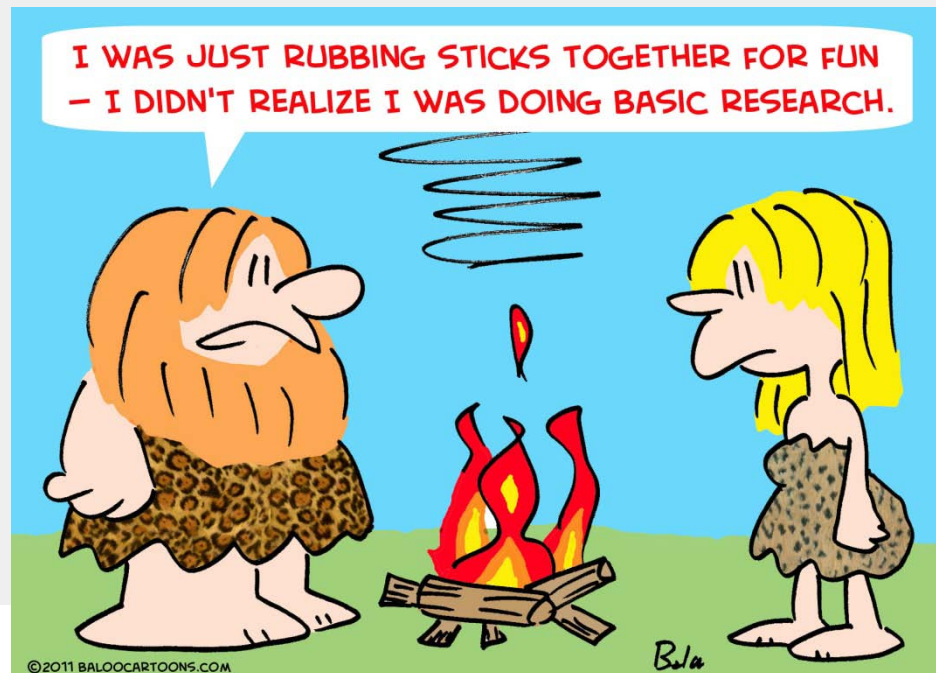
Baltic Cyber Shield

- Mixed-reality
 - Internet simulated at FOI cluster
 - Isolated corporate networks connect to cluster through VPN tunnels
 - Corporate factory replicas accessible through the cluster



Objectives

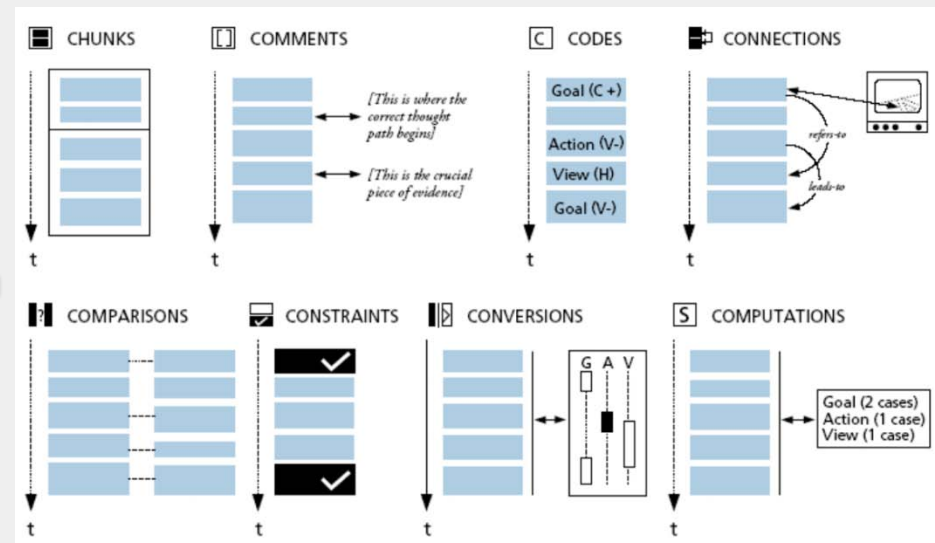
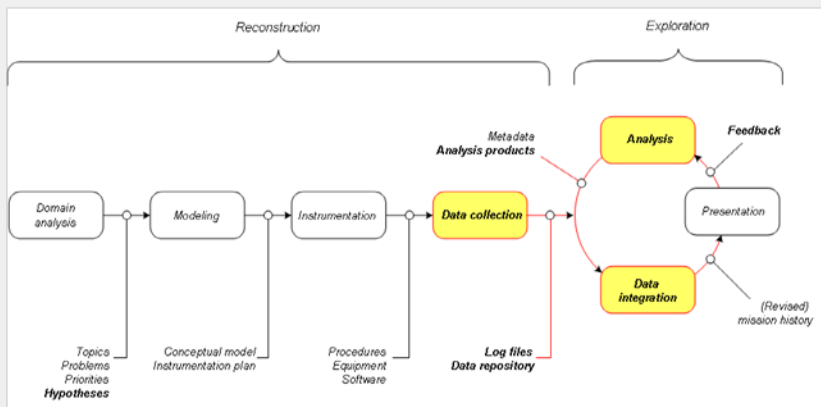
- Training aspect
 - Improve capability of conducting technical IT security exercises
- Scholarly aspect
 - Investigate how to study IT attacks and defence of critical infrastructure



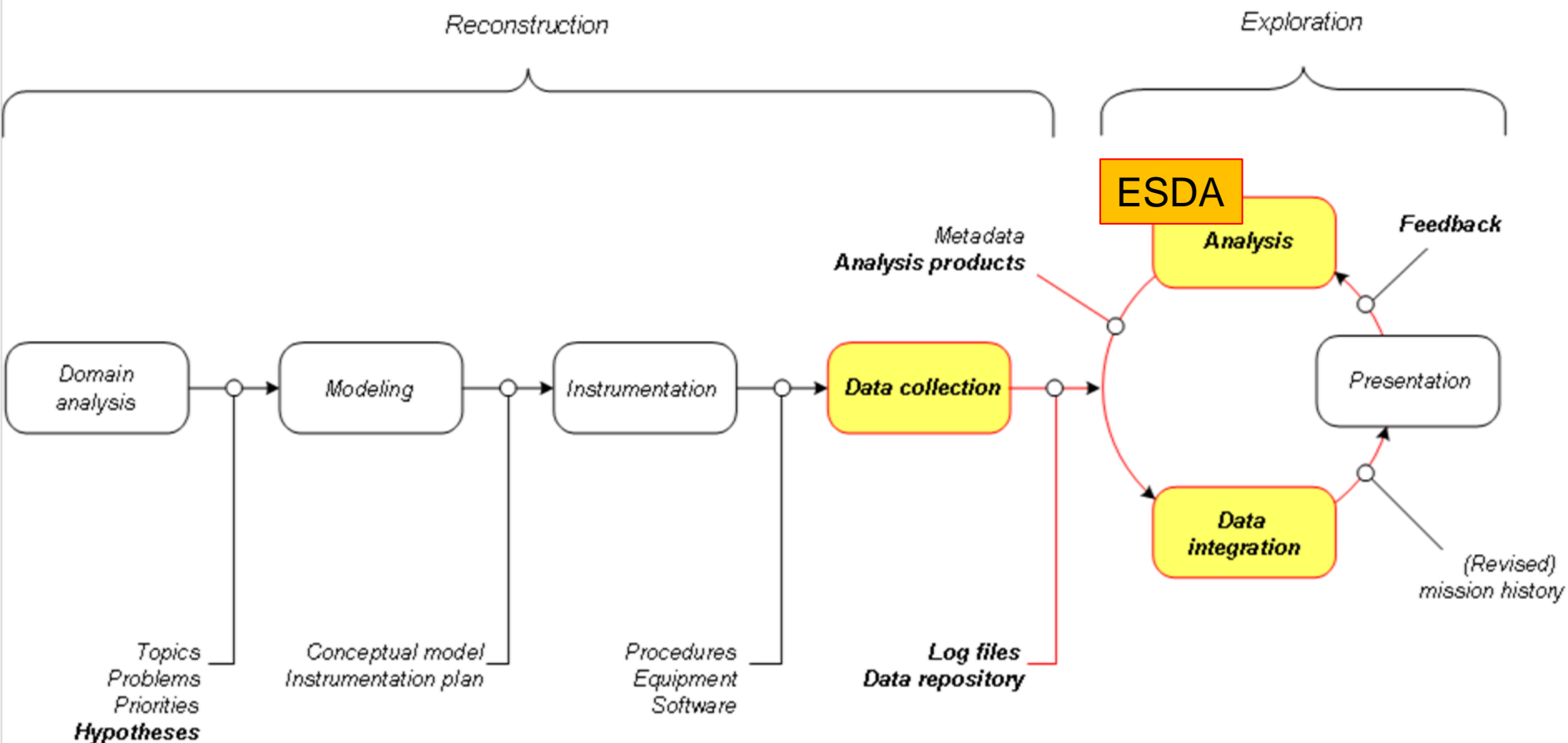
Used with permission from artist [Rex May]

Scholarly aspect

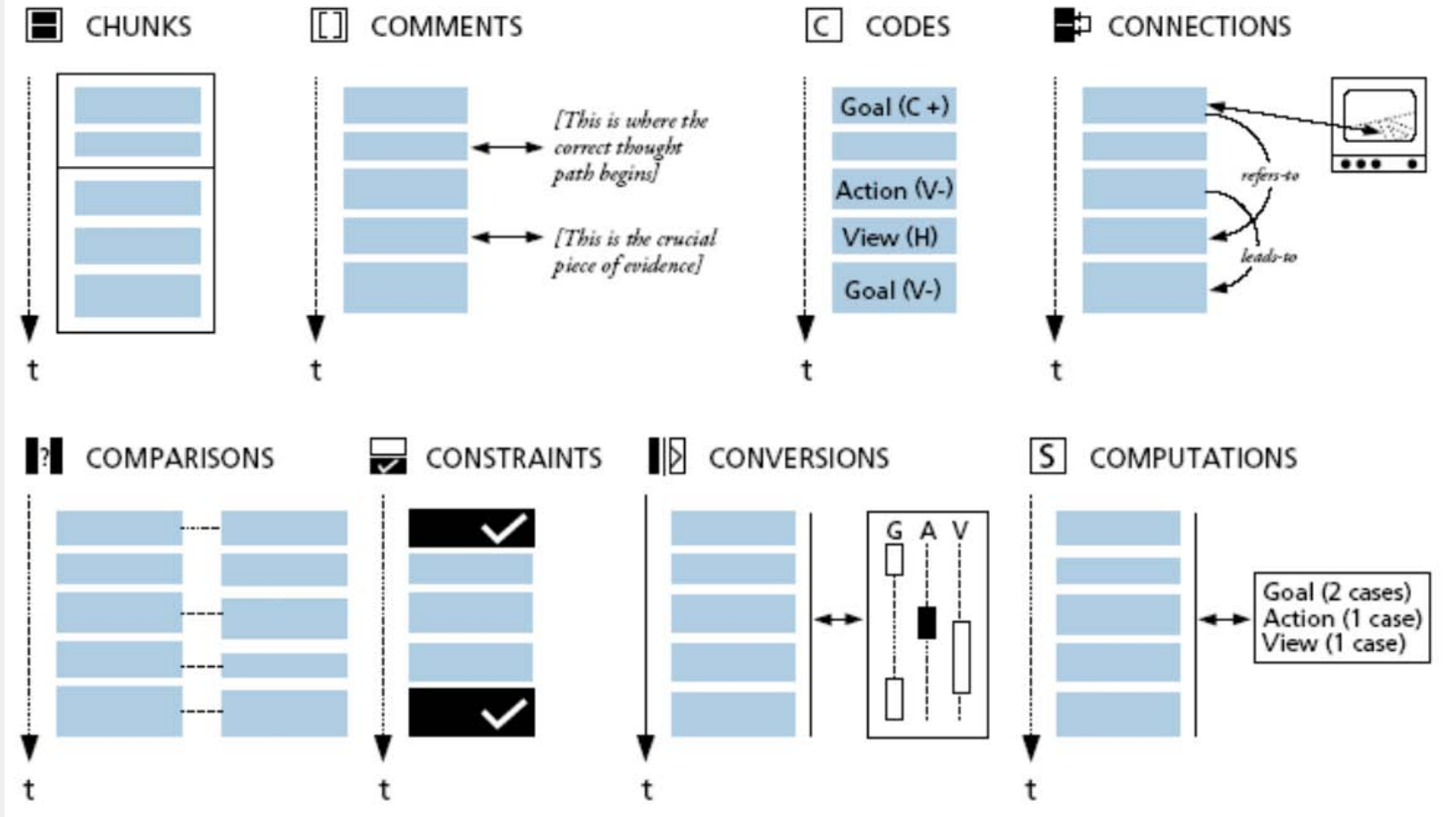
- Can we use Reconstruction & Exploration (R&E) to capture and analyze CDXs?
- Can Exploratory Sequential Data Analysis (ESDA) be combined with R&E to analyze CDXs?



Reconstruction & Exploration

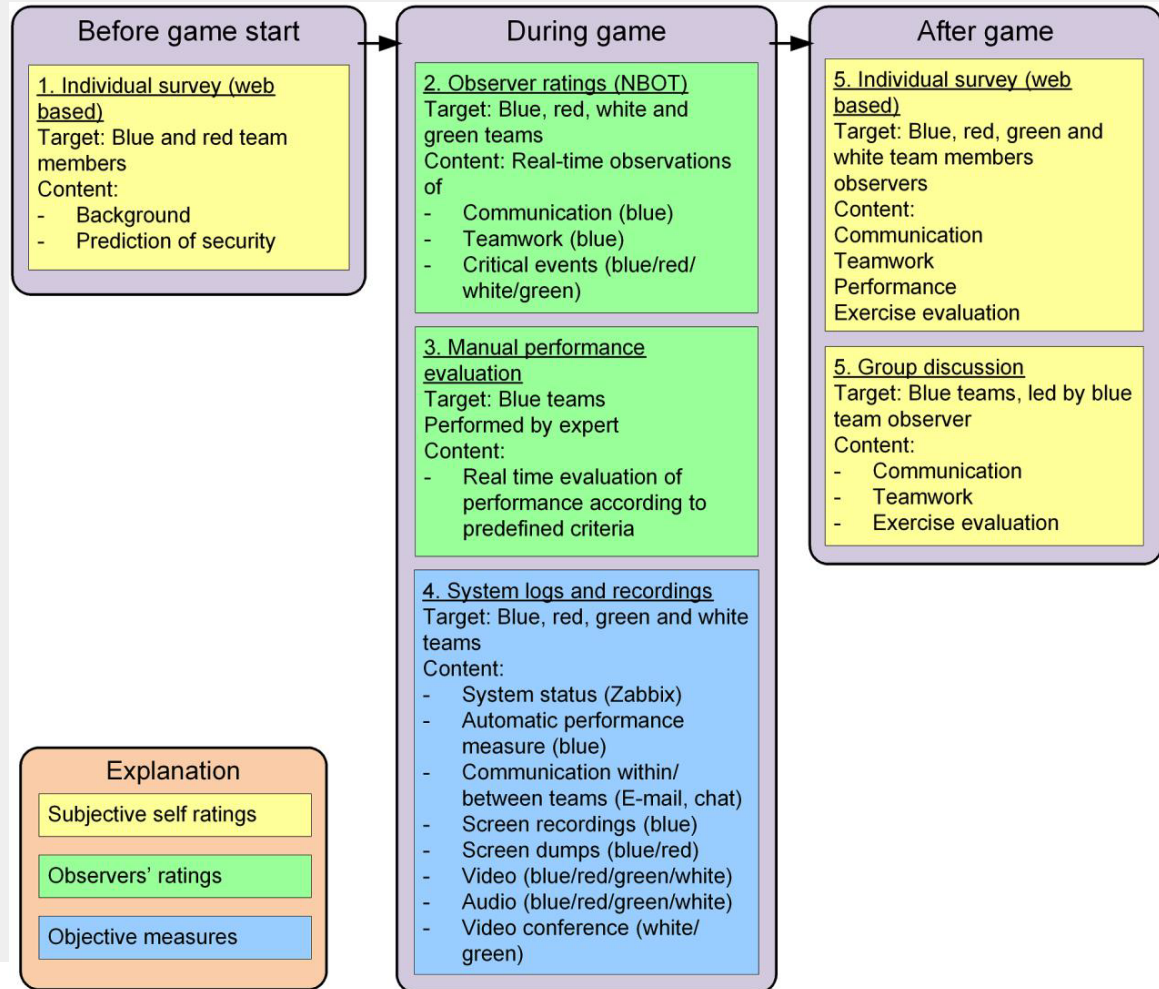


Exploratory Sequential Data Analysis



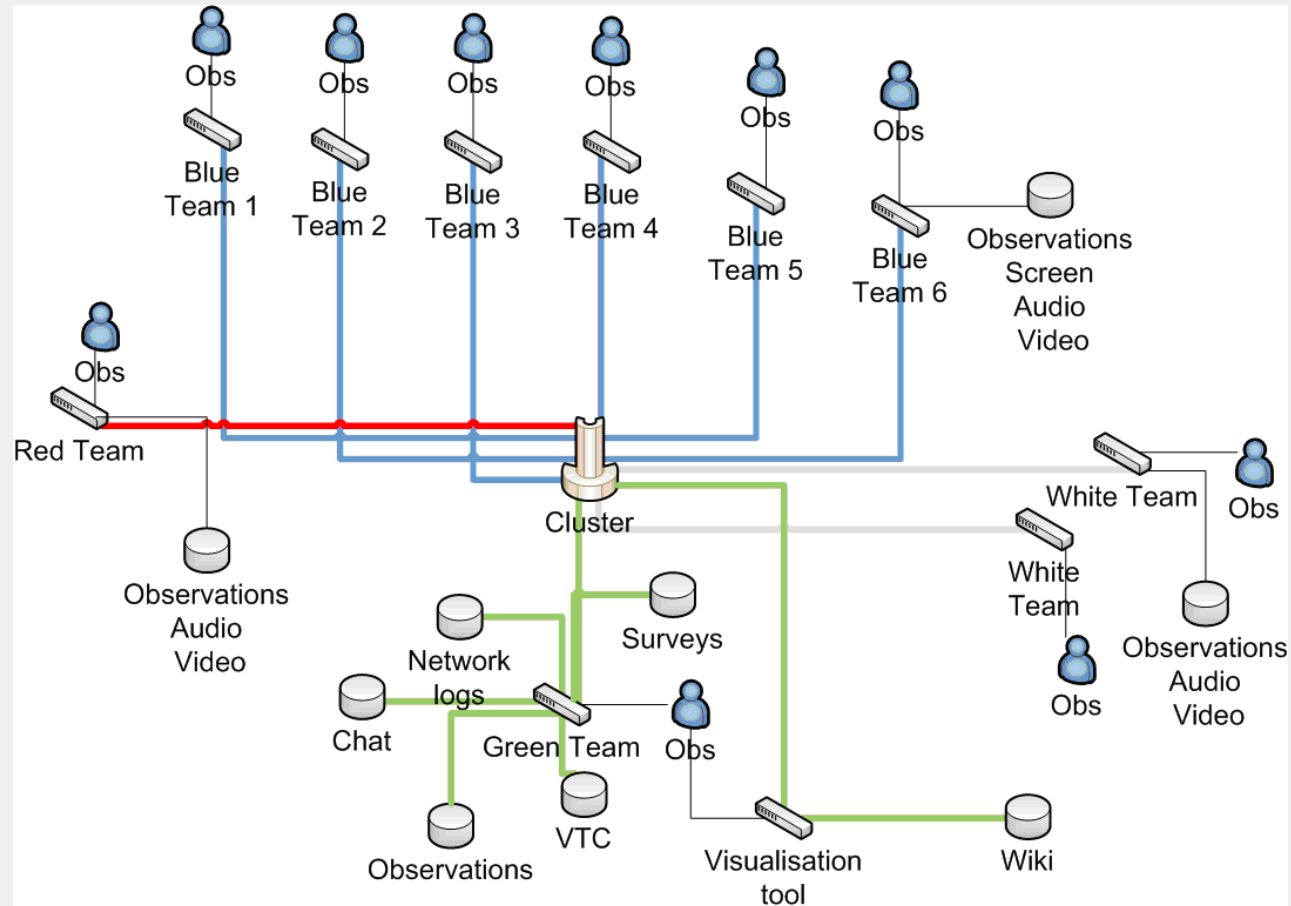
Conceptual model

- Behaviour aspects
 - team performance
 - decision-making
 - collaboration
 - communication
- Technical aspects
 - network status
 - processor utilization
- Background
 - Expertise
 - Background
- Exercise feasibility
 - Training aspect
 - Scholarly aspect



Instrumentation plan

- Interactions
 - Human-Machine
 - Human-Human
 - Machine-Machine
- Technical logging
- Observer reports



Presentation and analysis with F-REX

The screenshot displays the FOI Reconstruction & Exploration Studio (F-REX) interface. The main window is divided into several panes:

- Observer Reports:** A list of events with columns for Time, Task, Summary, Site, and ID. Callout: "Observer reports".
- Timelines:** A large grid showing activity for various entities (e.g., BT2-mic1, BT3-mic1, BT5-mic1, BT6-4, BT6-6, BT6-7, BT6-9, BT2-1, BT2-2, BT2-3, BT2-4, BT3-2, BT3-3, BT3-4, BT3-5, BT3-6, BT3-7, BT3-8, BT3-9, BT6-1, BT6-2, BT6-3, BT6-5, BT6-8) over a time period from 06:00 to 16:00. Callout: "Timelines".
- Time-synchronized model:** A table view of events, similar to the Observer Reports pane. Callout: "Time-synchronized model".
- Configurable views:** A pane showing a list of tasks and their details. Callout: "Configurable views".
- Quickly shift focus:** A callout pointing to the task list. Callout: "Quickly shift focus".
- Virtual chat rooms:** A pane showing a chat log with messages and timestamps. Callout: "Virtual chat rooms".
- Communication/video/reports:** A callout pointing to the chat log. Callout: "Communication/video/reports".
- Chunking:** A callout pointing to the chat log. Callout: "Chunking".
- Commenting:** A callout pointing to the chat log. Callout: "Commenting".
- Coding:** A callout pointing to the chat log. Callout: "Coding".
- Connections:** A pane showing a list of connections and their details. Callout: "Connections".
- Users' e-mail logs:** A pane showing a list of email messages and their details. Callout: "Users' e-mail logs".
- Comparisons:** A callout pointing to the email view pane. Callout: "Comparisons".
- Constraints:** A callout pointing to the email view pane. Callout: "Constraints".
- Conversions:** A callout pointing to the email view pane. Callout: "Conversions".
- Computations:** A callout pointing to the email view pane. Callout: "Computations".

Results (case: reported attacks)

Service	# s_a	# s_d	s_d/s_a
Operator	2	1	0.500
Fileserver	5	1	0.200
External firewall	4	3	0.750
Historian	8	3	0.375
Mail server	6	9	1.500
News server	4	5	1.250
DNS/NTP	1	3	3.000
Database	3	3	1.000
Intranet	3	2	0.667
Public web server	11	12	1.091
Portal	6	7	1.167
Other	7	13	1.857

Results (Experimental study)

- Experimental studies
 - Weak indications from first study
 - The historian and the fileserver were easiest to attack without being detected by the defending team
 - More investigation needed
 - We have the data, i.e. network traffic and some detailed system logs
 - Detailed studies are under way from FOI and KTH

Conclusion

- The teams' self-reporting provide an excellent source of information in the early stages of analysis
- Scholarly objectives
 - R&E has shown great potential for analyzing CDXs
 - The ESDA 8C's have been found very useful as guidelines for R&E exploration

Conclusion (cont'd)

- A comprehensive dataset like the collected BCS data is a great resource for many different kind of studies
- Contact information:
Swedish Defence Research Agency
Dennis Andersson
denand@foi.se
+46 (0)13 378560
- Thank you for your attention!