16th ICCRTS
"Collective C2 in Multinational Civil-Military Operations"

Analysis of a Cyber Defense Exercise using Exploratory Sequential Data Analysis

Topics
Cyberspace Management
Experimentation, Metrics, and Analysis
Information and Knowledge Exploration

Dennis Andersson[1], Magdalena Granåsen[1], Thomas Sundmark[1], Hannes Holm[2], Jonas Hallberg[1]

[1]Swedish Defense Research Agency
Box 1165, SE-581 11 Linköping, Sweden

[2]KTH Royal Institute of Technology
Kungl Tekniska Högskolan, SE-100 44 Stockholm, Sweden

Point of Contact
Dennis Andersson
Swedish Defense Research Agency
+46 (0)13 - 37 85 60
dennis.andersson@foi.se

Abstract

Baltic Cyber Shield 2010 (BCS), a multi-national civil-military cyber defense exercise (CDX), aimed to improve the capability of performing a CDX and investigate how IT attacks and defense of critical infrastructure can be studied. The exercise resulted in a massive dataset to be analyzed and many lessons learned in planning and executing a large-scale multi-national CDX. A reconstruction & exploration (R&E) approach was used to capture incidents such as attacks and defensive counter-measures during the exercise. This paper introduces the usage of R&E combined with exploratory sequential data analysis (ESDA) and discusses benefits and limitations of using these methods for analyzing multi-national cyber defense exercises.

Using ESDA we were able to generate statistical data on attacks from BCS, such as number of reported attacks by the attackers and the defenders on different type of services. Initial results from these explorations will be analyzed and discussed.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Analysis of a Cyber Defense Exercise using Exploratory Sequential Data Analysis	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Swedish Defense Research Agency,Box 1165,SE-100 44 Stockholm Sweden,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**25**	

Introduction

Most organizations and services are critically dependent on reliable and secure information systems. Thereby, cyber warfare and terrorism is becoming a significant threat to recognize in today's society. Incidents such as the cyber attacks on Estonia in 2007 and the attacks on U.K., U.S., German and French resources in 2005 [4] are frequently cited and evidences of that the threat is real. However, the amount of publicly available data from such incidents is limited, which makes it difficult to study the associated phenomena. Hence, there is a need for data that conceptualize the phenomena of cyber warfare and terrorism, which thereby motivates cyber defense exercises (CDX) simulating such attacks and training teams in how to defend critical information systems.

In May 2010, the Cooperative Cyber Defense Centre of Excellence and the Swedish National Defense College hosted the Baltic Cyber Shield (BCS) international cyber defense exercise (CDX). For two days, six Blue Teams from northern European government, military and academic institutions defended simulated power generation companies against a Red Team of 20 computer hackers. The scenario described a volatile geopolitical environment in which a hired-gun Rapid Response Team of network security personnel defended Critical Information Infrastructure (CII) from cyber attacks sponsored by a non-state terrorist group. [3]

The technical infrastructure was designed and implemented in a computer cluster located at, and hosted by, the Swedish Defense Research Agency (FOI). Each blue team network consisted of a number of virtual computers on the cluster, containing vulnerabilities to be exploited by the red team. The network connections were established through Virtual Private Networks (VPNs) enabling the teams to be physically distributed. Moreover, the networks were connected to the Programmable Logic Controllers (PLCs) of a power infrastructure model, including steam engines, solar panels, a simulated distribution network and factories with butane flames that could be detonated by the red team. Thus, a mixed-reality supervisory control and data acquisition (SCADA) network was created. [5]

The BCS CDX had three main goals: training of the Blue Teams, highlighting the international aspects of cyber defense, and improving the knowledge on how to perform CDXs [3]. To accomplish those goals, the outcome of the CDX needs to be carefully studied. Thus, a massive data set was collected, containing both qualitative and quantitative data. The resulting data set has shown great potential for analysis. The objective of this paper is to describe the actual data collection, the analysis process, and discuss initial findings.

Method

During planning of the exercise, it was soon recognized that a structured way of organizing data collection was needed to be able to handle the multitude of available data sources and enable the analysis required to fulfill the goals of the BCS CDX. The Reconstruction & Exploration approach (R&E) (fig.1) was selected due to its capacity to deal with large and complex data sets as well as being well-known by the analyst team [1]. R&E was originally designed for use with distributed tactical operations (DTOs) like military or crisis management operations [6] and as such had never before been applied in its entirety to the IT security domain.

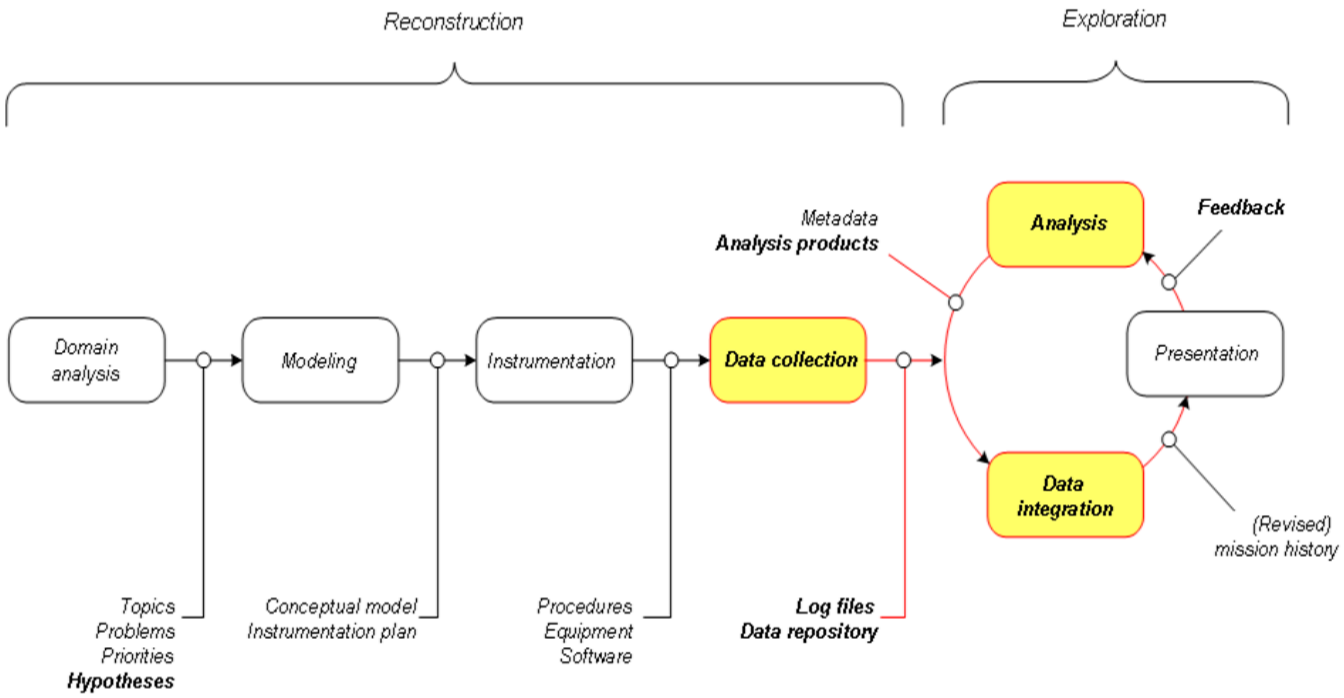


Figure 1. The process of Reconstruction & Exploration [1]

R&E consists of 7 steps, domain analysis, modeling, instrumentation, data collection, data integration, presentation and analysis. The output of the domain analysis and modeling showed the need for collection of both quantitative and qualitative data (fig.2), with the main focus on the blue teams. However, data collection also included red team activities as a reference for understanding blue team actions. Objective data in terms of system logs was assumed to provide results on the teams' activity in the system, but in order to understand why the teams chose the actions they did, there was a need to collect also the participants' views of what was happening and the reasoning within the teams. Therefore, it was decided that observers would be placed within each team, and that questionnaires would be used as a means to collect the subjective estimations of what they were experiencing.

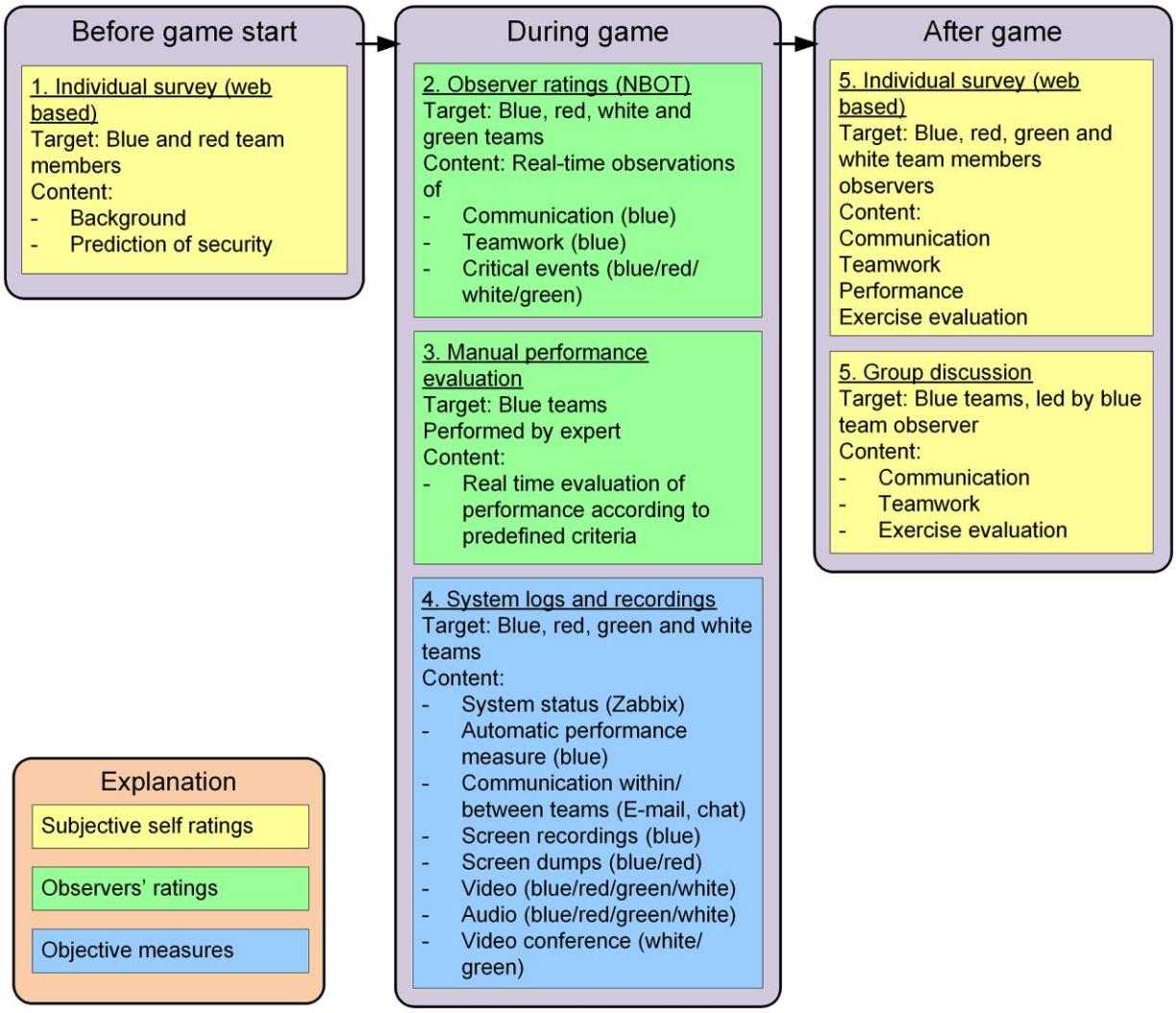


Figure 2. Prioritized data collection nodes

It was decided that video cameras, audio recorders, screen capture tools and human observers should be placed in each team and surveys were to be distributed among the training audience (fig.3) to try to capture the behavioral aspects of the teams. Observers were equipped with Network-Based Observation Tool (NBOT) [9] to enable quick and intuitive reporting of interesting events. Data collection for the objective measures included e-mails, chat sessions, keyboard interactions, network traffic and utilization of memory, processors and hard disk space on each node in the virtual network. In order to capture screen video and keyboard interactions, custom made scripts had to be installed on every machine used in the network. Because it was decided that some of the teams should use their own computers, the analyst team had to rely on participants' willingness to cooperate and install these scripts on their respective machines. For the teams that were supplied workstations by the exercise organizers, however, it was easier to setup and control this logging. For the supplied Windows computers a custom-made screen capture program was used, while on Linux the participants were recommended to use xvidcap[1], but any other appropriate application was allowed. To capture the terminal I/O a script to be executed by the participants was supplied as part of the team packages.

[1]http://xvidcap.sourceforge.net/

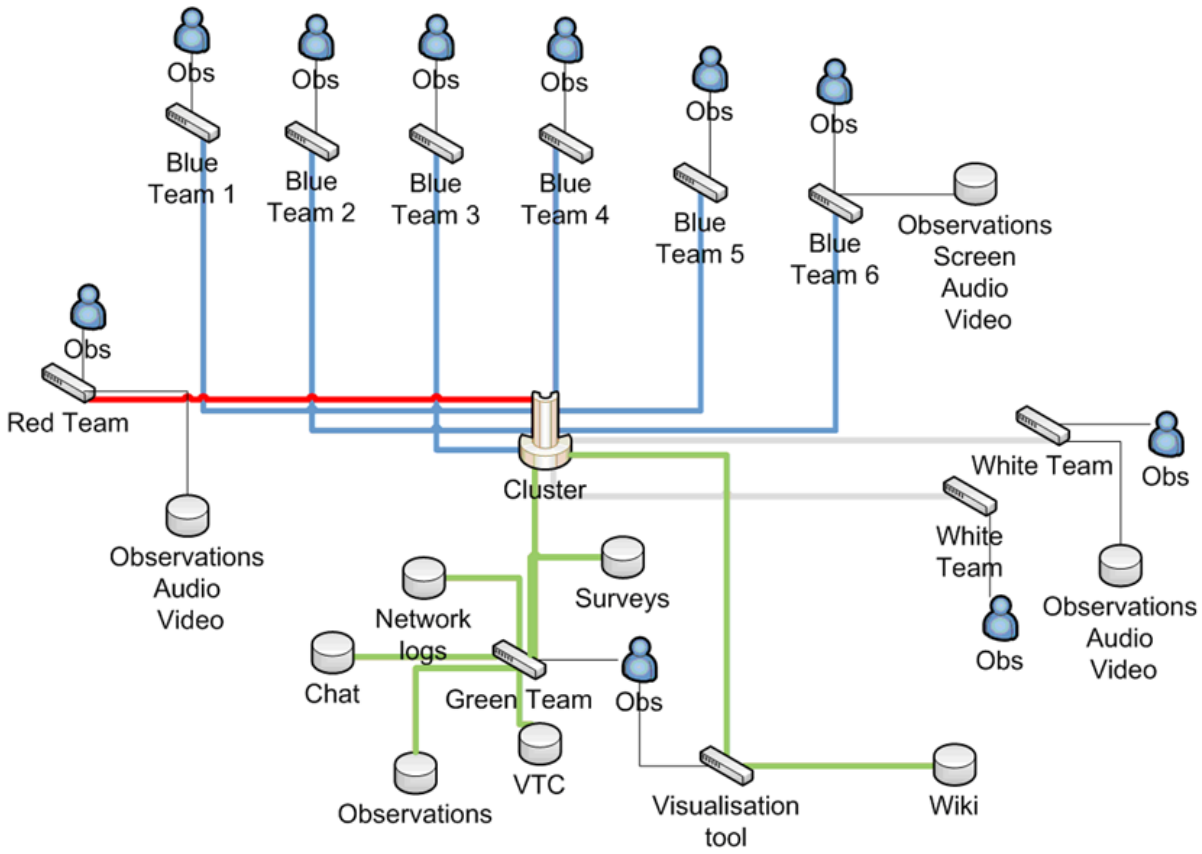


Figure 3. Logical distribution of teams, observers and data collection nodes [5]

Some data, such as e-mails, video feeds and NBOT reports were also available in real-time for the exercise judges (the White team, WT) who used that information to score blue team performance [3].

Data was collected throughout the whole two-day exercise, in total 3 TB of data was collected. F-REX [1] was used for the exploration part of R&E. F-REX (fig.4) is a completely configurable tool allowing users to view a large and heterogeneous data set in a uniform and synchronized manner, much like playing a DVD back and forth. Its features include quick and easy timeline-based navigation in data based on timestamps from the data collection tools. At any time the analyst can shift focus in F-REX by applying a new layout with any views he or she prefers.

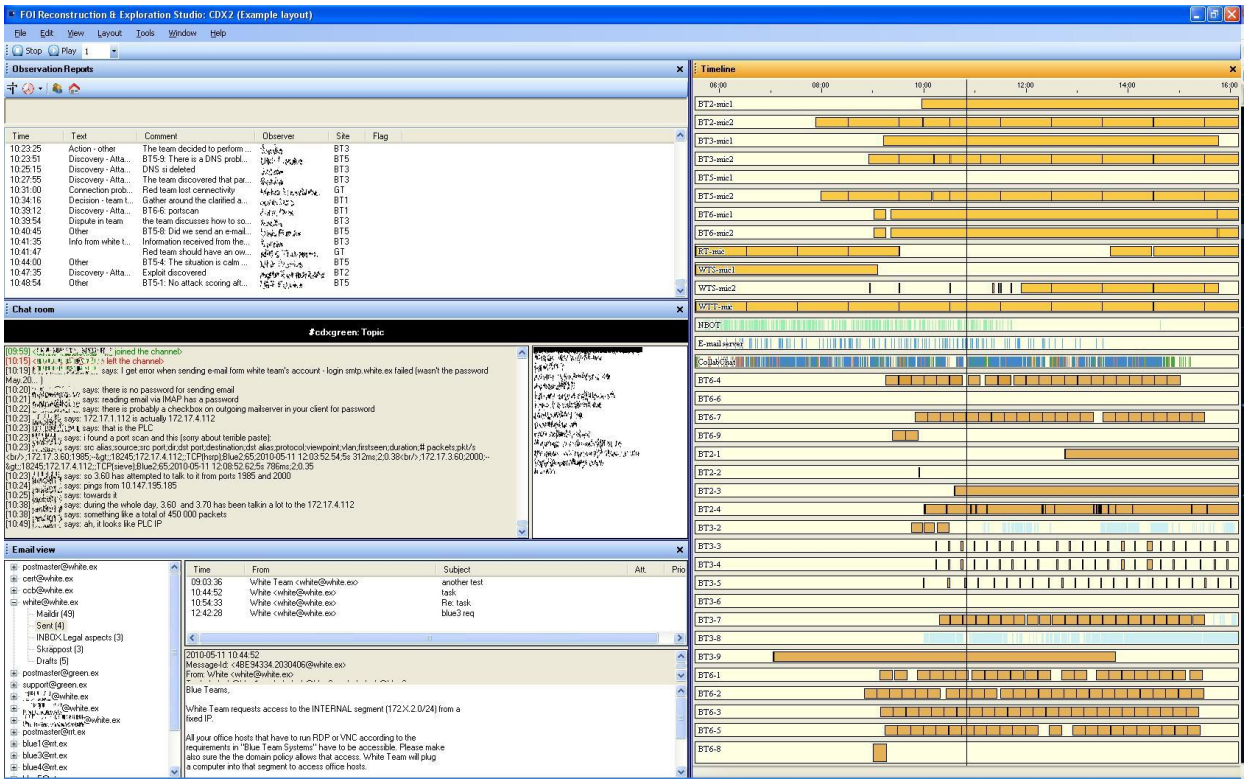


Figure 4. F-REX screenshot showing analysis in the first cycle. The layout shows observer reports, chat room log, e-mail to the left and a timeline of events currently in the mission history, separated by source, to the right. (Note: names are scrambled to preserve anonymity)

The captured data could be imported to an F-REX project, known in R&E as a mission history, for further synchronization, presentation and analysis according to the Exploratory Sequential Data Analysis (ESDA) method [7]. ESDA is an empirical exploratory approach, as opposed to confirmatory, in which the analyst uses temporal ordering of data to try to make sense of a dataset. Sanderson describes ESDA as a family of observational methodologies that are used when the objective is to observe what people do over time. Sanderson & Fisher [8] outlines the 8 C's (fig.5) as the main operations needed in ESDA, the reader is advised to read their article for a thorough explanation of the 8 C's. They do not claim that all of the 8 steps must be performed at every study, nor do they have to be performed in a particular order. However, the way that they present them seems to create a fairly logical work flow that can easily be followed using F-REX and the exploration part of R&E.

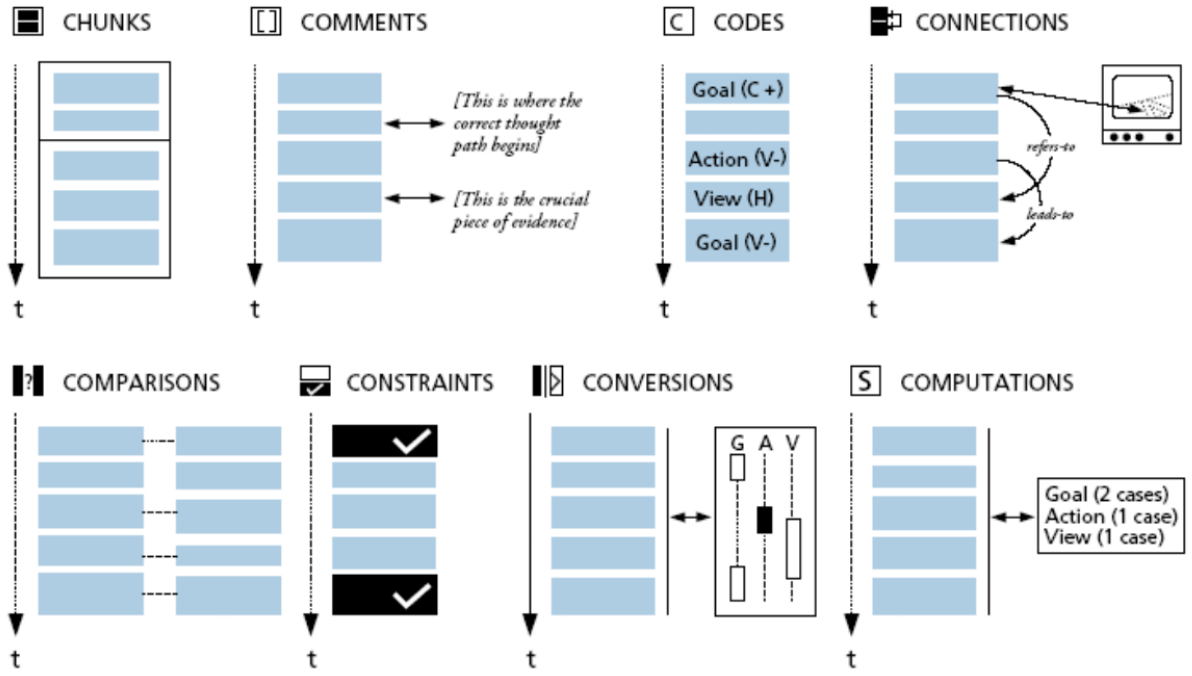


Figure 5. 8C's [7]

In R&E, the exploration phase is cyclic, with analysis results and presentation comments being fed back into the model to create revised mission histories. In this study, the first reconstruction cycle used only chat logs, e-mail communication and observer reports - simply because they were estimated to generate the most value for least effort into the analysis. It is easy to assume that neglecting a large portion of the data set as this will impact results. This is, however, merely a case of "data guilt" as Fisher & Sanderson so accurately defines "unless there is a formal commitment to analyzing all the data to meet sampling assumptions, it may not be necessary. Thoroughly analyzing a subset of the data may be more informative". [2]

Results

A CDX differs from the type of operations that are typically analyzed by the team in the sense that almost all data is in the virtual domain, and there is little real action to observe and analyze in the physical world. As such, the R&E approach had much to prove. Setting up the data capture was indeed a journey into uncharted waters as, to the authors' knowledge, this type of comprehensive data capture had never before been tried in a CDX.

Since most of the action happens in the virtual domain, in a CDX data capture is mostly a matter of running software that log system-system and human-system interactions. It turned out that it is not always easy to capture these interactions in a easily quantifiable format, as many programs, protocols and data formats being used are proprietary. The chosen fallback solution was to capture screen videos, keyboard interactions and network traffic for systems that could not be tapped in to in any other way. This data capture is not optimal because it is very crude and hard to interpret as needed to do the chunks, connections and codes. Still, the work proved possible, although very time consuming. The process became especially cumbersome since some of the blue teams were allowed to use their private laptops, and the data capturing was therefore dependent on their willingness to install and run special software and scripts to capture these interactions. Getting them to do so proved difficult, probably because of lack

of understanding of the importance of the evaluation process. As a result the data set is missing some interactions that could potentially be vital for the detailed analysis of the work that was going on in these teams.

Apart from the software logs, video cameras and audio recorders were placed in each team to capture human-human interactions. Analysis of these interactions is typically also very time consuming, but resembles more traditional R&E work (and ESDA for that matter). This analysis has yet to be performed, but is essential to answer questions such as how human-human interaction affects the team collaboration or performance in a CDX.

The third type of data capturing that took place during the BCS CDX was surveying. The background survey showed that the teams consisted of highly experienced personnel on both a technical and strategic level, most of which worked with IT security on a daily basis. Having this in mind, the participants perceived scenario complexity and realism as perfectly sufficient and were highly motivated throughout the exercise. Teamwork was experienced as smooth, probably due to that most team members were familiar to each other. In some teams, the members reported lacking technical competencies within fields experienced as crucial, which could be a possible explanation to differences in performance between the teams. Another aspect which was captured using surveys was the participants' prior assumptions regarding the probability of successful compromise of hosts with specific properties.

The first version of the mission history enabled finding an initial classification of the targets for all discovered compromises, as reported by the red and blue teams respectively (Table 1). The table does not yield any strong interpretations, however it hints that the most frequently attacked services during the BCS CDX were the historian, the public web server and the customer portal. The defending teams seem to have reported most of the incidents on the public web servers and the customer portals, while the attacks on the historians would be more likely to have passed undetected.

Table 1. Compromised services as reported by attacking vs defending teams

Service	# reports by attacking team (s_a)	# reports by defending teams (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

Our experience from this work is that ESDA is a very useful complement to R&E when analyzing massive multimedia-heavy datasets such as the one collected during the BCS CDX. While one can argue that any analysis made with the assistance of R&E could be categorized as ESDA, it is the structured way of working through the data set, as outlined by the 8C's, that makes ESDA so powerful. From our experience, the 8C's should be considered as guidelines that help structuring the analysis process.

Conclusion

This study has shown the successful use of R&E and F-REX for analyzing cyber defense exercises (CDXs). In order to perform the actual analysis, Exploratory Sequential Data Analysis was applied in the exploration phase. R&E with ESDA has shown great potential for analyzing CDXs.

It can be argued that any analysis with R&E is automatically ESDA and that would indeed be the case according to the definition of Fisher & Sanderson, since they do not enforce usage of all C's or enforce a certain ordering between the steps. Being aware of ESDA and the 8C's when performing the analysis helps with structuring the analysis and as such ESDA should be regarded as a useful technique to know for R&E analysts.

Capturing human-human interactions in a CDX is not very different from any DTO, although it is reasonable to assume that more of the communication will use digital foras, as opposed to a DTO which typically uses radio as the primary means of communication. A CDX does however, focus more on human-system interactions, which are not always easy to capture. To successfully do so, the analysts must carefully plan their instrumentation. Moreover, it is important to work closely together with the exercise organizers to make sure they understand the need for capturing the necessary data.

For the data collection part it could be concluded that having a observer tool with predefined coding schemas was very helpful for the observers and the analysts, but that the coding schema needs to be tested and verified in advance to avoid having to change schema during the exercise. The observer reports and the different teams' self-reporting via e-mail seem to be the most valuable resources for analyzing the data. From the reports it seems that the historians, the portals and the public web servers were the most frequently attacked targets during the BCS CDX.

References

[1] Andersson, D., "F-REX: Event-Driven Synchronized Multimedia Model Visualization", in *Proceedings of the 15th International Conference on Distributed Multimedia Systems*, September 10-12, 2009, Redwood City, CA, pp. 140-145, Published by Knowledge Systems Institute, ISBN 1-891706-25-25.

[2] Fisher, C. and Sanderson, P. (1996), "Exploratory sequential data analysis: exploring continuous observational data", *Interactions*: Vol. 3 : Iss. 2, pp 25-34, New York, NY, USA.

[3] Geers, K. (2010) "Live Fire Exercise: Preparing for Cyber War", *Journal of Homeland Security and Emergency Management*: Vol. 7 : Iss. 1, Article 74, published by Berkeley Electronic Press.

[4] Greenemeier, L. (2007) "China's Cyber Attacks Signal New Battlefield Is Online", *Scientific American*, September 18, 2007.

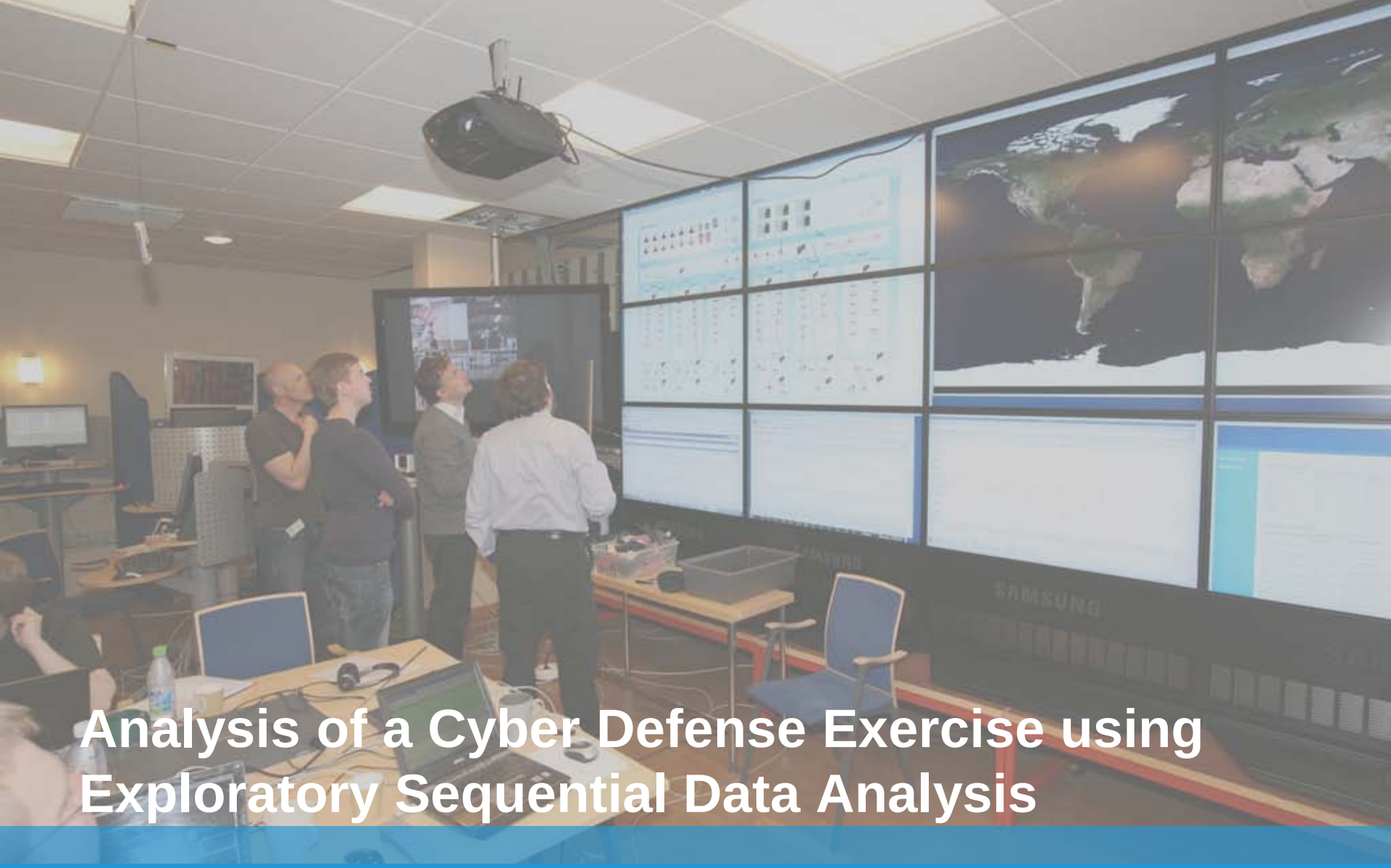
[5] Hammervik, M., Andersson, D. and Hallberg, J. (2010), “Capturing a Cyber Defence Exercise”, (extended abstract), In *Proceedings of the 1st National symposium on Technology and Methodology for Security and Crisis Management*, pp 30, Linköping, Sweden, October 27-28, 2010. (Note: Hammervik, M. is now publishing under Granåsen, M.)

[6] Pilemalm, S., Andersson, D., and Hallberg, N. (2008) “Reconstruction and exploration of large-scale distributed operations—Multimedia tools for evaluation of emergency management response”, *Journal of Emergency Management*, Vol. 6, No. 4, July/August, pp. 31-47.

[7] Sanderson, P. (1991), “Exploratory sequential data analysis”, Engineering Psychology Research Laboratory Technical Report EPRL-91-04, Department of Mechanical and Industrial Engineering, University of Illinois at Urbana-Champaign, Urbana, IL.

[8] Sanderson, P. and Fisher, C. (1994), “Exploratory Sequential Data-Analysis: Foundations”, *Human-computer interaction*: vol:9 iss:3-4 pp:251-317, published by Taylor & Francis.

[9] Thorstensson, M. (2008) *Using Observers for Model Based Data Collection in Distributed Tactical Operations*, Linköping Studies in Science and Technology, Thesis No. 1386, Linköping, Sweden, Linköpings Universitet.



Analysis of a Cyber Defense Exercise using Exploratory Sequential Data Analysis

Dennis Andersson
Magdalena Granåsen
Jonas Hallberg

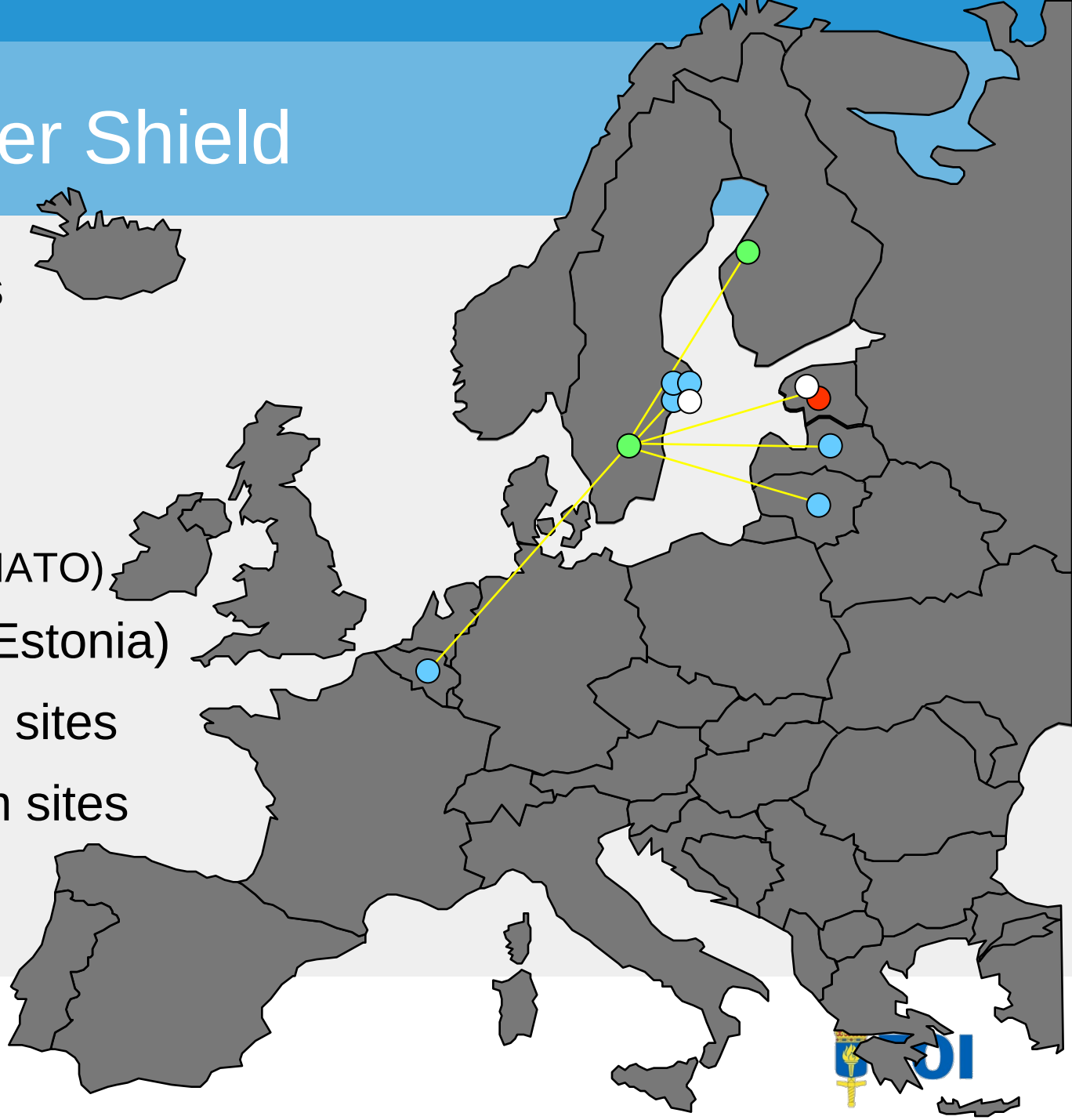
FOI

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

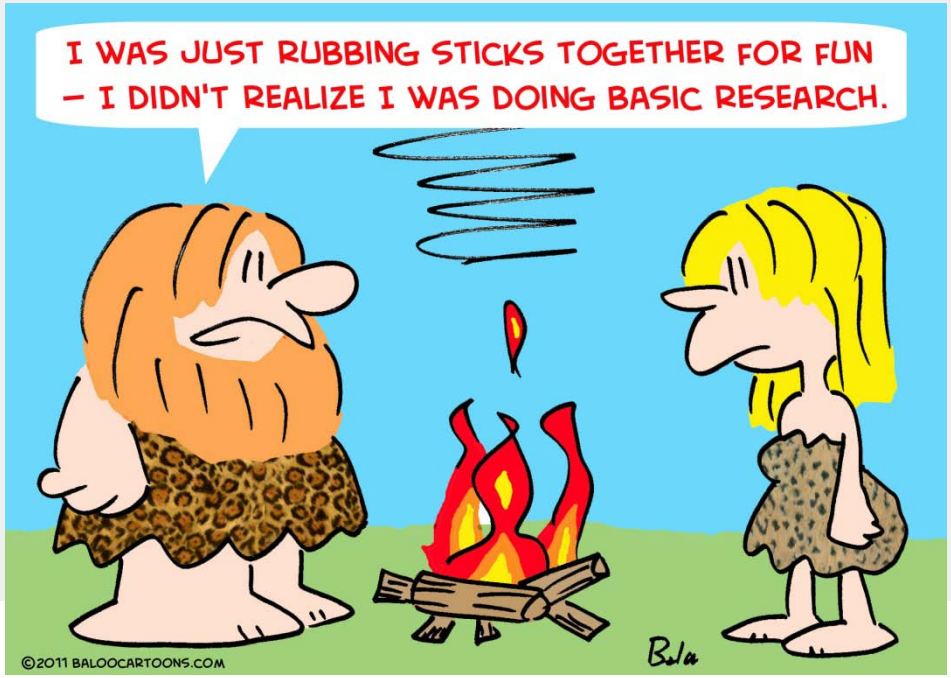


Baltic Cyber Shield

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

Objectives

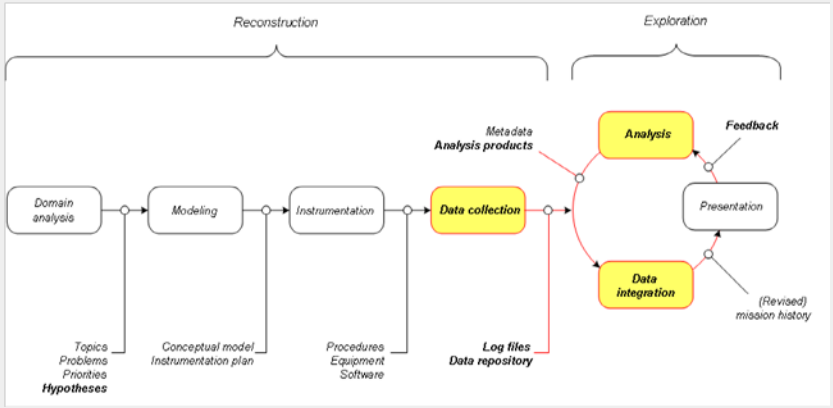
- Training aspect
  - Improve capability of conducting technical IT security exercises
- Scholarly aspect
  - Investigate how to study IT attacks and defence of critical infrastructure

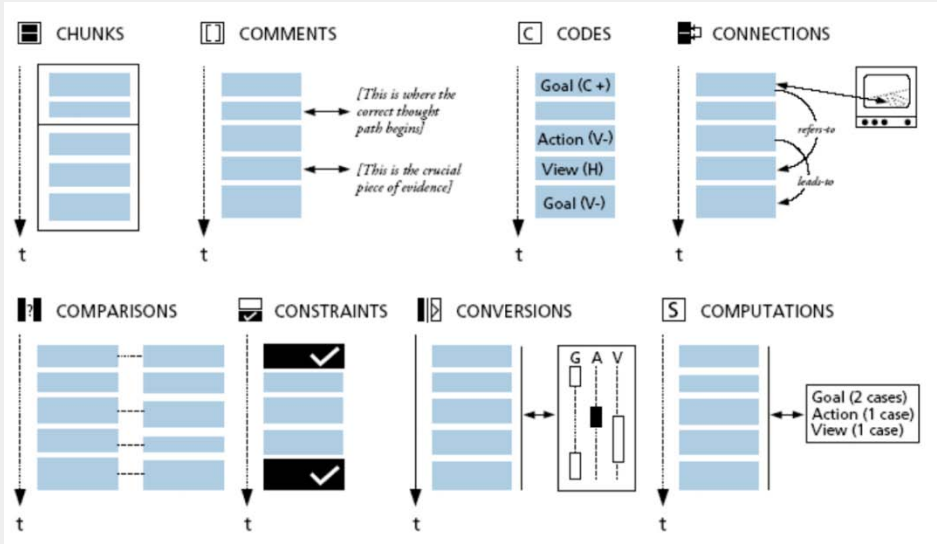


Used with permission from artist [Rex May]

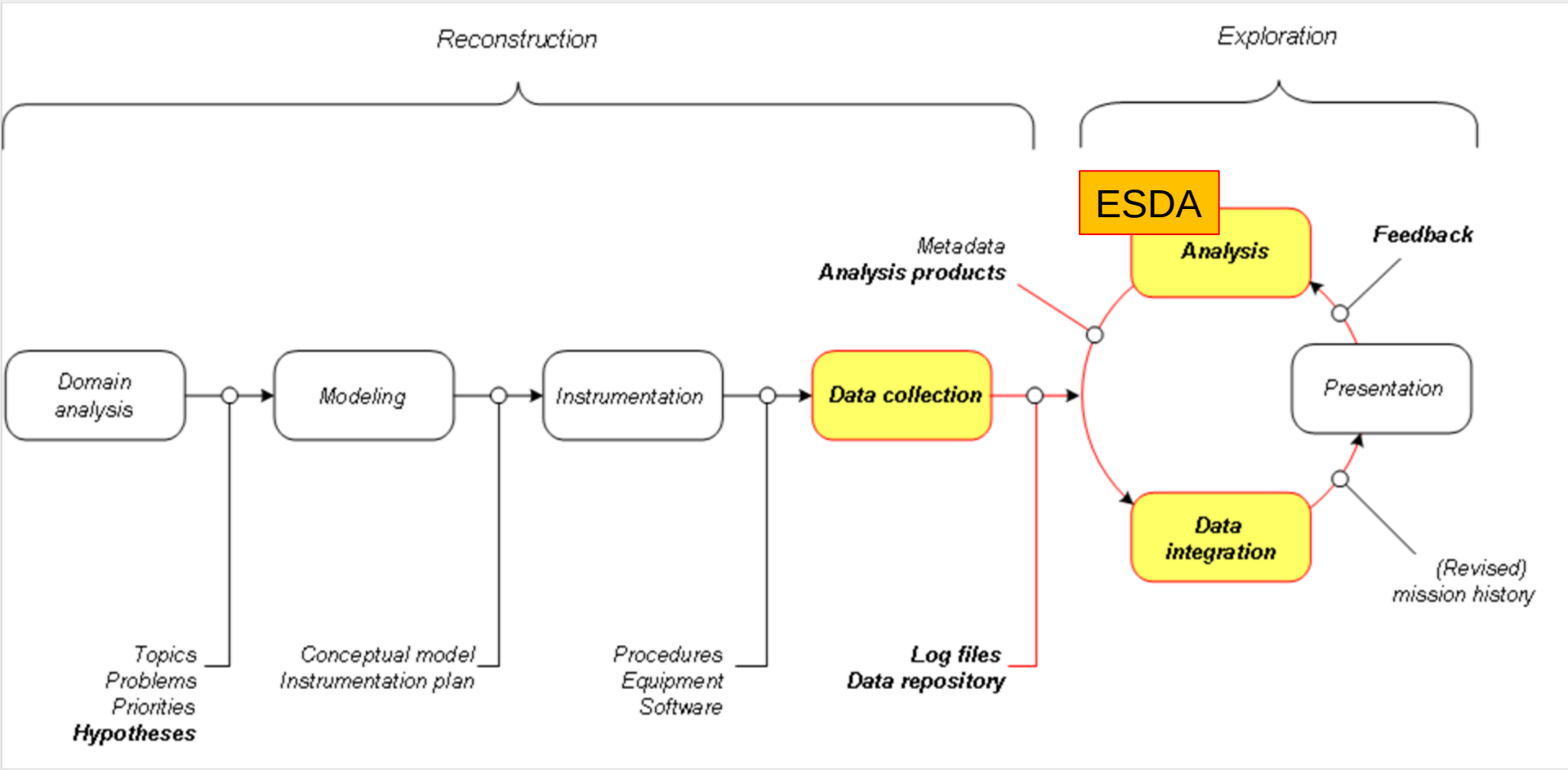
Scholarly aspect

- 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?

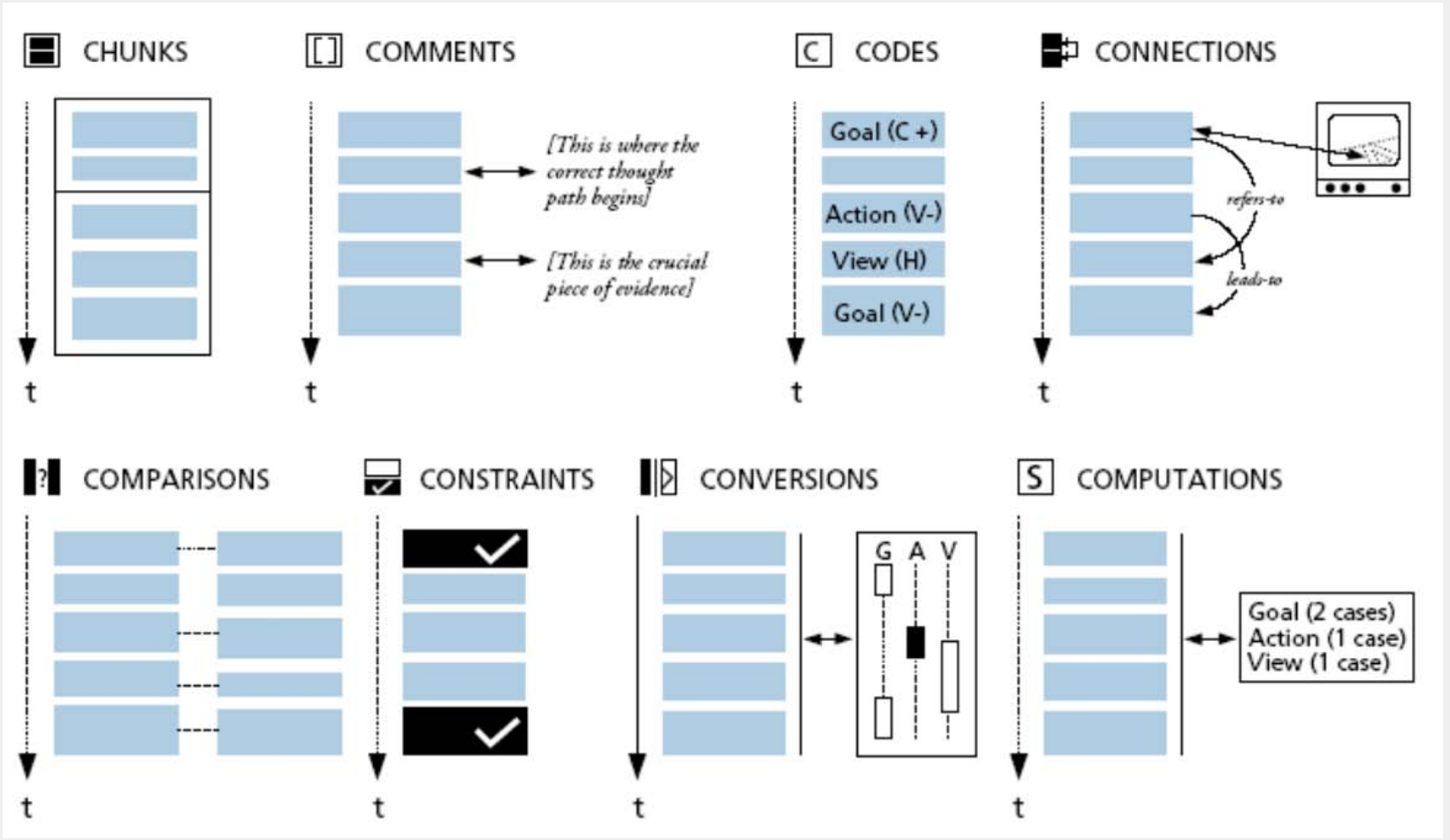




Reconstruction & Exploration

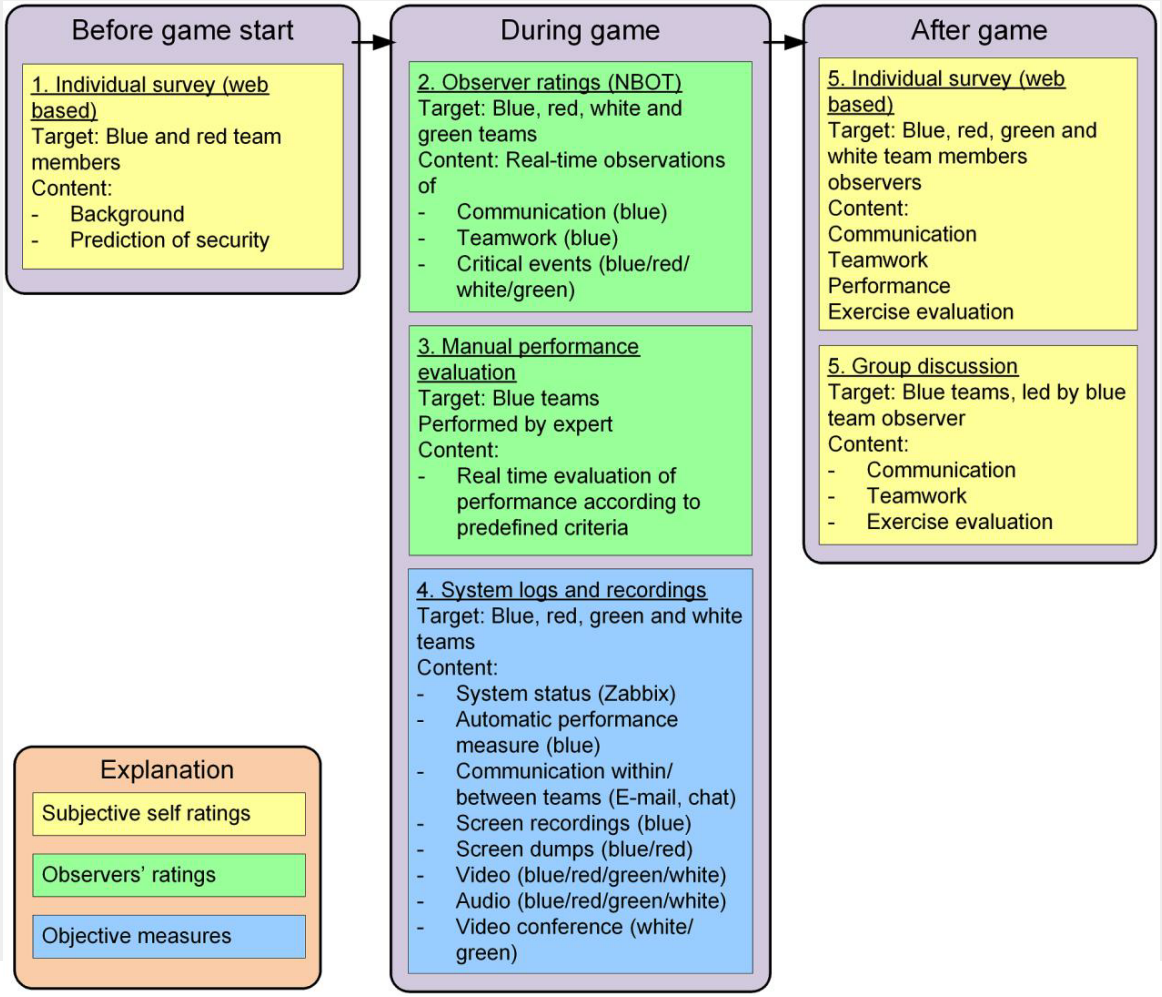


Exploratory Sequential Data Analysis



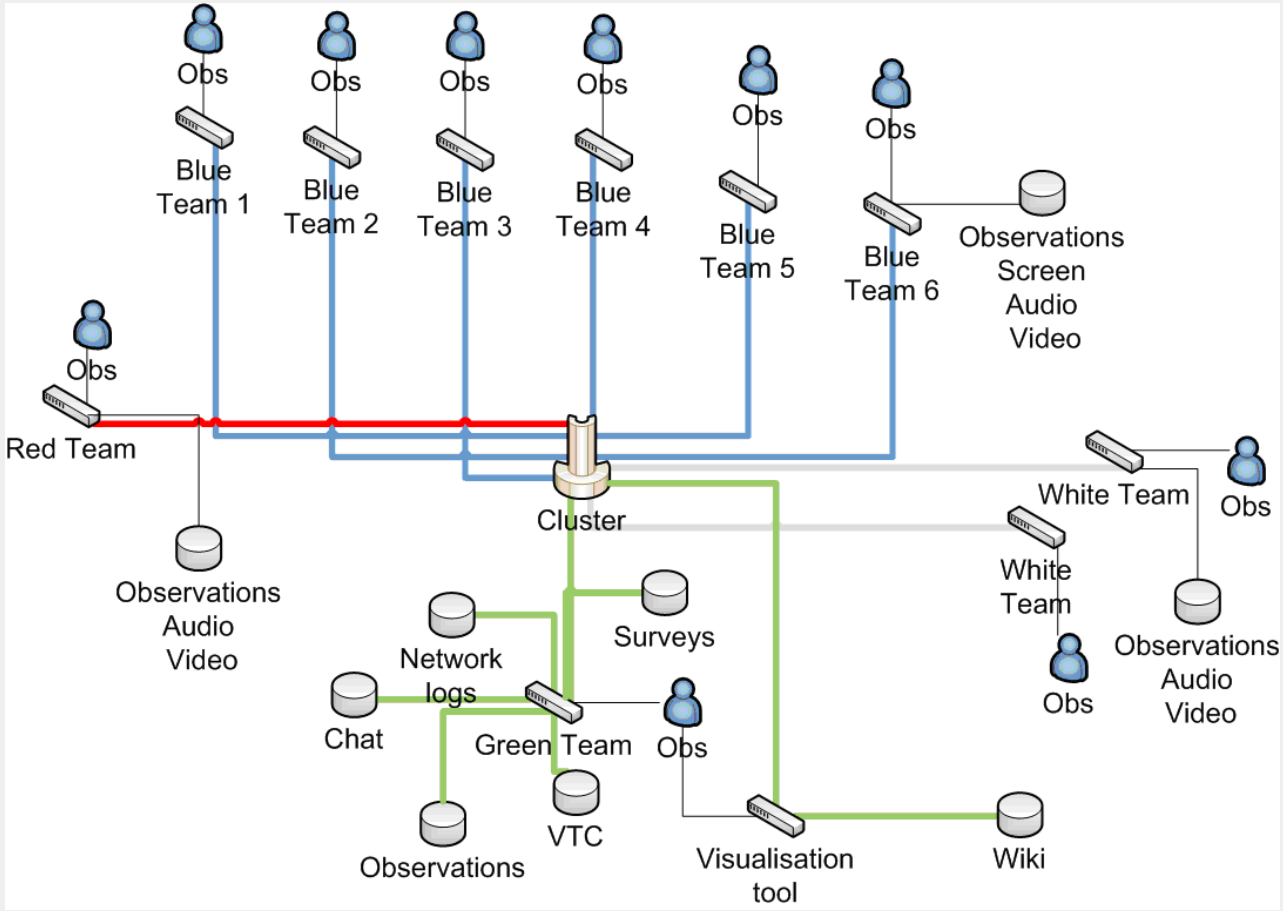
Conceptual model

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

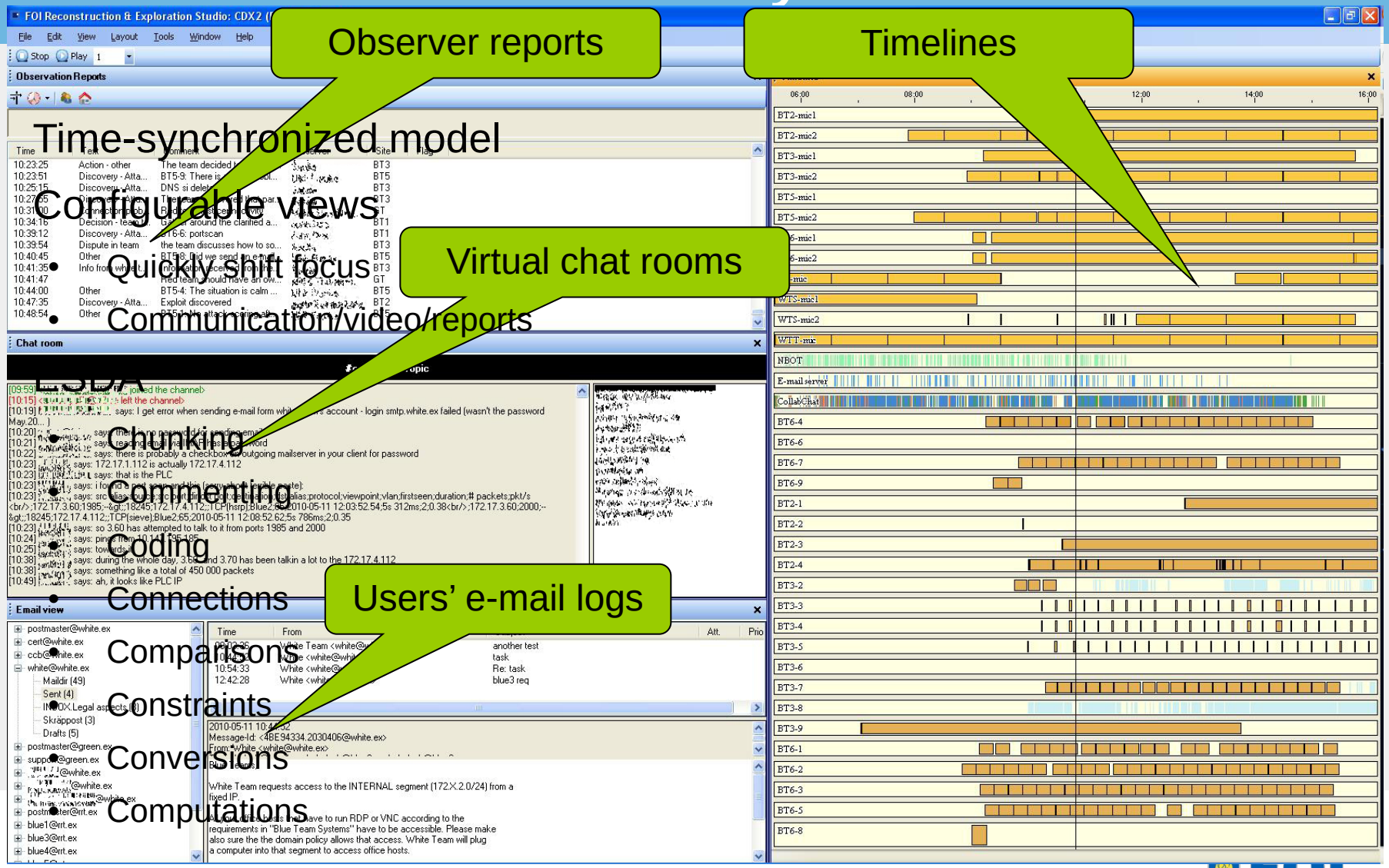


Instrumentation plan

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



Presentation and analysis with F-REX



- Time-synchronized model
- Configurable views
  - Quickly shift focus
  - Communication/video/reports
- TESDA
  - Chunking
  - Coding
  - Connections
  - Comparisons
  - Constraints
  - Conversions
  - 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!