Cyber threats optimization for e-government services

Veselin Politov, Zlatogor Minchev, Pablo Crotti,
Doychin Boyadzhiev, Marusia Bojkova, Plamen Mateev

Problem Definition

A discrete model of e-government (e-gov) services, encompassing: n different components – state bodies (e.g. ministries, agencies etc., engaged after the legal basis regulations), working during m time intervals are used.

One of the key measures that assure the model reliable work is the prevention from cyber attacks that will block the available e-gov services.

In order to achieve business continuity of these services, a certain amount of funding has to be invested. The correct spending of these funds will assure external interventions block or repairing after passed cyber attacks.

Model for Cyber attacks Optimization

Let a matrix $P = (p_{ij})$ be given, noting probability of a cyber attack in the time moment i, $i = 1, 2, \ldots, m$ and service j, $j = 1, 2, \ldots, n$. Another matrix $C = (c_{ij})$ for damages, resulting from a cyber attack in the interval i, $i = 1, 2, \ldots, m$ concerning the service j, $j = 1, 2, \cdots, n$ is also used.

Different cyber attacks prevention is provided with M funding, distributed amongst the e-gov services in the different time moments.

The aim of such funding distribution is to minimize the "overall damage".

The "overall damage" is the sum of multiplied probabilities for cyber attacks and the resulting damages for the different, used in the model, state bodies and periods. The maximal possible "overall damage" Z (excluding preventive investment) is as follows:

$$Z = \sum_{i=1}^{m} \sum_{j=1}^{n} p_{ij} c_{ij}.$$

The presented model is similar to [1] but is extended with additional "damage reduction function" – $q(x)$, which is defined for non-negative argument values. The following properties are valid for $q(x) : q(0) = 1$, the function is monotonically decreasing and $\lim_{x \to \infty} q(x) = 0$. This creates a specific damage reduction coefficient, if a certain amount of funding x is invested.

The logic behind is as follows: "more prevention investments – less damages from the expected cyber attacks".

Good examples for $q(x)$ are: e^{-x} and $\dfrac{1}{1+x}$. In this way if we invest x_{ij} funds for prevention of the j-th state body in the i-th moment, the resulting damage is decreased in accordance with the investment towards $p_{ij}q(x_{ij})c_{ij}$ and the aggregated one is:

$$z(x_{ij}) = \sum_{i=1}^{m}\sum_{j=1}^{n} q(x_{ij})p_{ij}c_{ij}.$$

Because of practical limitations, a low investments boundary ε ($x_{ij} \geq \varepsilon$) concerning different periods and services directions is used.

Thus, the following optimization task is formulated:

Find the funding investment distribution that provides a prevention of size M and minimize the "aggregated cyber attacks damage":

$$Z(M) = \min z(x_{ij}) = \min \sum_{i=1}^{m}\sum_{j=1}^{n} q(x_{ij})p_{ij}\ c_{ij} \tag{1a}$$

under the following constraints:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} x_{ij} \leq M, \qquad x_{ij} \geq \varepsilon, \quad i = 1 \div m,\ j = 1 \div n. \tag{1b}$$

Modification of the Model

The already described problem could be generalized as follows: the overall sum for cyber attacks countering consists of two components: cyber attacks prevention sum – X and cyber attacks repairing sum – U; $M = X + U$. An example for this, considers a part of M to be used for preliminary insurance from possible cyber attacks or repairing activities, following the idea: "more insurance investments for cyber attacks prevention, less repairing ones".

In order to describe the effectiveness of such an investment we use the function $r(u)$, which is analogous to $q(x)$ and is giving the reduction of a certain cyber attack damage, investing the sum u.

The following new model is accomplished:

$$Z(X,U) = \min z(x_{ij}, u_{ij}) = \min \sum_{i=1}^{m}\sum_{j=1}^{n} q(x_{ij})p_{ij}\, r(u_{ij})\, c_{ij} \tag{2a}$$

under the following constraints:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} x_{ij} \le X,\ \sum_{i=1}^{m}\sum_{j=1}^{n} u_{ij} \le U,\ x_{ij} \ge \varepsilon,\ u_{ij} \ge 0,\ i = 1 \div m,\ j = 1 \div n. \quad (2b)$$

Numerical experiments

In order to illustrate the presented models four different tasks concerning different e-government services from real projects experts' data (*E-gov portal*, *Portal for cyber security*, *Cloud services*, *Information Systems for Administrations*) have been solved. The total, prevention and repairing investments have been calculated for the years: 2010, 2015, 2020, 2030.

The values of matrix P (probabilities of cyber attacks) and C (damages, resulting from cyber attacks) are defined by STEMO Ltd. experts, taking into account the trends from [1], [2] and for six areas (facets): 1 – "Human Factor", 2 – "Digital Society", 3 – "Governance", 4 – "Economy", 5 – "New Technologies", 6 – "Environment of living".

The overall sum for cyber attacks countering is $M = 28$ units (with cyber attacks prevention sum $X = 21$ and cyber attacks repairing sum $U = 7$).

The low investments boundary is $\varepsilon = 0.2$. Exponent functions for $q(x)$ and $r(u)$ were used.

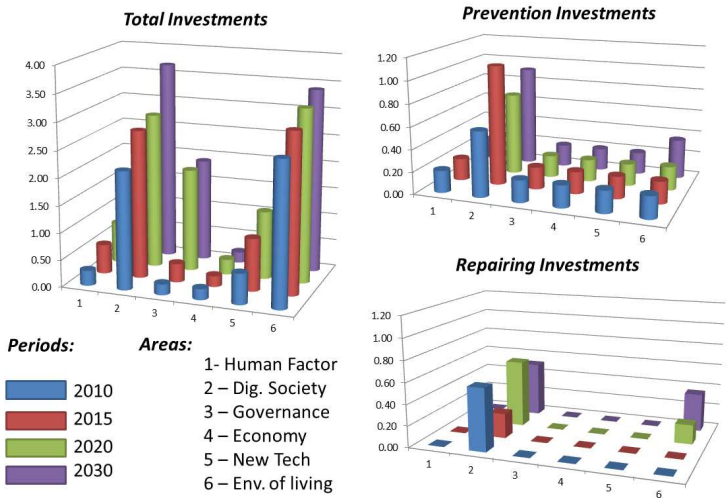

Figure 1: E-gov portal investments for cyber security

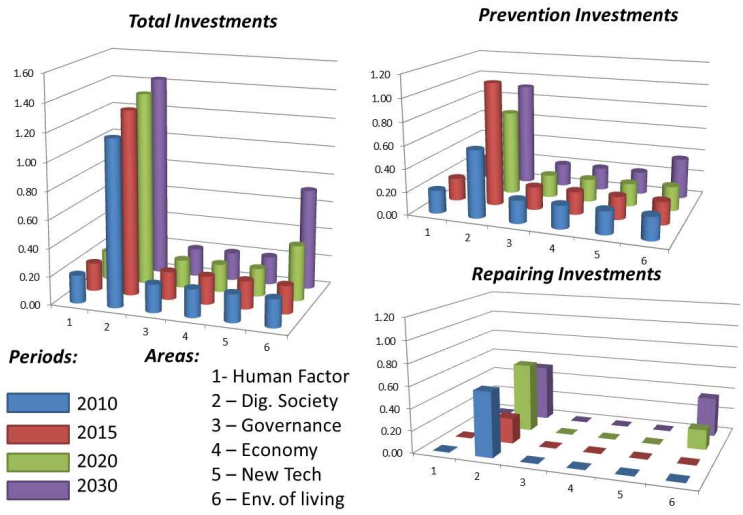

Figure 2: Portal for cyber security investments

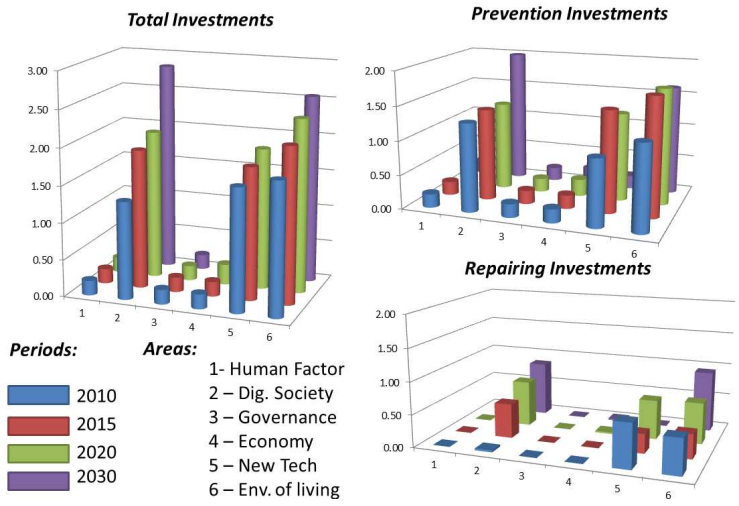

Figure 3: Cloud services cyber security investments

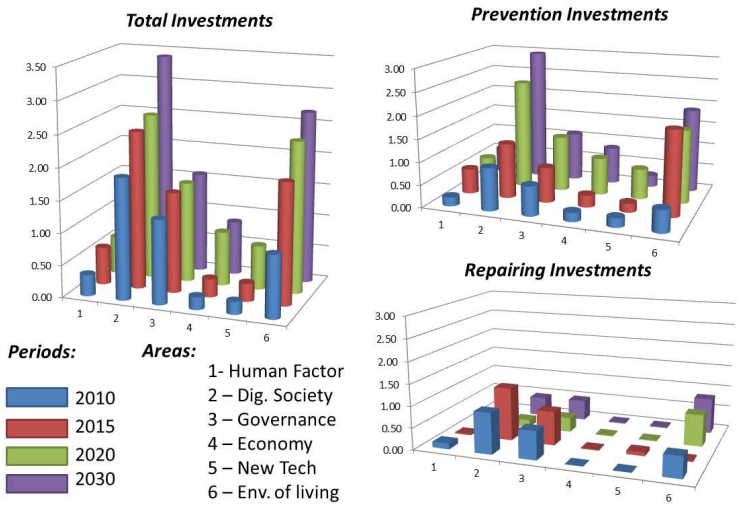

Figure 4: Information Systems for Administrations Cyber Security Investments

As input data could be presented in a small matrix form, MS EXCEL© 2010 product with build-in SOLVER was used [3].

A numerical summary of the results is given in Table 1:

Table 1: Numerical summary of the investments for cyber security

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

The numerical results obtained from our experimental calculations, though based on some experts' beliefs, are demonstrating a sustainable necessity of growing investments for cyber attacks prevention and repairing for the *Digital society* area, concerning the whole landscape of e-gov services. Apart of this, some other areas like: *New Technologies*, *Environment of living* and *Governance* were also noted as important ones.

The summarized results from Table 1 are outlining also an important point for the implemented model idea regarding the Portal for Cyber Security services, which is with minimal total investments and generates maximum potential global losses.

Obviously, this show the important role of cyber threats prevention investments in general for the created and studied e-gov services in the new digital society.

References

[1] Zlatogor Minchev & Emil Kelevedjiev, Multicriteria Assessment Scale of Future Cyber threats Identification, In: Proceedings of "Mathematics Days in Sofia", July 7–9, 2014, 93–94.

[2] Evangelos Markatos, Davide Balzarotti, Zlatogor Minchev et al., The Red Book – A Roadmap in the area of Systems Security, The SysSec Consortium, 2013.

[3] Christopher Zappe, Ch., Winston W., Ch. Albright, Data Analysis/Optimization/ Simulation Modelling with Microsoft Excel, International Edition, 2011.