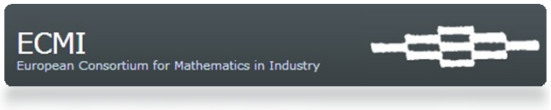
CYBER THREATS OPTIMIZATION FOR E-GOVERNMENT SERVICES

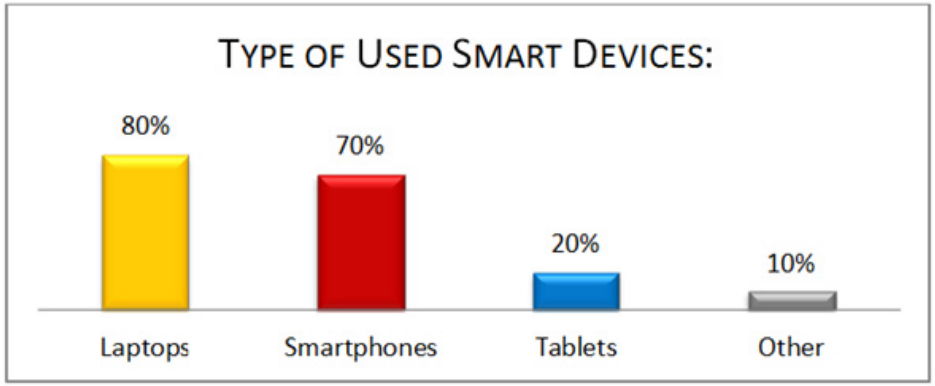
V. Politov, Z. Minchev, P. Crotti, D. Boyadzhiev,
M. Bojkova and P. Mateev

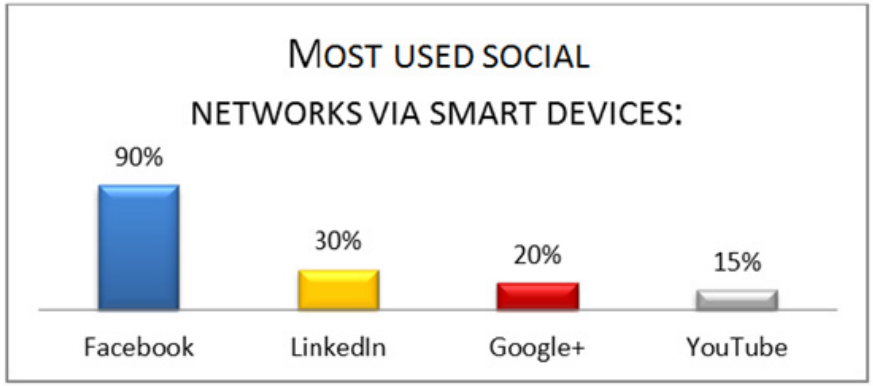
Final Report



SOFIA, BULGARIA European Study Group with Industry'104 SEPTEMBER 27, 2014

Potential sources of cyberthreats go smart & Future quite uncertain...





Threats

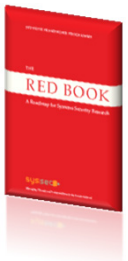
- Malware
- Targeted Attacks
- Social Engineering - Phishing

Areas

- Mobile Devices
- Social Networks
- Critical Infrastructures

Challenges

- No Device Should Be Compromisable
- Give Users Control Over Their Data
- Provide Private Moments in Public Places
- Develop Compromise-Tolerant Systems



...critical services; changing cyber security nature..
...we educate for the unknown...

MULTICRITERIA EXPERTS' ASSESSMENT EXAMPLES*

SOCIAL NETWORKS CYBER THREATS MULTICRITERIA ASSESSMENT

Threat/Area	Human Factor	Digital Society	Governance	Economy	New Technologies	Environment of Living
Social Engineering						
Malware						
Spam & Scam						
Multimedia Influences						
Espionage & Privacy						

SMART HOMES CYBER THREATS MULTICRITERIA ASSESSMENT

Threat/Area	Human Factor	Digital Society	Governance	Economy	New Technologies	Environment of Living
Targeted Attacks						
Compromised Devices						
Malware						
Technologies Influences						
Privacy & Allianation						

Risk levels for Web 2.0/Web3.0 Technological Progress Stage Assessments:

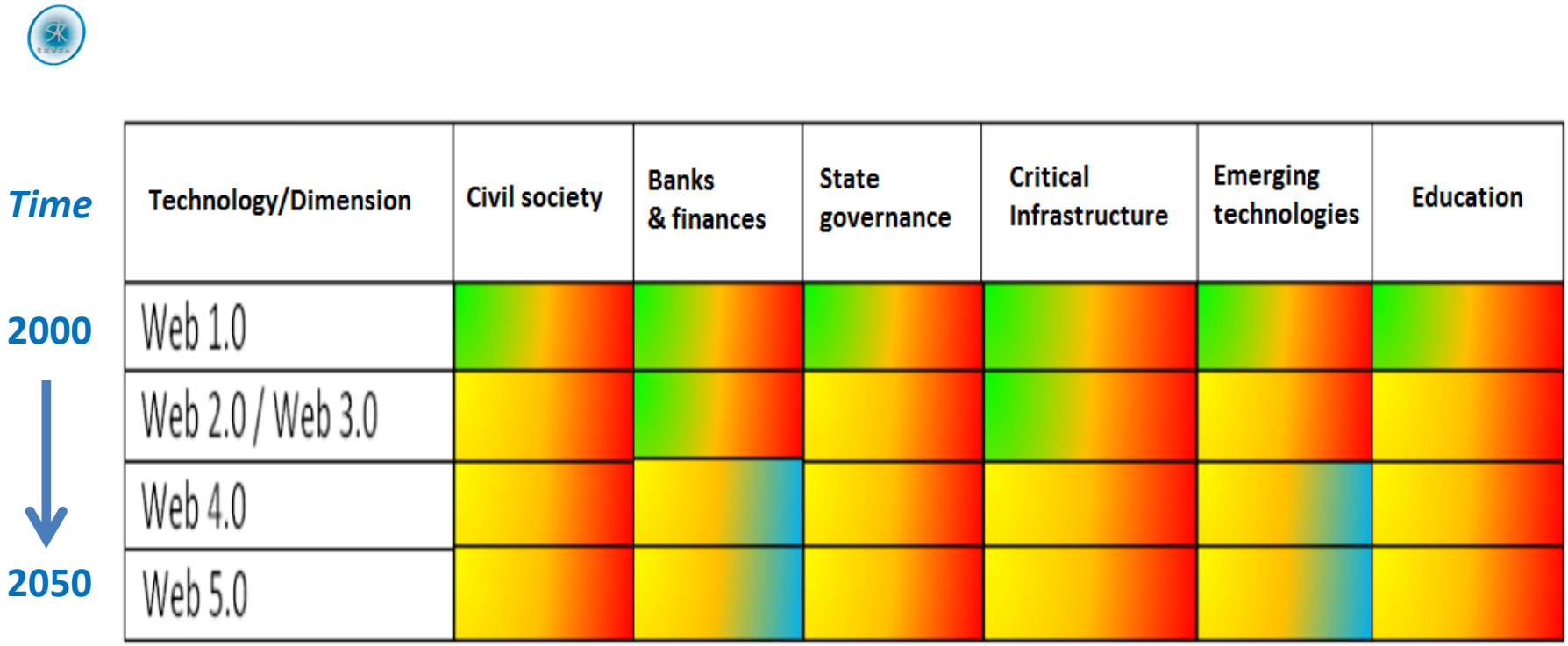
2, High

3, Severe

1, Uncertain

*THE CLASSIFICATION RESULTS ARE GATHERED FROM 75 NATIONAL & INTERNATIONAL EXPERTS' BRAINSTORMING MEETING DISCUSSIONS IN THE FRAMEWORK OF DMU 03/22, DFNI T01/4 ACTIVE COLLABORATION WITH JTSAC IN 2014.

Cyber Threats Multiple Risks Prognosis*



Risk levels:

- 5, Weak
- 4, Moderate
- 3, Severe
- 2, High
- 1, Uncertain

* The classification results are gathered from 250 national & international experts in the framework of Bulgarian Cyber security Strategy Draft preparation from JTSAC for Ministry of Defence in 2013.

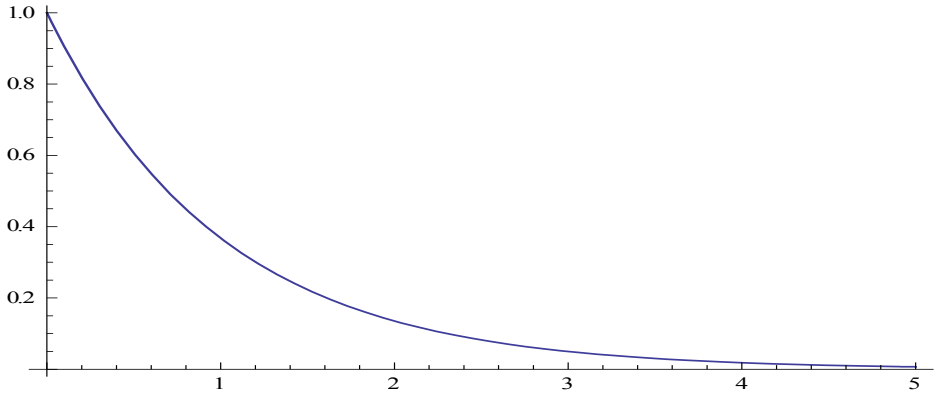
Math Model Description

Let two matrices *P* and *C* are given:

P [p_{ij}] – probabilities,
that at period “i” there is threat “j”.

C [c_{ij}] – damage of attack
“j” at the period “i”.

Our idea



We introduce function q(x)

(for example e^{-x} or $\frac{1}{1+x}$) to describe the investment of *x* money to avoid the threat. (more money we pay – less effective is the threat).

x_{ij} - cost to prevent attack “j” at time period “i” with minimum value ε (ε = 0.2).

$$x_{ij} \geq \varepsilon$$

Upper bound for the total cost for all periods:

$$\sum_{i,j} x_{ij} \leq \text{ M}$$

Objective function (nonlinear):
minimize the global loss of attacks:

$$\sum_{i,j} c_{ij}\, p_{ij}\, q(x_{ij})$$

Nonlinear objective function
with linear constrains,
but based on interaction
with users (experts)
for matrices P and C data

We have made some experiments
with sample data
(very artificially chosen)
using MS EXCEL.

We refine the model by including the costs of repairing the damages.

Similarly, we introduce function r(u), like q(x), to describe the investment of *u* money to decrease the costs of repairing (more money we pay for insurance – less costly is the damage).

Now:

x_{ij} - cost to prevent attack “j” at time period “i”,
u_{ij} - money for insurance to repair effect of attack “j” at time period “i”.

We divide money in two parts – for prevention X and for repairing U: M = X+U (for example U=M/3)
Upper bound for the total cost for all periods:
$\sum_{i,j} x_{ij} \leq$ X and $\sum_{i,j} u_{ij} \leq$ U

Objective function:

minimize the global loss of attacks:

$$\sum_{i,j} c_{ij}\, p_{ij}\, q(x_{ij}) r(u_{ij}) \rightarrow min$$

Constraints:

$$\sum_{i,j} x_{ij} \leq \mathrm{X},$$

$$\sum_{i,j} u_{ij} \leq \mathrm{U},$$

$x_{ij} \geq \varepsilon$, $u_{ij} \geq 0$ and $x_{ij} \geq u_{ij}$.

PRACTICAL PROBLEM DATA EXAMPLE

Damage cost:	***3***	***50***	***8***	***10***	***20***	***40***
Threat/Area	Human Factor	Digital Society	Governance	Economy	New Technologies	Environment of Living
eGov Portal						
e-Authentication						
e-Authorization						
Supply of electronic docs						
Interoperability Registers						
Unified Informtion Exchange Env.						
Electronic Payments						
Portal for Cyber Security						
Cloud Services						
IS of Administrations						

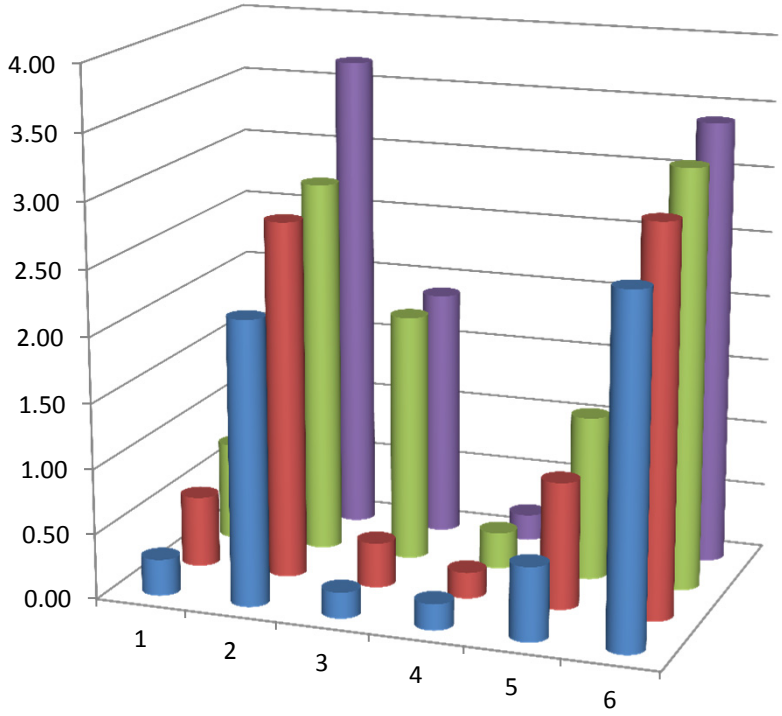
1. Uncertain
2. High
3. Severe

The marked services are selected for further problem formulation

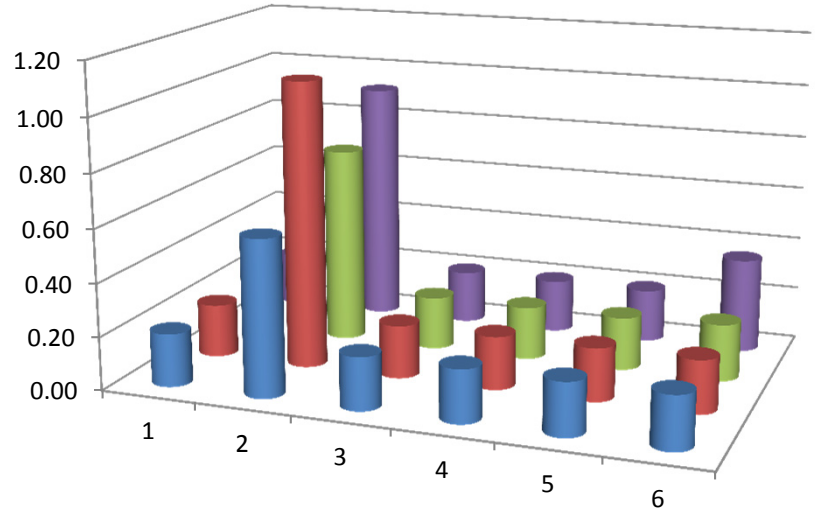
Risk probability level:

E-governmental Portal Investments

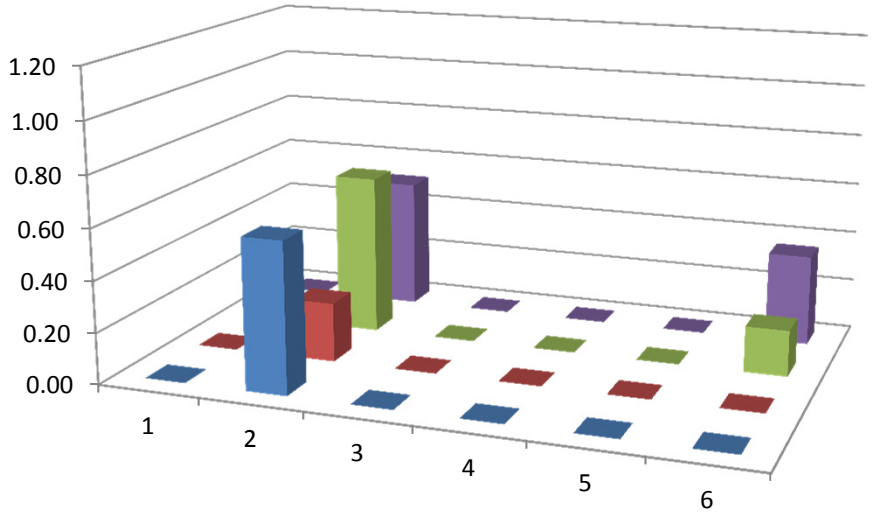
Total Investments



Prevention Investments



Repairing Investments



Periods:

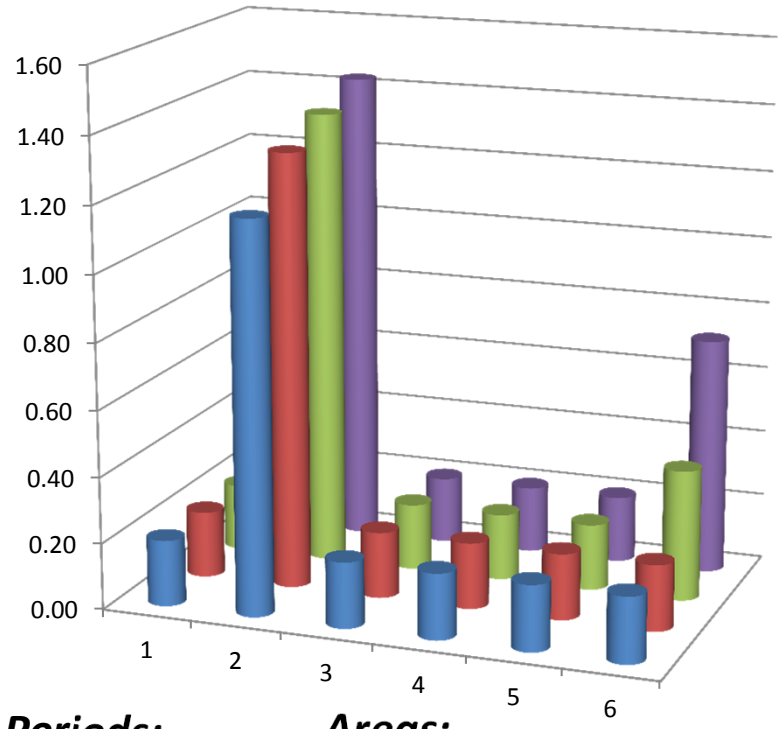
2010
2015
2020
2030

Areas:

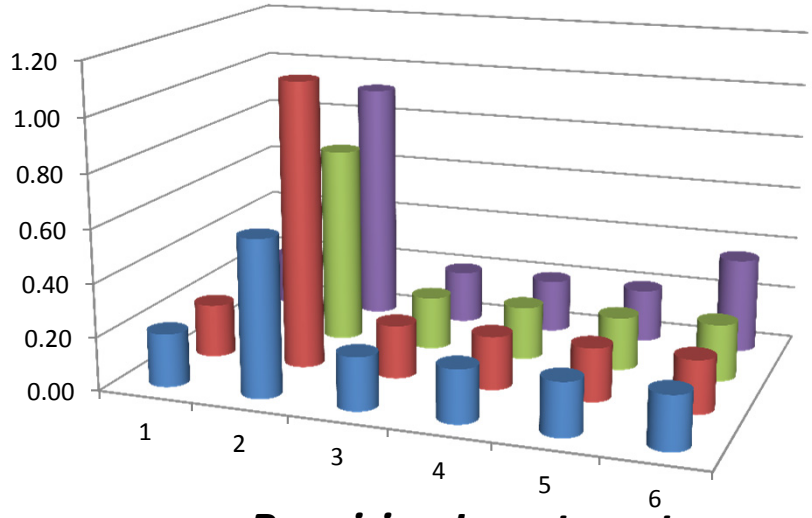
1- Human Factor
2 – Dig. Society
3 – Governance
4 – Economy
5 – New Tech
6 – Env. of living

Portal for Cyber Security

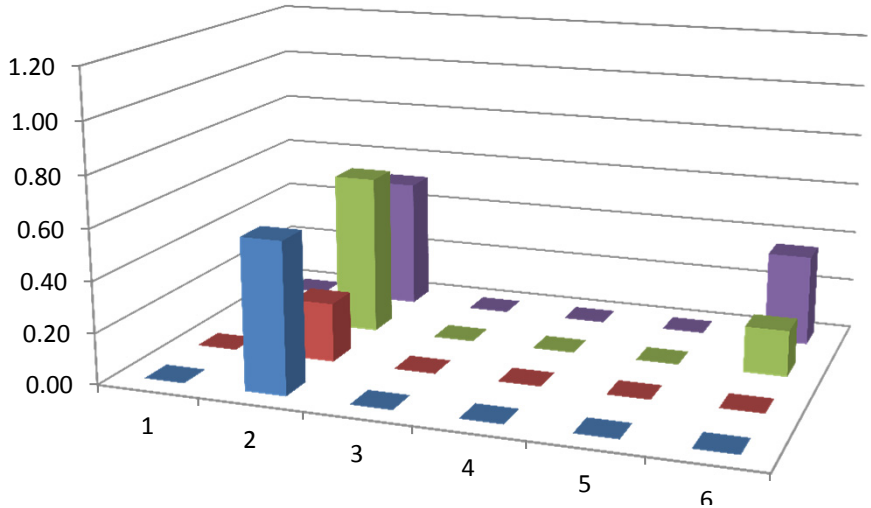
Total Investments



Prevention Investments



Repairing Investments



Periods:

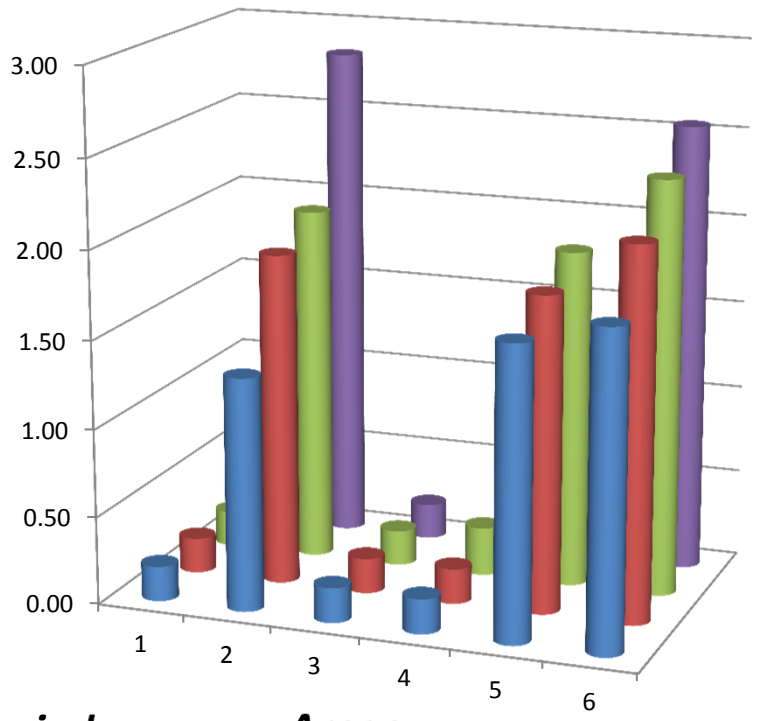
2010
2015
2020
2030

Areas:

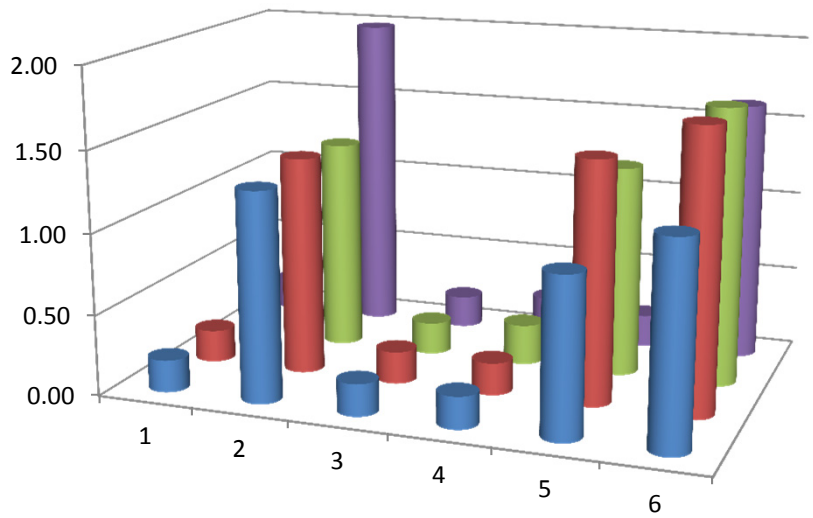
1- Human Factor
2 – Dig. Society
3 – Governance
4 – Economy
5 – New Tech
6 – Env. of living

Cloud Services

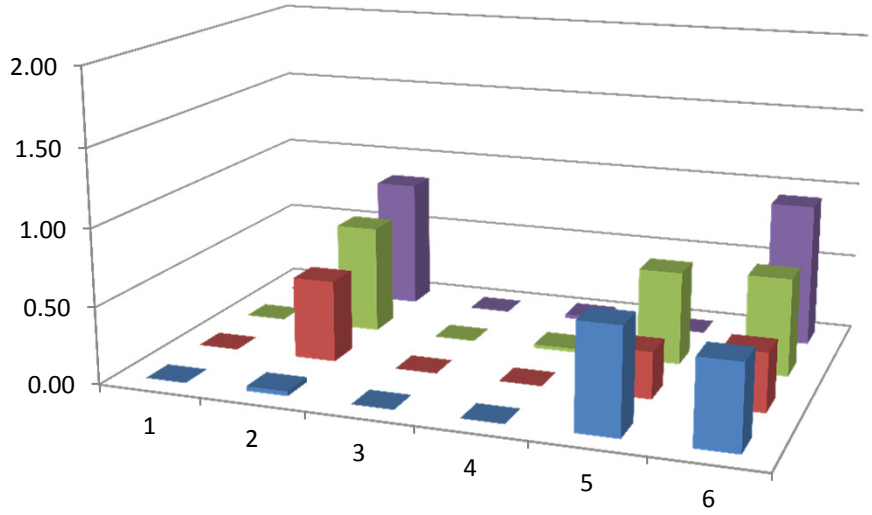
Total Investments



Prevention Investments



Repairing Investments



Periods:

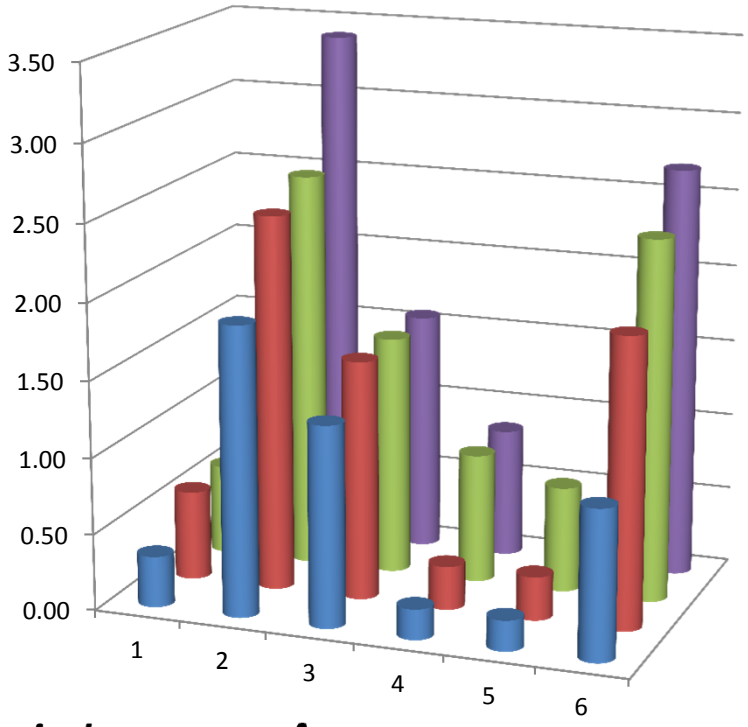
2010
2015
2020
2030

Areas:

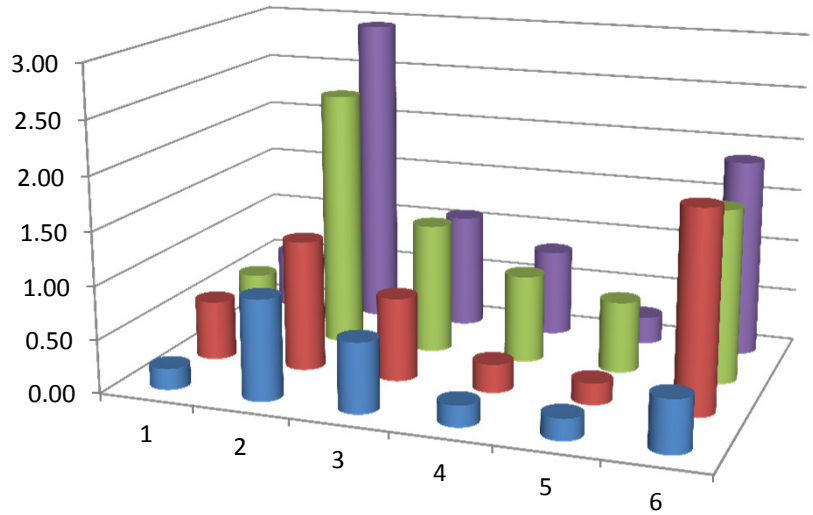
1- Human Factor
2 – Dig. Society
3 – Governance
4 – Economy
5 – New Tech
6 – Env. of living

Inf. Systems of Administrations

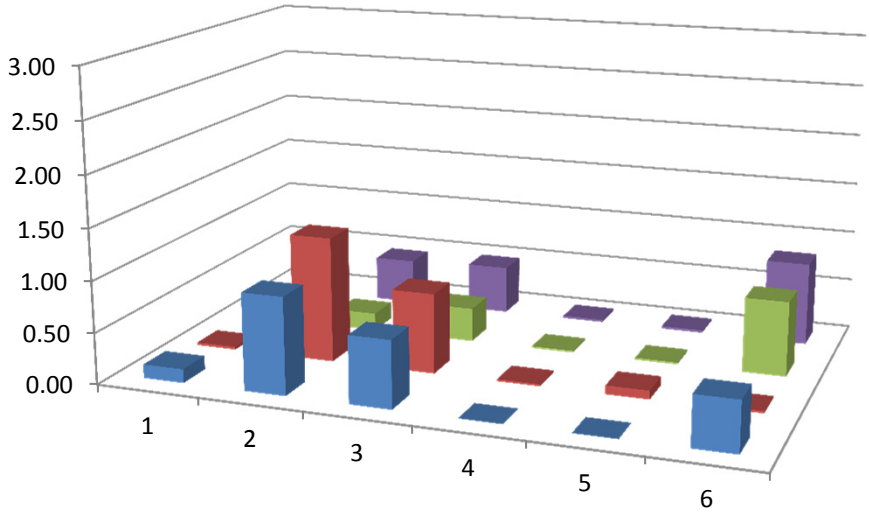
Total Investments



Prevention Investments



Repairing Investments



Periods:

2010
2015
2020
2030

Areas:

1- Human Factor
2 – Dig. Society
3 – Governance
4 – Economy
5 – New Tech
6 – Env. of living

GENERALIZED INVESTMENTS SHARES

Services/ Investments	Total Investments	Global Losses	Maximum Single Loss
e-Government Portal	35.00	24.33	1.13
Portal for Cyber Security	10.00	115.09	10.78
Cloud Services	25.00	46.87	2.65
Inf. Systems of Administrations	30.00	33.07	1.50

DISCUSSION

OBVIOUSLY, THE IDENTIFICATION OF FUTURE CYBER THREATS IS A COMPLEX TASK, ENCOMPASSING BOTH: EXPERTS' KNOWLEDGE AND A SUITABLE VALIDATION PROCESS. AS 'VALIDATION IN GENERAL' IS DIFFICULT TO BE ACHIEVED, CONTEXT DEPENDENT AND GOAL ORIENTED MULTICRITERIA OPTIMIZATION COULD BE IMPLEMENTED .

THIS IN COMBINATION WITH EXPERTS' BELIEFS SIMULATION PRODUCES A LESS UNCERTAIN, EXPLANATORY RESULT, CONCERNING THE UPCOMING DIGITAL FUTURE CYBER THREATS & ECONOMICAL INVESTMENTS EFFECT.

THANK YOU FOR YOUR ATTENTION!