3J4E – JIGSAW, JUMPSTART, JUNCTURE for Exercises

Three ways to enhance your cyber exercise experience

Stefan Ritter
FIRST Conference Berlin / 2015/06/15
National IT-Situation-Center
3J4E - Modules
LUEKEX
- 70 BSI-players (3000, 5+7 DE states, 80 institutions)

Cyber Europe
- 20 BSI-players (25 nations)

Cyber Storm IV
- 40 BSI-players 56h (14 nations)

NATO CC (~29 nations)
## Preparation Participation Matrix

<table>
<thead>
<tr>
<th>Basic</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unidirectional Communication</td>
<td>Multidirectional Communication</td>
<td>Multidimensional Communication</td>
</tr>
<tr>
<td>1 Person</td>
<td>2 – 5 Persons</td>
<td>5 or more persons</td>
</tr>
<tr>
<td>Point of Contact with reply</td>
<td>Contribute to planning conferences</td>
<td>High contribution in top level exercise planning</td>
</tr>
<tr>
<td>Basic adoption of prepared scenario elements</td>
<td>Influence scenario Advanced adoption of prepared scenario elements Own local elements</td>
<td>Make scenario decisions Develop complete storyline Create own objectives</td>
</tr>
</tbody>
</table>
## Playing Participation Matrix

<table>
<thead>
<tr>
<th>Basic</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unidirectional Communication</td>
<td>Multidirectional Communication</td>
<td>Multidimensional Communication</td>
</tr>
<tr>
<td>1 Person</td>
<td>2 – 5 Persons</td>
<td>5 or more persons</td>
</tr>
<tr>
<td>Take part in confcalls</td>
<td>Contribute in confcalls with own ideas</td>
<td>Play with national crisis management team</td>
</tr>
<tr>
<td>Play of basic adoption of prepared scenario elements</td>
<td>Basic incident handling</td>
<td>Leading role in IT Crisis-Management Incident Facilitator</td>
</tr>
<tr>
<td>Receive information</td>
<td>Share information</td>
<td>Detailed technical and situational reports</td>
</tr>
</tbody>
</table>
Multilevel Jigsaw Scenario

AND / OR Key-and-Lock Scenario Elements
Scenario Design

Supporting Basic Scenario

storylines/tracks + consolidation = solution
### Standard Workflow

<table>
<thead>
<tr>
<th>Objectives</th>
<th>&gt;</th>
<th>Expected Player Actions</th>
<th>&gt;</th>
<th>Storyline</th>
<th>&gt;</th>
<th>MSEL</th>
<th>&gt;</th>
<th>Play</th>
</tr>
</thead>
</table>

Scenario Workflow(s)

2015/06/15 National IT-Situation Center and CERT-Bund
## Scenario Workflow(s)

### Standard Workflow

<table>
<thead>
<tr>
<th>Objectives</th>
<th>&gt; Expected Player Actions</th>
<th>&gt; Storyline</th>
<th>&gt; MSEL</th>
<th>&gt; Play</th>
</tr>
</thead>
</table>

### Modified clustered Workflow

<table>
<thead>
<tr>
<th>Objectives + Participation Commitment</th>
<th>&gt; Clustered Expected Player Actions</th>
<th>&gt; Clustered Storyline</th>
<th>&gt; Jigsaw MSEL</th>
<th>&gt; Clustered Play</th>
</tr>
</thead>
</table>
Exercising is story telling...

- Baseline
- Dramaturgy
- Characters
- High and Low Action
- Turning Points

USE IT!
 Costs for High Active Players don't rise significantly. The others can participate from them.
3J4E Modules

JIGSAW

JUMP START

JUNCTURE

2015/06/15 National IT-Situation Center and CERT-Bund
JUMPSTART: Basics

- Observe
- Orient
- Decide
- Act

Pre-Crisis | Detection | Reporting / Alerting | Response | Wrap Up
---|---|---|---|---
STARTEX | ENDEX
Pre-EX | EX-Play | POST-EX (NOT PLAYED!)
JUMPSTART: As Is

STARTEX

ENDEX

Crisis Management Intensity

Pre-Crisis Detection Reporting / Alerting Response Wrap Up

Pre-EX EX-Play POST-EX (NOT PLAYED)

International Play

National Play

Pre-EX

EX-Play

POST-EX (NOT PLAYED)
JUMPSTART: Enhancement

- Pre-Crisis
- Detection
- Reporting / Alerting
- Response
- Wrap Up
- Pre-EX
- EX-Play
- POST-EX

Crisis Management Intensity

JUMP START

International Play

National Play

ENDEX

2015/06/15 National IT-Situation Center and CERT-Bund
JUMPSTART: Timeline Compression
3J4E - Modules

- JIGSAW
- JUMP
- START
- JUNCTURE
„Why should I participate?“
„What is my benefit?“
„Too technical“
„My focus is political“
„Too much details“
„Not my management level“
„Sorry, I don‘t understand“
„I feel misunderstood“
„You don‘t understand my strategy“
JUNCTURE: Enhancement

Focus on:

- Strategic level information needs
- Decision Support
- Decision Making
- Aggregated Events
- Singular Events
- (physical) CONSEQUENCES
Slightly modified information on Singularity Event

Highly diversified single event information and information on Singularity Event

National IT-Situation Center and CERT-Bund

2015/06/15
JUNCTURE: HowTo (Aggregation)

Compressed and highly aggregated situational information

Highly diversified single event information.
3J4E: Conclusion

- 3J4E is an inspiration
  - expectation management of players
  - jigsaw story-telling
    - key + lock scenario
  - play different parts of incident timeline
  - involve management adequately

- first experiences successful
  - do not think too complicated

- try it!
Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

National IT-Situation Centre and CERT-Bund
Godesberger-Allee 185 - 189
53175 Bonn

Tel: +49 (0)22899-9582-5110
Fax: +49 (0)22899-10-9582-5110
lagezentrum@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de