MODERN SOCIAL NETWORKS EMERGING CYBER THREATS IDENTIFICATION

(A PRACTICAL METHODOLOGICAL FRAMEWORK WITH EXAMPLES)

Zlatogor Minchev & Suzan Feimova

Institute of ICT, Bulgarian Academy of Sciences
IT for Security Department, JTSAC

24 March, 2014 6th AFCEA Student Conference Bucharest, Romania
MODERN SOCIAL NETWORKS COMPLEXITY

METHODODOLOGICAL FRAMEWORK

Believes

Brainstorming, discussions, q-based surveys

Present situation

Alternative future 1

Morphological Analysis

System Analysis

Validated Believes

Alternative future n

Scenario 1

Scenario k

Results Assessment

Validation

Multicriteria & BSC Analysis

Interactive agent based simulation with environment & users monitoring
250 studied users’ selected results

**Most Used Social Networks via Smart Devices:**
- Facebook: 90%
- LinkedIn: 30%
- Google+: 20%
- YouTube: 15%

**Type of Information Exchanged via Smart Devices:**
- Documents: 10%
- Multimedia: 20%
- Text Messages: 70%
- Other: 5%

**Activities for Using Smart Devices:**
- Entertainment: 30%
- Household Support: 20%
- Everyday Work: 10%
- Communications: 90%

**Context Definition**

**Threats**

**Ranking**
- Level 1
- Level 2
- Level 3
- Level 5
- Level 6
- Level 7
- Level n

**Contextualization**

- **Scenario 1**
  - Driving Factors 1

- **Scenario 2**
  - Driving Factors 2
  - Driving Factors k

- **Scenario 3**
  - Driving Factors 3
  - Driving Factors k
**Plausible Scenarios Set**

*Morphological Analysis*

<table>
<thead>
<tr>
<th>Users</th>
<th>Goods/Networks</th>
<th>Hardware Technologies</th>
<th>Communications</th>
<th>Software Platforms</th>
<th>Web standards</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Students</td>
<td>Students</td>
<td>Popular Mobile</td>
<td>Devices</td>
<td>Wireless</td>
<td>Mobile OS</td>
<td>Web 3.0</td>
</tr>
<tr>
<td>Workers</td>
<td>Designer</td>
<td>Planning</td>
<td>Office</td>
<td>Meetings</td>
<td>Travel</td>
<td>Training</td>
</tr>
<tr>
<td>Other</td>
<td>Professional</td>
<td>Consulting</td>
<td>Law</td>
<td>Engineering</td>
<td>Research</td>
<td>Development</td>
</tr>
</tbody>
</table>

*N = 2016 scenario combinations*

**Experimental Monitoring**

**Validation**

**Quantitative Assessment**
ACKNOWLEDGEMENTS

The authors express a special gratitude for the financial support to: A Study on IT Threats and Users’ Behaviour Dynamics in Online Social Networks, DMU03/22, Bulgarian Science Fund, Young Scientists Grant, 2011-2014, www.snfactor.com.


CONTACT US

Institute of ICT, Bulgarian Academy of Sciences
IT for Security Department, Joint Training Simulation & Analysis Center
Sofia 1113, Acad. Georgi Bonchev Str., Bl. 25A, Room 116
E-mails: zlatogor@bas.bg, coeoa@bas.bg