Cyber Terror Exercise

C Y T E X

Attack on Critical Infrastructrues

12-14 November 2001 at IABG

Objectives

- Development and Evaluation of Scenario
- Sensitizing for Risks, Vulnerabilities, Damage Potential
- Testing of Protection & Reaction Strategies
- Evaluation of Communications and Messaging
- Evaluation of the Complex Interdependencies Between Critical Infrastructures
- Exercising of Tasks and Roles of Individuals and Organisations
- Development of Measures and Recommendations
- Information to the Public/Media

Characteristics

- First Time in Germany
- Interdisciplinary
- Tool Based / Network Based
- Concentration on IT-Attacks
- Realistic Scenario
- Good Professional Support
- Media Attention

Scenario Framework

- Economo-Political Situation in 200x
- Militant Anti-Globalization Organization
- Well concerted Attack on All Major Infrastructures in the Berlin Area
- Attacker Objectives
  - Massive Breakdown of the Public Life
  - Blackmailing of the German Government
  - Release of Captive Terrorist Colleagues
  - Publication of a Manifesto
  - Minimizing of Own Risks

The Scenario

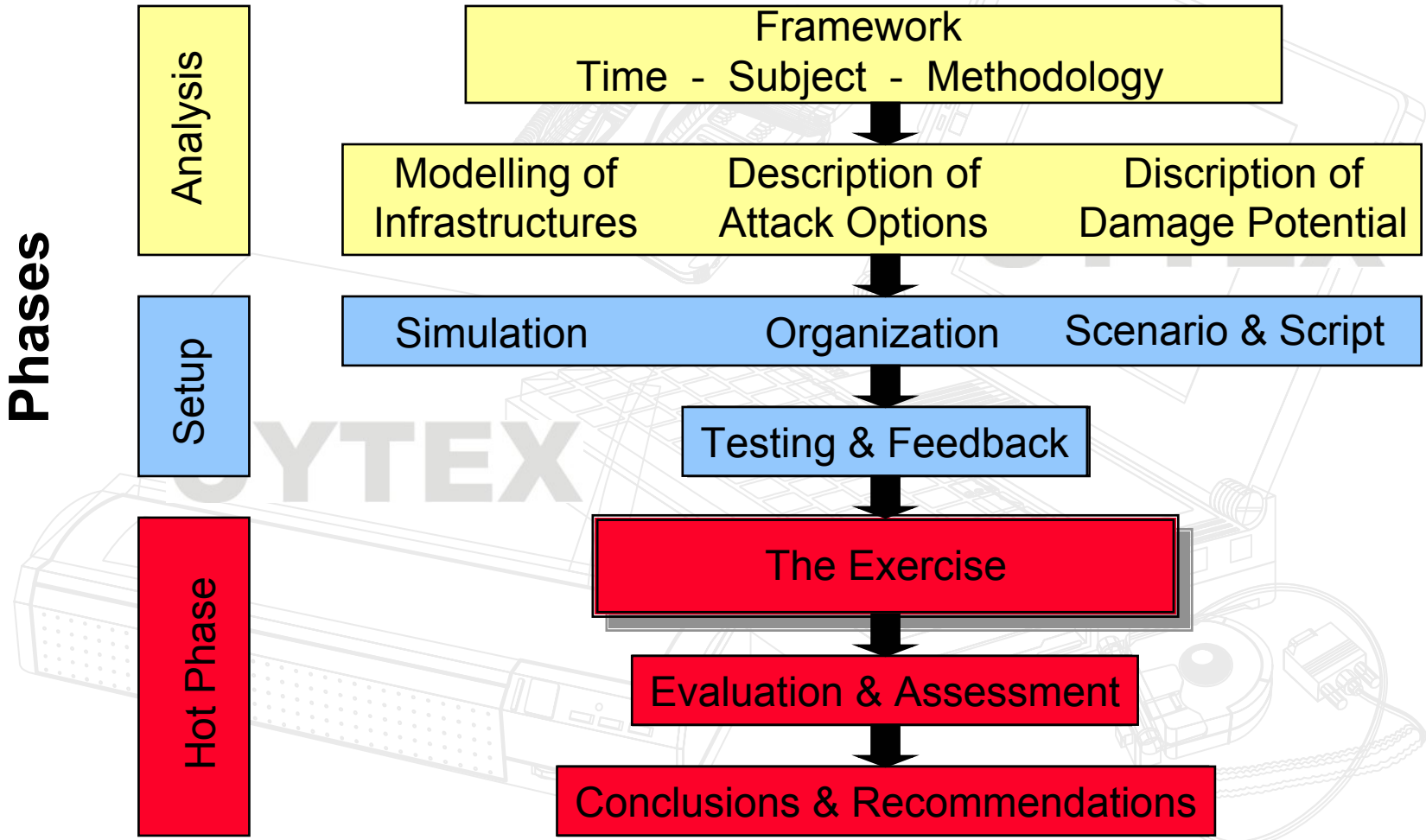
28.01.200x	The German Federal Government will host G8 Summit
21.01	Manifesto Appears on BMI Homepage
22.01	Government Assesses Intelligence and Establishes Task Force
23.01	Top Level Crisis Meeting with Bundeskanzler
24.01	Government Press Conference
24.-28.01	Massive Replanning of Security Forces
28.01	08:00 Start of co-ordinated and well timed IT-Attacks on

- The Telecommunications Network
- The IT-Infrastructure of the Largest Bank
- The Air Traffic Management System
- The Local and Wide Area Railway System
- The Street Traffic Control System
- The Electrical Power Supply System
- The Federal Agency on IT-Security

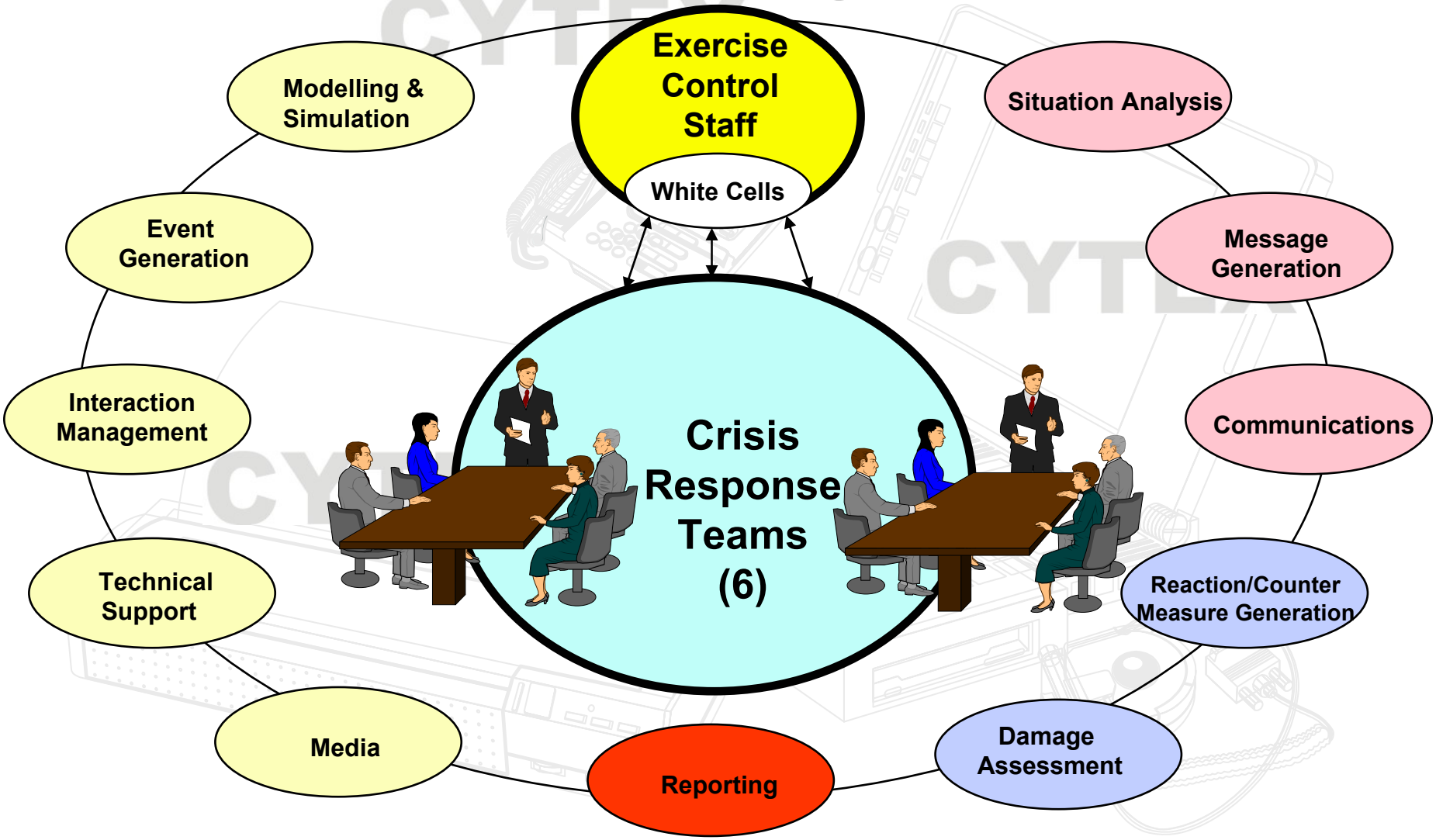
The Attack is a Mixture of

- DoS' and Saturation Attacks
- Virus Attacks
- Electronic Bombs
- Malicious Actions of Internal Personnel
- Manipulation via Maintenance Channels
- Infiltration of False Information
- Psychological Influence Through Media
- Random Events out of Context

Methodology

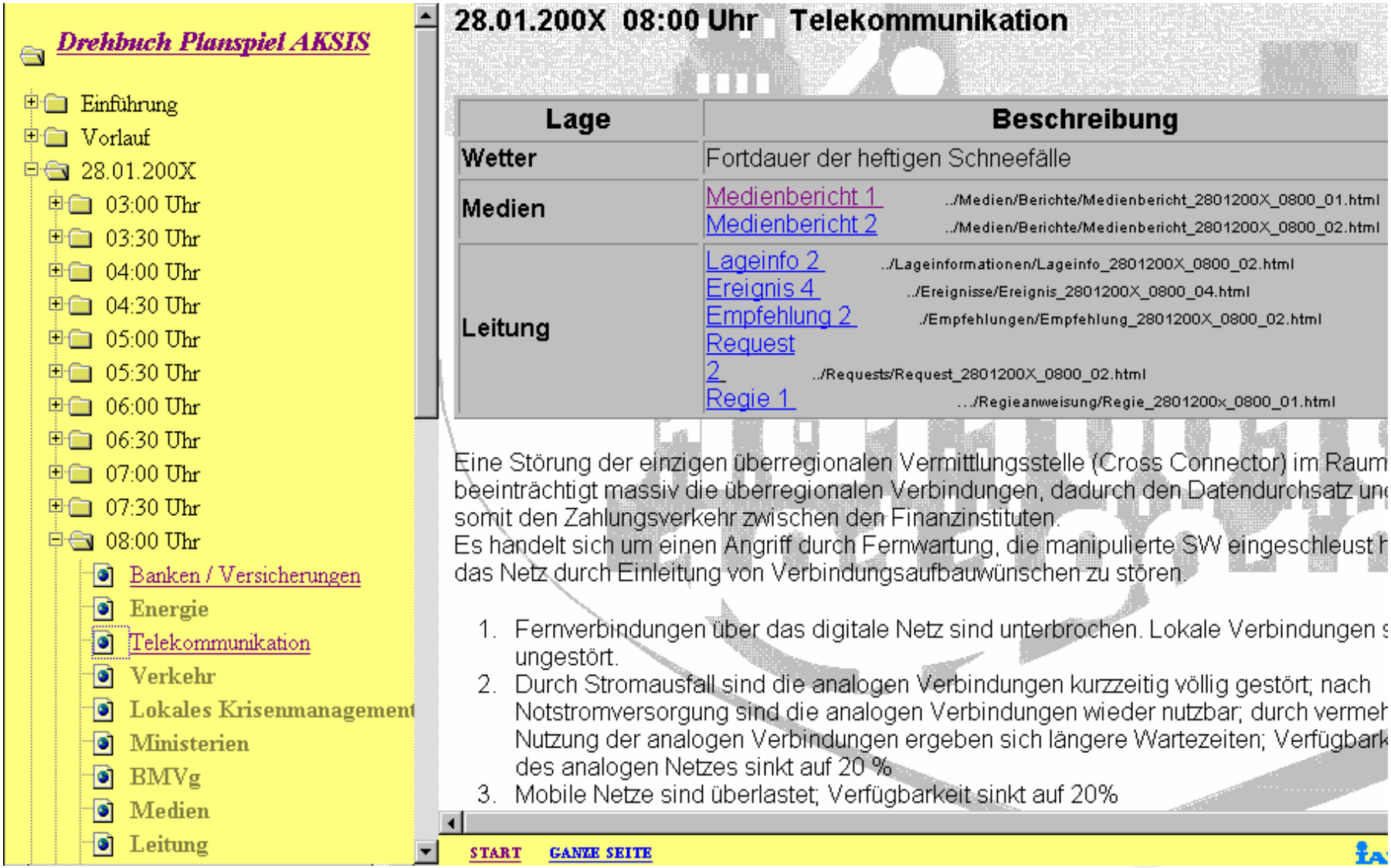


Game Elements and Organisations



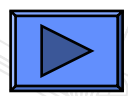
Tools & Products
- DEMOKRIT -
- Demonstration & Modelling of Critical Infrastructures -

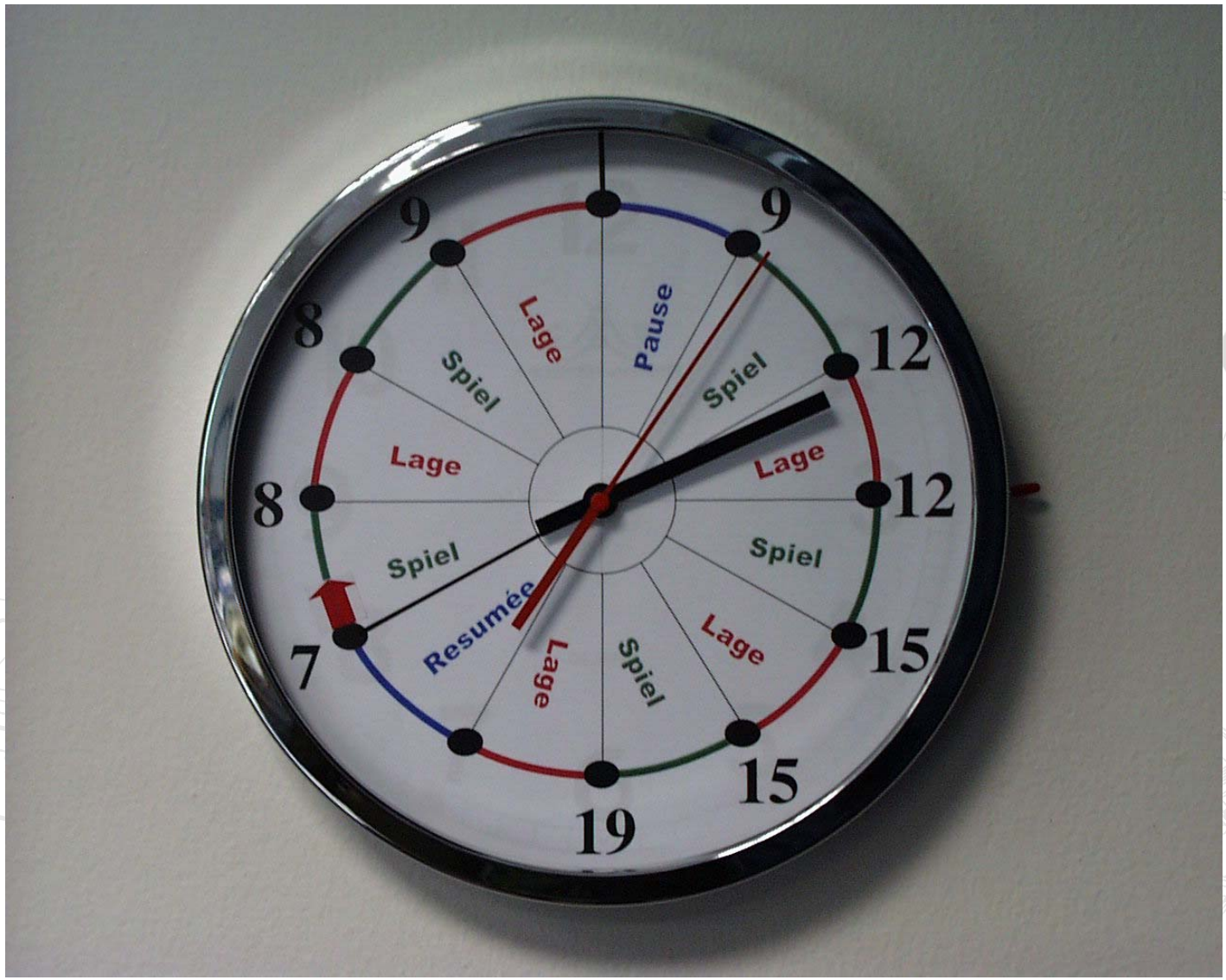
1. Scenario Description
2. Detailed Computerized Script (html)
3. Attack & Damage Matrices
4. Dedicated CYTEX-LAN
5. Support Tools / Time Manager
6. GAMMA Network Models
7. POWERSIM
8. Event Pool
9. Evaluation Methodology
10. Report(s)


Drehbuch Planspiel AKSIS
Einführung
Vorlauf
28.01.200X
03:00 Uhr
03:30 Uhr
04:00 Uhr
04:30 Uhr
05:00 Uhr
05:30 Uhr
06:00 Uhr
06:30 Uhr
07:00 Uhr
07:30 Uhr
08:00 Uhr
Banken / Versicherungen
Energie
Telekommunikation
Verkehr
Lokales Krisenmanagement
Ministerien
BMVg
Medien
Leitung
28.01.200X 08:00 Uhr Telekommunikation
Lage
Beschreibung
Wetter
Fortdauer der heftigen Schneefälle
Medien
Medienbericht 1 ../Medien/Berichte/Medienbericht_2801200X_0800_01.html
Medienbericht 2 ../Medien/Berichte/Medienbericht_2801200X_0800_02.html
Leitung
Lageinfo 2 ../Lageinformationen/Lageinfo_2801200X_0800_02.html
Ereignis 4 ../Ereignisse/Ereignis_2801200X_0800_04.html
Empfehlung 2 ./Empfehlungen/Empfehlung_2801200X_0800_02.html
Request 2 ../Requests/Request_2801200X_0800_02.html
Regie 1 .../Regieanweisung/Regie_2801200x_0800_01.html
Eine Störung der einzigen überregionalen Vermittlungsstelle (Cross Connector) im Raum
beeinträchtigt massiv die überregionalen Verbindungen, dadurch den Datendurchsatz un
somit den Zahlungsverkehr zwischen den Finanzinstituten.
Es handelt sich um einen Angriff durch Fernwartung, die manipulierte SW eingeschleust h
das Netz durch Einleitung von Verbindungsaufbauwünschen zu stören.
1. Fernverbindungen über das digitale Netz sind unterbrochen. Lokale Verbindungen s
ungestört.
2. Durch Stromausfall sind die analogen Verbindungen kurzzeitig völlig gestört; nach
Notstromversorgung sind die analogen Verbindungen wieder nutzbar; durch vermeh
Nutzung der analogen Verbindungen ergeben sich längere Wartezeiten; Verfügbark
des analogen Netzes sinkt auf 20 %
3. Mobile Netze sind überlastet; Verfügbarkeit sinkt auf 20%
START
GANZE SEITE

Tools & Products
- DEMOKRIT -
- Demonstration & Modelling of Critical Infrastructures -

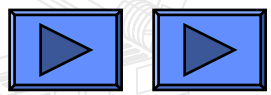
1. Scenario Description
2. Detailed Computerized Script (html)
3. Attack & Damage Matrices
4. Dedicated CYTEX-LAN
5. Support Tools / Time Manager
6. GAMMA Network Models
7. POWERSIM
8. Event Pool
9. Evaluation Methodology
10. Report(s)

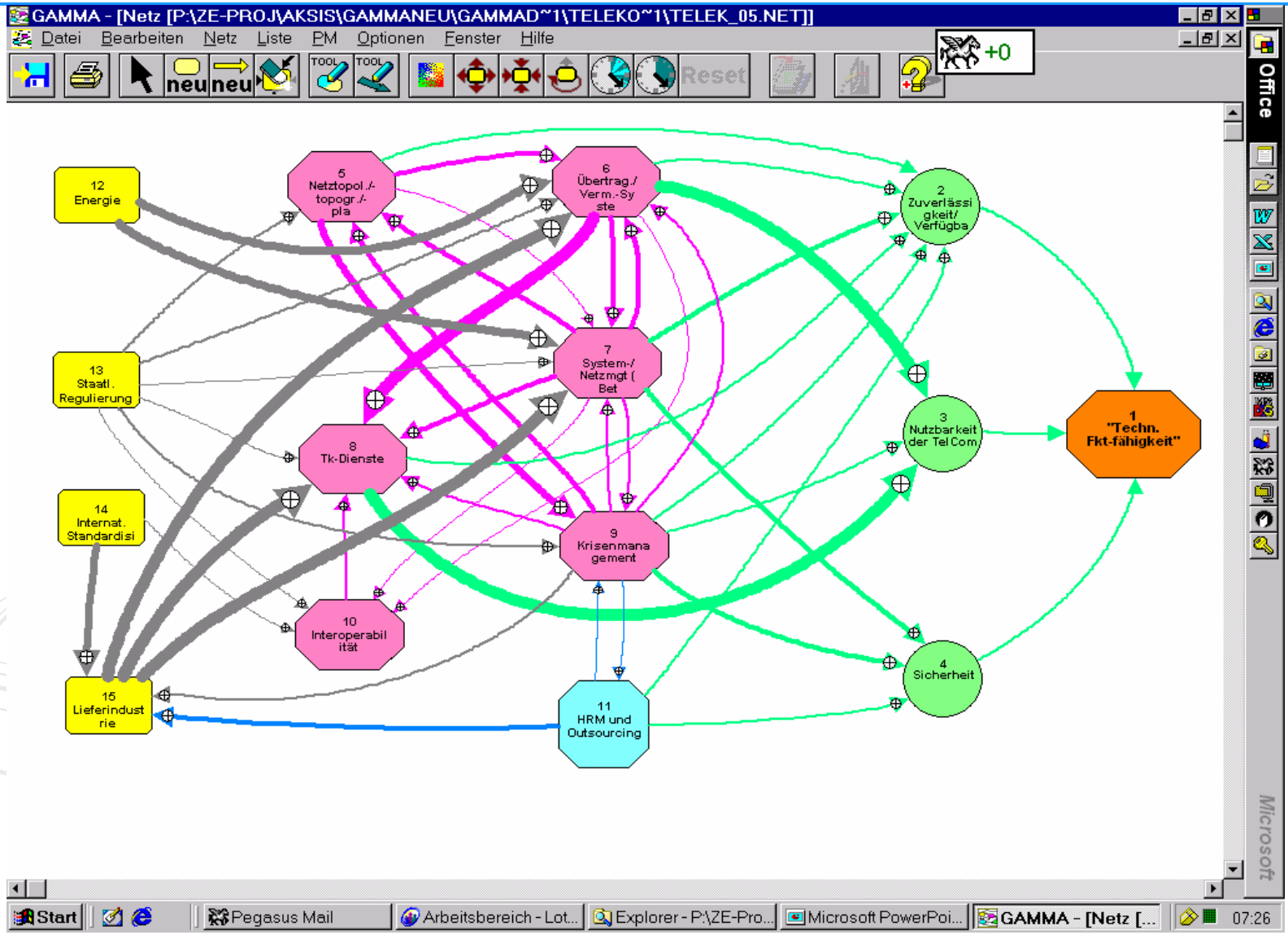


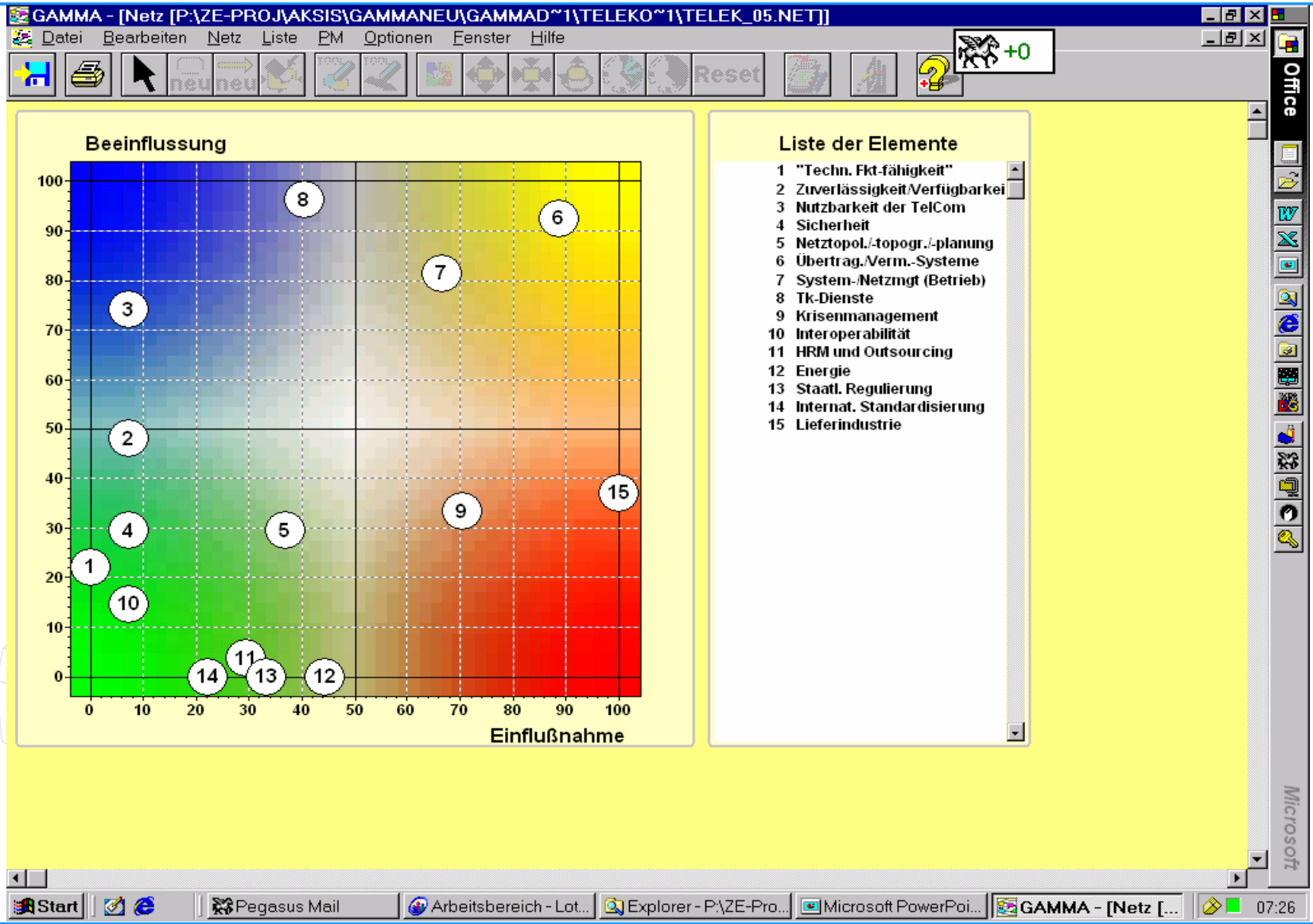

9
8
7
19
15
12
Lage
Pause
Spiel
Lage
Spiel
Lage
Spiel
Lage
Spiel
Resumée
Lage
Spiel
Lage

Tools & Products
- DEMOKRIT -
- Demonstration & Modelling of Critical Infrastructures -

1. Scenario Description
2. Detailed Computerized Script (html)
3. Attack & Damage Matrices
4. Dedicated CYTEX-LAN
5. Support Tools / Time Manager
6. GAMMA Network Models
7. POWERSIM
8. Event Pool
9. Evaluation Methodology
10. Report(s)

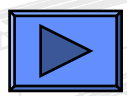


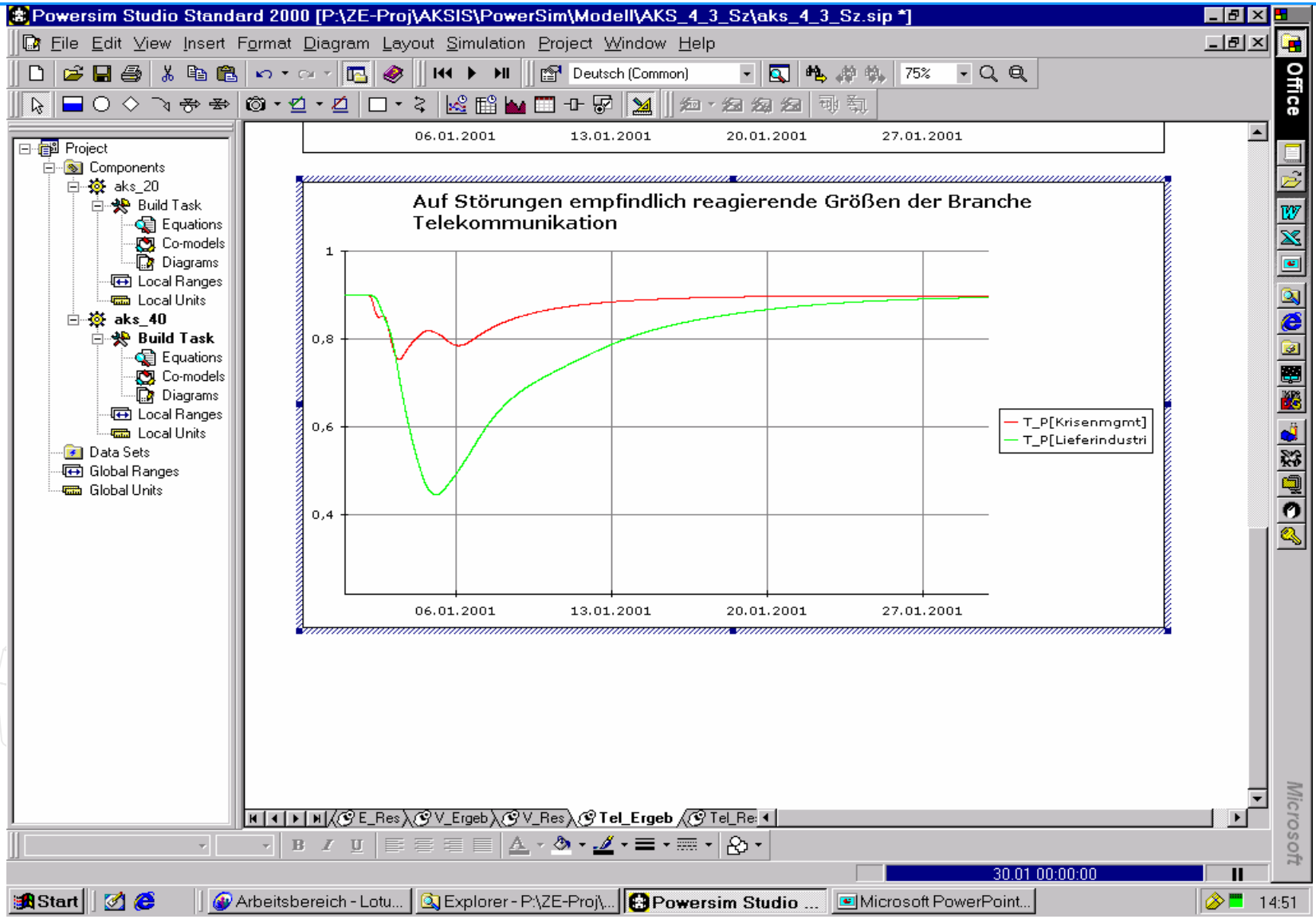

GAMMA - [Netz [P:\ZE-PROJ\AKSIS\GAMMANEU\GAMMAD~1\TELEKO~1\TELEK_05.NET]]
Datei Bearbeiten Netz Liste PM Optionen Fenster Hilfe
+0
12 Energie
5 Netztopol./-topogr./-pla
6 Übertrag./ Verm.-Syste
2 Zuverlässigkeit/ Verfügba
13 Staatl. Regulierung
7 System-/ Netzmgt (Bet
3 Nutzbarkeit der TelCom
1 "Techn. Fkt-fähigkeit"
8 Tk-Dienste
14 Internat. Standardisi
9 Krisenmanagement
10 Interoperabilität
4 Sicherheit
15 Lieferindustrie
11 HRM und Outsourcing
Office
Microsoft
Start
Pegasus Mail
Arbeitsbereich - Lot...
Explorer - P:\ZE-Pro...
Microsoft PowerPoi...
GAMMA - [Netz [...
07:26


GAMMA - [Netz [P:\ZE-PROJ\AKSIS\GAMMANEU\GAMMAD~1\TELEKO~1\TELEK_05.NET]]
Datei Bearbeiten Netz Liste PM Optionen Fenster Hilfe
+0
Beeinflussung
Einflußnahme
Liste der Elemente
1 "Techn. Fkt-fähigkeit"
2 Zuverlässigkeit/Verfügbarkei
3 Nutzbarkeit der TelCom
4 Sicherheit
5 Netztopol./-topogr./-planung
6 Übertrag./Verm.-Systeme
7 System-/Netzmgt (Betrieb)
8 Tk-Dienste
9 Krisenmanagement
10 Interoperabilität
11 HRM und Outsourcing
12 Energie
13 Staatl. Regulierung
14 Internat. Standardisierung
15 Lieferindustrie
Start
Pegasus Mail
Arbeitsbereich - Lot...
Explorer - P:\ZE-Pro...
Microsoft PowerPoi...
GAMMA - [Netz [...
07:26

Tools & Products
- DEMOKRIT -
- Demonstration & Modelling of Critical Infrastructures -

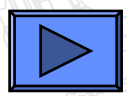
1. Scenario Description
2. Detailed Computerized Script (html)
3. Attack & Damage Matrices
4. Dedicated CYTEX-LAN
5. Support Tools / Time Manager
6. GAMMA Network Models
7. POWERSIM
8. Event Pool
9. Evaluation Methodology
10. Report(s)




Powersim Studio Standard 2000 [P:\ZE-Proj\AKSIS\PowerSim\Modell\AKS_4_3_Sz\aks_4_3_Sz.sip *]
File Edit View Insert Format Diagram Layout Simulation Project Window Help
Deutsch (Common)
75%
Project
Components
aks_20
Build Task
Equations
Co-models
Diagrams
Local Ranges
Local Units
aks_40
Build Task
Equations
Co-models
Diagrams
Local Ranges
Local Units
Data Sets
Global Ranges
Global Units
06.01.2001
13.01.2001
20.01.2001
27.01.2001
Auf Störungen empfindlich reagierende Größen der Branche Telekommunikation
1
0,8
0,6
0,4
T_P[Krisenmgmt]
T_P[Lieferindustri
E_Res
V_Ergeb
V_Res
Tel_Ergeb
Tel_Re:
30.01 00:00:00
Start
Arbeitsbereich - Lotu...
Explorer - P:\ZE-Proj\...
Powersim Studio ...
Microsoft PowerPoint...
14:51
Office
Microsoft

Tools & Products
- DEMOKRIT -
- Demonstration & Modelling of Critical Infrastructures -

1. Scenario Description
2. Detailed Computerized Script (html)
3. Attack & Damage Matrices
4. Dedicated CYTEX-LAN
5. Support Tools / Time Manager
6. GAMMA Network Models
7. POWERSIM
8. Event Pool
9. Evaluation Methodology
10. Report(s)



Preliminary Conclusions

- CYTEX/DEMOKRIT is a powerful Method & Tool for the investigation of the Critical Infrastructure domain
- The Game received high acceptance by and appreciation from the participants
- The Game Results give a very detailed insight into the mutual interdependencies between Critical Infrastructures
- The Availability of appropriate and redundant Telecommunication Systems is most critical

Preliminary Conclusions (cont.)

- The Security Policy and Standards of individual Infrastructure domains differ drastically, therefore
- Co-operation and Management Organizations and Procedures across the various Infrastructures are strongly requested, particularly those between Public Services and the Private/Commerical Sector
- The Scenario was considered realistic - under the Impression of September 11 it could have been even more demanding -

Future R & D

Methodology & Tools

- Up Front Investment Done
- Integration of Further Support Tools (e.g. Maps, Damage Assessment Tools)
- Refinement & Extension of Infrastructure Models
- In Course Simulation
- Distributed Internet Version

Future R & D

Applications

- Tailoring for Specific Infrastructures
- Evaluation of Alternative Scenarios
- Development of Co-operation Strategies
- Evaluation of a Common AWR System
- Raising of Awareness e.g. via:
  - Political Exercises
  - Media Exercises
  - Management Exercises
- Training Exercises

Customers	real	in Acquis.
Federal Ministry of Defense	x	
European Commission	x	
Federal Agency for IT Security	x	
Federal Ministry of Interior	x	
Federal Ministry of Economy	x	
Deutsche Telekom	x	
Infrastructure Providers	x	x
C2-SNR WG on Min.Ess.Def. Infastruct.		x
Federal Acad. for Emergency Plg. and Civil Safety		x
Foreign Office		x
State and Local Administrations		x
Federal Ministry of Transportation		x
Intelligence Services		x
Federal Academy for Security Politics		x