IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 19, 2020, accepted September 12, 2020, date of publication September 29, 2020, date of current version October 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3027527

Two-Level System of on-Line Risk Assessment in the National Cyberspace

ANDRZEJ KARBOWSKI[1] AND KRZYSZTOF MALINOWSKI[2]
[1]Institute of Control and Computation Engineering, Warsaw University of Technology, 00-665 Warsaw, Poland
[2]Research and Academic Computer Network (NASK), 01-045 Warsaw, Poland

Corresponding author: Andrzej Karbowski (andrzej.karbowski@pw.edu.pl)

ABSTRACT The paper presents a hierarchical, two-level approach to on-line cyber risk assessment at the national level. It takes into account cyber threats and vulnerabilities identified at the lower level formed by essential service operators and digital service providers. A computational algorithm is proposed, making use of the local measurements and assessments and its asynchronous convergence is proved. At the end a case study concerning a system consisting of four entities is presented.

INDEX TERMS Convergence, distributed algorithms, hierarchical systems, network security, risk analysis.

I. INTRODUCTION

The article develops a hierarchical, two-level approach to an on-line national level risk assessment (NLRA), taking into account cyber threats and vulnerabilities identified at the lower level, which comprises key service operators and digital service providers. A key service operator or a digital service provider will be further referred to as a local entity (LE), while the unit responsible for risk assessment at the national level will be referred to as the Center (CNT).

It should be noted, that there are very few proposals of approaches to cyber risk assessment at a national level, in particular to on-line assessment [1]. According to ENISA's November 2013 analytical report [2], the NLRA could be carried out ''through a formalized central framework or approach...'' or ''based on a decentralized model where each actor prepares their own risk assessment to be integrated by a coordinating authority''. This document also says that NLRA approaches are either ''scenario-based, where actors are gathered together to consider scenarios in the round; such scenarios describe risks as a narrative and label them by applying simple categories of likelihood[1] and impact (low, medium, high)'' or ''quantitative approaches which apply ordinal thresholds...'', or ''approaches which combine elements of all of the above (for example, using scenarios and then qualitative and quantitative methods)''.

On the other hand, the Directive (EU) 2016/1148 of 6 July 2016 [3], concerning measures for a high common level of security of network and information systems across the European Union, requires the national Computer Security Incident Response Teams (CSIRTs) to provide, ''dynamic risk and incident analysis and situational awareness''.

Accordingly, two approaches can be taken to implement the NLRA. The first would be to build an aggregated model of a national cyberspace covering all relevant actors and taking into account their interdependencies. The second approach would be to propose a decentralized, hierarchical, two-level on-line framework for the NLRA, where LEs, on the basis of their local measurements, will repetitively produce their own assessments for use by the CNT to coordinate them and to estimate the overall risk (Fig. 1). This article is about the latter possibility.

It is also important that an on-line risk assessment should be predictive, taking into account, hopefully in a simplified way, temporal dependencies of LEs, in view of their local risk assessments on cyber threats and services provided by other LEs.

Other on-line mechanisms, based on different assumptions, were presented in [4], [5] and [6]-[11]. Some of the preliminary results of the author's work were presented in the conference communiqué [12]. This paper concentrates on the kernel of the proposed method: the computational algorithm and its convergence. The name of the approach has been changed for a better description of its essence.

II. GENERAL APPROACH – ITERATED FAILURE SCENARIOS

We assume that the risk assessment is to be performed in a repetitive mode, at times t_c, where $c = 1, 2, 3, \ldots$ and

[1]In this text the term ''likelihood'' is used to refer to a subjective, descriptive or numerical representation of a belief regarding the possibility of an event.

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.

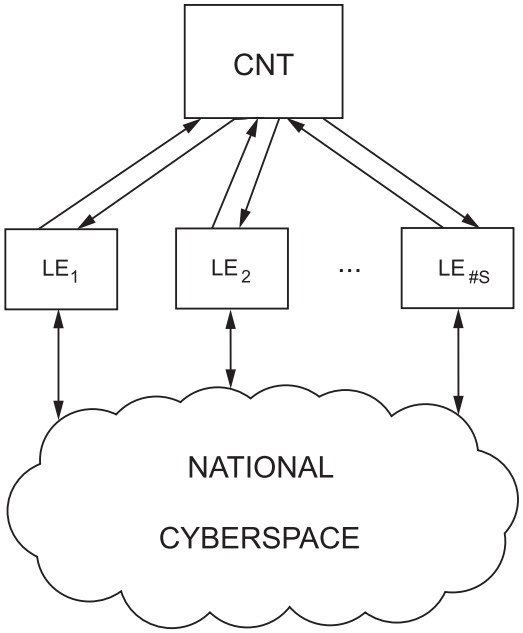

FIGURE 1. Two-level system of on-line risk assessment countrywide; S - the set of all considered services.

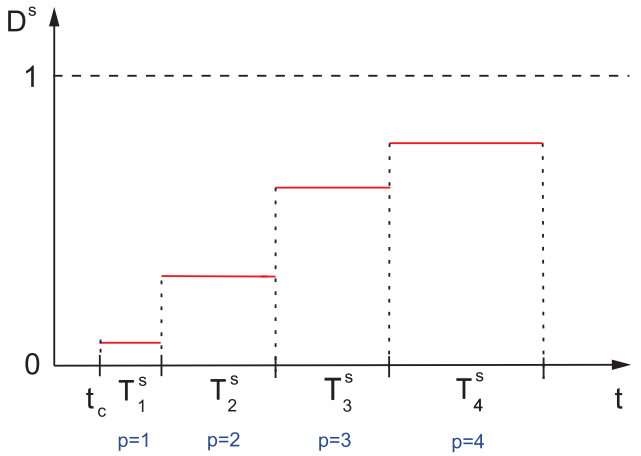

FIGURE 2. Exemplary possible failure scenario; $D^s(p)$ - level of likelihood of failure of the service s during subinterval T^s_p.

that the full NLRA may be performed at the beginning of each time period $[t_c, t_{c+1}]$ in such a fast mode, that the time required for the analysis is small when compared to the duration of the inter-analysis interval.

Assume that the current risk analysis of the service s at a given time t_c is concerned with future time interval T^s composed of a number of subintervals T^s_p, where $p = 1, \ldots, P^s$; i.e.,

$$T^s = T^s_1 \cup T^s_2 \cup \cdots \cup T^s_{Ps} \tag{1}$$

For each of these subintervals let the likelihood of failure of a service s be denoted as $D^s(p)$. In the simplest case this can be a real number, e.g., $D^s(p) \in [0, 1]$. The possible failure scenario (PFS) of the service s is then defined as $D^s = (D^s(p);\ p = 1, \ldots, P^s)$. The current time, at which the iterative process to be described is to be performed, is associated formally with the beginning of the subinterval T^s_1.

We assume that we allow for any appropriate risk assessment method to be used at a given local entity (LE) level, which is able to take into account:

- the current situation concerning its internal cyber security,
- PFSs of those LEs that are relevant to proper functioning of the considered LE,

and to produce its own PFS.

Intervals T^s_p can be of different length, related to periods of time relevant to various services. In particular, suppose that $P^s = 4$ and T^s_1 refers to short immediate future period during which some services may get affected by currently existing threats, including the observed cyber incidents. Other entities may be more concerned with the subsequent, longer, periods T^s_2, T^s_3 (mid-term), and T^s_4 (long-term) (Fig. 2).

PFSs of key services will represent crucial information at the CNT level and may be used, in particular, for graphical threat presentation and for the risk assessment (analysis) performed at this level, especially in case when the Center can assign numerical loss (cost) values to PFSs.

III. COORDINATION

Assume now that we initiate at a given time the analysis that will provide us with an overall risk assessment, under current conditions, over future time intervals T^s as defined above for all $s \in S$, where S is the set of all considered entities (services).

At the CNT level we may propose to adopt the iterative approach, following the interaction prediction method [13], [14]. One may begin with a set of initial PFSs $D^{s,(0)}$ for $s \in S$. This allows to initiate the iterations, i.e., to start the coordination process. The initial scenarios can be defined, e.g., as the result of calculations at time t_{c-1} or current local static risk analysis.

At iteration $k = 1, 2, 3, \ldots$ the set of PFSs given by $D^{s,(k)}$ for $s \in S$ is modified as follows. Let us take that for each entity s the set of those entities on which this entity is dependent is denoted as U^s. The scenarios $D^{u,(k)}$ for $u \in U^s$ are used together with all currently available information at LE level (likelihoods of cyber threats, local vulnerabilities, observed incidents, etc.) to perform local risk analysis and to estimate a new value $D^{s,(k),new}$ of the (output) scenario of the entity s. After this is done for all entities, the suite of new predicted scenarios for iteration $k + 1$ may be computed at the CNT level. For this purpose many algorithms can be used. The simplest of them is the direct re-injection whereby

$$D^{s,(k+1)} := D^{s,(k),new} \text{ for } s \in S \tag{2}$$

It usually would be better to use relaxation, smoothing, algorithm for computing $D^{s,(k+1)}$ as

$$D^{s,(k+1)} := \rho D^{s,(k),new} + (1 - \rho) D^{s,(k)} \tag{3}$$

where $0 < \rho \leq 1$ is the relaxation coefficient; if $\rho = 1$ then (3) reduces to (2). In both algorithms the substitutions are made component-wise.

The iterations defined by the algorithm are performed until a satisfactory convergence is achieved. It may happen that during the iterations, each of which may take some time, the information available at the LE level changes due to, for example, new incidents being observed and/or new vulnerabilities identified. This may affect the iterative process. Furthermore, the T_p^s range can be modified if needed. It can therefore be assumed, that the iterative process can be viewed as a continuous activity. Then the properties of this process should be examined in terms of the relevant factors, in particular the LE level analysis procedures and the dynamics of the local assessment problems.

IV. ANALYSIS AT LE LEVEL

To illustrate the procedure, let us now consider the risk assessment at the local entity level. Assume that the s-th LE information system suffers from a number of vulnerabilities that can be exploited by a number of cyber threats. The set of these vulnerabilities is denoted by V^s; $v \in V^s$ when vulnerability v is present in the information system of the considered entity. When this vulnerability is exploited there is an impact I_v^s on the likelihood of service provided by LE to be degraded or disrupted (service failure). These impacts may be, in particular, expressed as [4]: Very Low (0-0.04), Low (0.05-0.20), Moderate (0.21-0.79), High (0.80-0.95), Very High (0.96-1). The likelihood of vulnerability v that can be exploited may be defined as related to possible cyber threats, where, say, threat j may affect the s-th LE when $j \in J^s$. With each threat it should be possible to associate the level of likelihood that this threat may exploit vulnerability $v \in V^s$, namely L_{vj}^s. In addition to these internal cyber threats it may happen, that services external to the s-th LE, on which this entity is dependent, can be substantially degraded or disrupted for certain time periods. The set of those entities is denoted as U^s, while I_u^s represents an impact of the failure of service u on the service s. The likelihood of service s to fail within the subinterval T_p^s can be then defined as

$$L^s(p) = \sum_{v \in V^s} I_v^s \sum_{j \in J^s} L_{vj}^s \, R_j^s(p) + \sum_{u \in U^s} I_u^s D^u(p - \sigma_u^s) \quad (4)$$

where $p = 1, \ldots, P^s$ and $\sigma_u^s = 1, \ldots, P^s$ represent delays associated with time periods after which a failure of service u may affect in a substantial degree the s-th LE regarding its own capability to provide required service. Those delays can be either assumed to be different for various components of the failure function or the same for all components. In particular, they may be set as equal to zero whenever appropriate. In the case when $p < \sigma_u^s$ the value of $D^u(p - \sigma_u^s)$ refers to the past and is set to zero unless the service u is already compromised or interrupted at time of the ongoing risk analysis. In such a case, the above formulae allows to take into account the already observed level of service degradation, represented, for example, as $D^u(-1) = 1$.

Risk activation function may be defined as

$$R_j^s(p) = \begin{cases} 1 & \text{when threat } j \text{ is expected} \\ & \text{to be present within } T_p^s \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

It is assumed that $L^s(p)$ is dependent on cyber threats associated with subinterval T_p^s, while this likelihood may depend upon the failure likelihood of other services related to earlier subintervals. It is possible, of course, to introduce similar dependence of $L^s(p)$ on earlier threat occurrences.

In the simplest case, the output failure $D^s(p)$ of service s may be set as equal to $L^s(p)$, assuming that $L^s(p) \in [0, 1]$.

$$D^s(p) = \min\left(1, L^s(p)\right) \quad \text{for } p = 1, \ldots, P^s \quad (6)$$

It can be observed immediately, that we need to know the failure scenarios of services affecting the s-th LE to compute $L^s(p)$ (4) for $p = 1, \ldots, P^s$ and $D^s(p)$ may be computed only after $L^s(p)$ is known (6). So, for computing $L^s(p)$ from (4) at iteration k of the CNT level coordination step one should use $D^{s,(k)}$, while $D^s(p)$ computed then from (6) becomes a component of $D^{s,(k+1),new}$.

V. CONVERGENCE OF THE ALGORITHM

Now we will analyze the conditions under which the algorithm (3), (6), (4) is convergent.

Since the first component of the sum in (4) is a constant, we may represent this algorithm in the following general form:

$$x := F(x) \quad (7)$$

where $x \in \mathbb{R}^n$ is the vector of all variables $D^s(p)$, $p = 1, \ldots, P^s$, $s \in S$ and for $i = 1, \ldots, n$

$$F_i(x) = \rho \min(1, b_i + \sum_{j \neq i} a_{ij} x_j) + (1 - \rho) x_i \quad (8)$$

So, the general form of the algorithm (3),(6), (4) is as follows:

$$\begin{aligned} x_i &:= F_i(x) \\ &= \rho \min(1, b_i + \sum_{j \neq i} a_{ij} x_j) + (1 - \rho) x_i, \quad i = 1, \ldots, n \end{aligned} \quad (9)$$

The mapping $F(x)$ is nonsmooth, hence we cannot use directly the precise formula concerning nonlinear mappings from [15], based on Jacobian matrix. Instead, we will derive a sufficient condition of convergence making use of the theory of convergence for asynchronous iterative algorithms [15]–[17]. One of the most general theorems says, that a sufficient condition for the algorithm (7) to be convergent when implemented in a totally asynchronous way is the contractive character of the mapping $F : \mathbb{R}^n \mapsto \mathbb{R}^n$ in the maximum norm, that is [15]:

$$\|F(x) - F(y)\|_\infty < \|x - y\|_\infty \quad \forall x, y \in \mathbb{R}^n, x \neq y \quad (10)$$

Theorem 1: We consider a nonlinear mapping $F : \mathbb{R}^n \mapsto \mathbb{R}^n$ where the coordinate functions are defined as follows:

$$F_i(x) = \rho \min(1, b_i + \sum_{j \neq i} a_{ij} x_j) + (1 - \rho) x_i \quad i = 1, \ldots, n \quad (11)$$

for $\rho \in (0, 1]$. *If the coefficients* a_{ij} *are nonnegative and satisfy the conditions:*

$$\sum_{j\neq i} a_{ij} < 1, \quad i = 1, \ldots, n \tag{12}$$

then the mapping F *is a contractive mapping in the maximum norm.*

Proof: Let us consider two vectors $x, y \in \mathbb{R}^n$ and denote by i^* the index of the coordinate which determines the maximum norm of $x - y$, that is

$$\|x - y\|_\infty = \max_{i=1,\ldots,n} |x_i - y_i| = |x_{i^*} - y_{i^*}| \tag{13}$$

Taking into account definition (11) of functions F_i, when all coefficients a_{ij} are nonnegative and $0 < \rho \leq 1$, we have for the mapping F:

$$\begin{aligned}
&\|F(x) - F(y)\|_\infty \\
&= \max_{i=1,\ldots,n} \Big| \rho \min(1, b_i + \sum_{j\neq i} a_{ij}x_j) \\
&\quad + (1-\rho)x_i - \rho \min(1, b_i + \sum_{j\neq i} a_{ij}y_j) - (1-\rho)y_i \Big| \\
&= \max_{i=1,\ldots,n} \Big| \rho[\min(1, b_i + \sum_{j\neq i} a_{ij}x_j) - \min(1, b_i + \sum_{j\neq i} a_{ij}y_j)] \\
&\quad + (1-\rho)(x_i - y_i) \Big| \\
&\leq \rho \max_{i=1,\ldots,n} \Big| \min(1, b_i + \sum_{j\neq i} a_{ij}x_j) - \min(1, b_i + \sum_{j\neq i} a_{ij}y_j) \Big| \\
&\quad + (1-\rho) \max_{i=1,\ldots,n} |x_i - y_i|
\end{aligned} \tag{14}$$

Let us concentrate now on the term:

$$\Big| \min(1, b_i + \sum_{j\neq i} a_{ij}x_j) - \min(1, b_i + \sum_{j\neq i} a_{ij}y_j) \Big|$$

There are four combinations to analyze:

1) $b_i + \sum_{j\neq i} a_{ij}x_j < 1 \wedge b_i + \sum_{j\neq i} a_{ij}y_j < 1$
We have here:

$$\begin{aligned}
&\Big| \min(1, b_i + \sum_{j\neq i} a_{ij}x_j) - \min(1, b_i + \sum_{j\neq i} a_{ij}y_j) \Big| \\
&= \Big| b_i + \sum_{j\neq i} a_{ij}x_j - (b_i + \sum_{j\neq i} a_{ij}y_j) \Big| \\
&= \Big| \sum_{j\neq i} a_{ij}(x_j - y_j) \Big| \leq \sum_{j\neq i} a_{ij}|x_j - y_j|
\end{aligned}$$

2) $b_i + \sum_{j\neq i} a_{ij}x_j < 1 \wedge b_i + \sum_{j\neq i} a_{ij}y_j \geq 1$

We have here:

$$\begin{aligned}
&\Big| \min(1, b_i + \sum_{j\neq i} a_{ij}x_j) - \min(1, b_i + \sum_{j\neq i} a_{ij}y_j) \Big| \\
&= \Big| b_i + \sum_{j\neq i} a_{ij}x_j - 1 \Big| = 1 - (b_i + \sum_{j\neq i} a_{ij}x_j) \\
&\leq (b_i + \sum_{j\neq i} a_{ij}y_j) - (b_i + \sum_{j\neq i} a_{ij}x_j) \\
&= \sum_{j\neq i} a_{ij}(y_j - x_j) \leq \sum_{j\neq i} a_{ij}|y_j - x_j| \\
&= \sum_{j\neq i} a_{ij}|x_j - y_j|
\end{aligned}$$

3) $b_i + \sum_{j\neq i} a_{ij}x_j \geq 1 \wedge b_i + \sum_{j\neq i} a_{ij}y_j < 1$
We have here:

$$\begin{aligned}
&\Big| \min(1, b_i + \sum_{j\neq i} a_{ij}x_j) - \min(1, b_i + \sum_{j\neq i} a_{ij}y_j) \Big| \\
&= 1 - (b_i + \sum_{j\neq i} a_{ij}y_j) \\
&\leq (b_i + \sum_{j\neq i} a_{ij}x_j) - (b_i + \sum_{j\neq i} a_{ij}y_j) \\
&= \sum_{j\neq i} a_{ij}(x_j - y_j) \leq \Big| \sum_{j\neq i} a_{ij}(x_j - y_j) \Big| \\
&\leq \sum_{j\neq i} a_{ij}|x_j - y_j|
\end{aligned}$$

4) $b_i + \sum_{j\neq i} a_{ij}x_j \geq 1 \wedge b_i + \sum_{j\neq i} a_{ij}y_j \geq 1$
We have here:

$$|1 - 1| = 0 \leq \sum_{j\neq i} a_{ij}|x_j - y_j|$$

Summing up all these cases, we may write:

$$\Big| \min(1, b_i + \sum_{j\neq i} a_{ij}x_j) - \min(1, b_i + \sum_{j\neq i} a_{ij}y_j) \Big| \leq \sum_{j\neq i} a_{ij}|x_j - y_j| \tag{15}$$

Taking this, (13) and the assumption (12) into account in the assessment (14), it means that:

$$\begin{aligned}
&\|F(x) - F(y)\|_\infty \\
&\leq \rho \max_{i=1,\ldots,n} \sum_{j\neq i} a_{ij}|x_j - y_j| \\
&\quad + (1-\rho) \max_{i=1,\ldots,n} |x_i - y_i| \\
&\leq \rho \Big(\max_{i=1,\ldots,n} \sum_{j\neq i} a_{ij}|x_{i^*} - y_{i^*}| \Big) + (1-\rho)|x_{i^*} - y_{i^*}| \\
&= |x_{i^*} - y_{i^*}| \Big(\rho \max_{i=1,\ldots,n} \sum_{j\neq i} a_{ij} + (1-\rho) \Big) \\
&< |x_{i^*} - y_{i^*}|(\rho + 1 - \rho) = |x_{i^*} - y_{i^*}| = \|x - y\|_\infty
\end{aligned} \tag{16}$$

what means, that F is a contraction mapping in the maximum norm. □

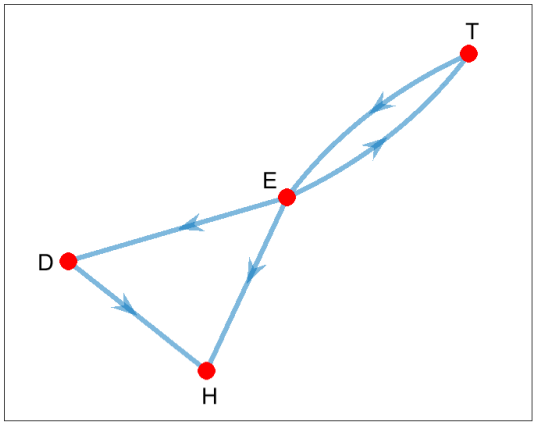

FIGURE 3. Graph of services. Notation: E - power company, T - transport company, H - hospital, D - data center.

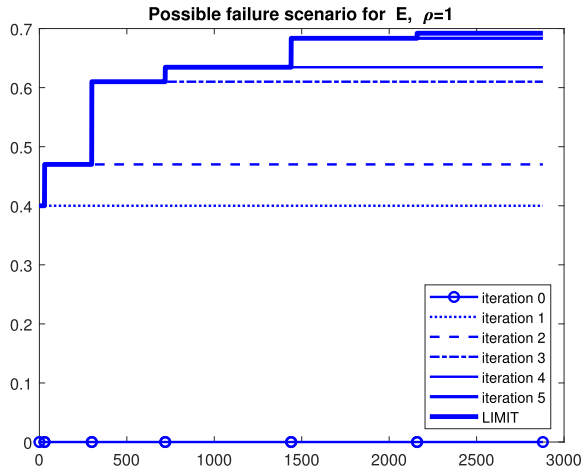

FIGURE 4. Possible failure scenarios for power plant (E) when the direct re-injection strategy was used.

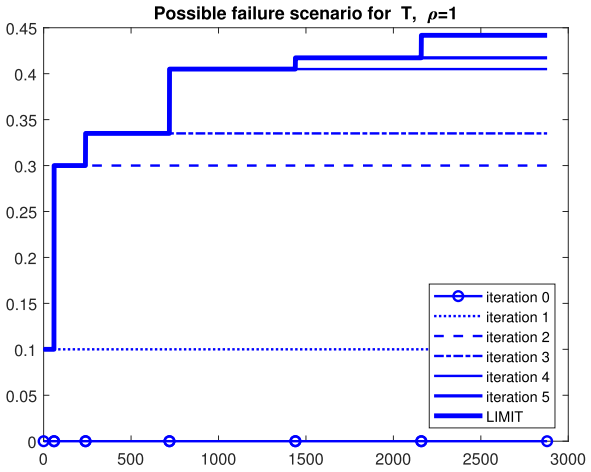

FIGURE 5. Possible failure scenarios for transport company (T) when the direct re-injection strategy was used.

VI. EXAMPLE OF A FOUR-ENTITY SYSTEM

To better illustrate the ideas introduced above and coordination strategies let us introduce a four-entity system consisting of the power company (E), the transport company (T), the hospital (H) and the data center (D). Assume that in case of each entity s we consider the possible failure scenario components concerned with service availability $D^s(p)$ for every possible value of p, as defined in (6). The graph of services and dependencies between them is presented if Fig. 3.

In all cases of the example entities considered it is assumed that formulae given by (4) are used together with (6) to compute the possible service failure scenarios, while the first term in (4), related to internally assessed threats, is represented by a given number.

Now let us start with the electricity company (E) and assume the following timing and formulae defining the relevant scenarios:

$$\begin{aligned} &D^E(p),\ p = 1, 2, \ldots, 6; \\ &T^E = [0,\ 30\text{ min}) \cup [30\text{ min},\ 5\text{ h}) \cup [5\text{ h},\ 12\text{ h}) \\ &\quad \cup [12\text{ h},\ 24\text{ h}) \\ &\quad \cup [24\text{ h},\ 36\text{ h}) \cup [36\text{ h},\ 48\text{ h}] \\ &L^E(p) = 0.4 + 0.7 \cdot D^T(p-1), \end{aligned}$$

Then define relevant likelihood and failure scenarios of the other services.

For the transport company (T) they are as follows:

$$\begin{aligned} &D^T(p),\ p = 1, 2, \ldots, 6; \\ &T^T = [0,\ 1\text{ h}) \cup [1\text{ h},\ 4\text{ h}) \cup [4\text{ h},\ 12\text{ h}) \cup [12\text{ h},\ 24\text{ h}) \\ &\quad \cup [24\text{ h},\ 36\text{ h}) \cup [36\text{ h},\ 48\text{ h}] \\ &L^T(p) = 0.1 + 0.5 \cdot D^E(p-1), \end{aligned}$$

The likelihoods and scenarios of the data center (D) are specified as:

$$\begin{aligned} &D^D(p),\ p = 1, 2, \ldots, 6; \\ &T^D = [0,\ 2\text{ h}) \cup [2\text{ h},\ 5\text{ h}) \cup [5\text{ h},\ 12\text{ h}) \cup [12\text{ h},\ 24\text{ h}) \\ &\quad \cup [24\text{ h},\ 36\text{ h}) \cup [36\text{ h},\ 48\text{ h}] \\ &L^D(p) = 0.05 + 0.2 \cdot D^E(p-1), \end{aligned}$$

And finally, for the hospital (H) we define the likelihoods and failure scenario as:

$$\begin{aligned} &D^H(p),\ p = 1, 2, \ldots, 6; \\ &T^H = [0,\ 1\text{ h}) \cup [1\text{ h},\ 3\text{ h}) \cup [3\text{ h},\ 12\text{ h}) \cup [12\text{ h},\ 24\text{ h}) \\ &\quad \cup [24\text{ h},\ 36\text{ h}) \cup [36\text{ h},\ 48\text{ h}] \\ &L^H(p) = 0.15 + 0.2 \cdot D^E(p-1) + 0.15 \cdot D^D(p-1). \end{aligned}$$

It can be seen that both the number of time periods and their duration vary between different scenarios, while it is assumed that the overall time horizon is equal to 48 hours.

The objective now is to demonstrate the coordination process at the central level, while using the coordination strategy (3) with various relaxation coefficients.

The results of computations when the direct re-injection strategy (2) ($\rho = 1$ in algorithm (3)) was used are presented in

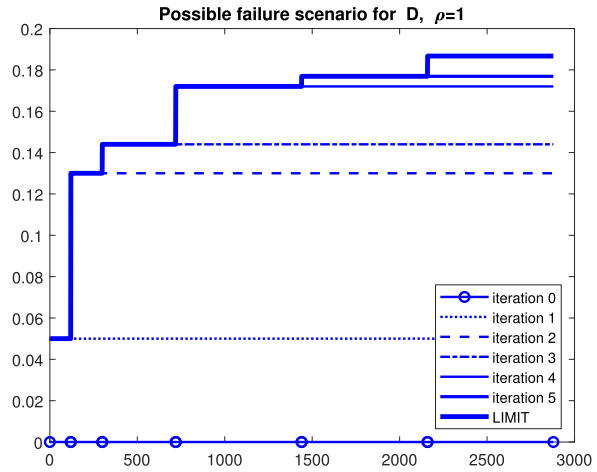

FIGURE 6. Possible failure scenarios for data center (D) when the direct re-injection strategy was used.

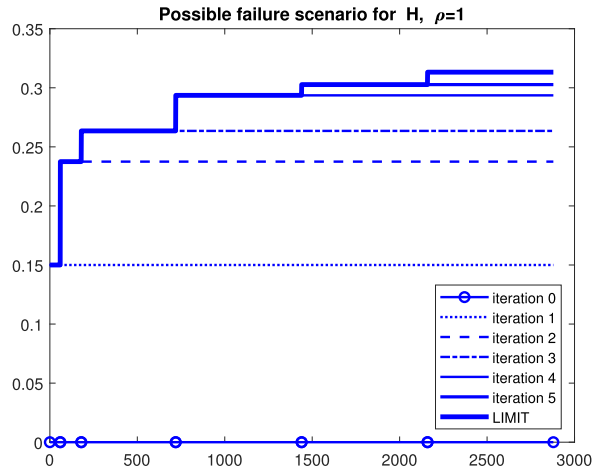

FIGURE 7. Possible failure scenarios of the services delivered by hospital (H) when the direct re-injection strategy was used.

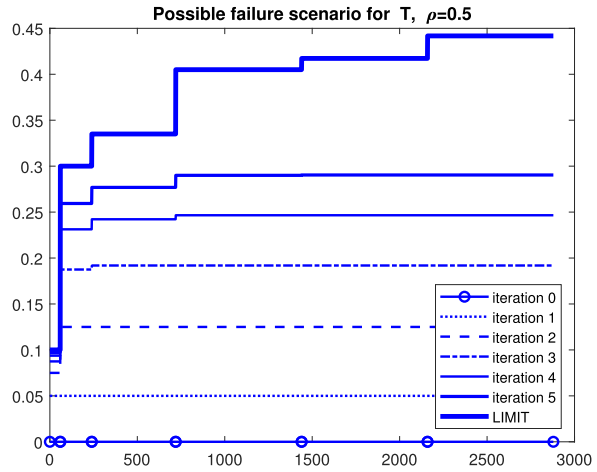

FIGURE 8. Possible failure scenarios for the transport company (T) when the relaxation algorithm with $\rho = 0.5$ was used.

Figs. 4-7. For the termination condition $\varepsilon = 10^{-6}$ we needed 7 iterations to obtain the convergence.

It can be observed that the rise of the likelihood of failure in the delivery of electricity (e.g., caused by weather conditions) results in immediate jumps of the likelihoods of failure of the railway system (that is transport company) and a little later we can see the same effect for the data center and the hospital. Since the disruption of power supply prolongs over next day, all cyber threats remain on higher levels for all services.

The results of computations of the D^T scenario (for other scenarios we observed the same effects) when the relaxation strategy was used are presented in Fig. 8. We used $\rho = 0.5$ in the algorithm (3). It can be seen that the result is the same as in the case of the re-injection strategy, but the changes between iterations are smoother. Unfortunately, in this case for the same termination condition $\varepsilon = 10^{-6}$ the calculations took more time: to obtain the convergence 33 iterations were needed.

VII. CONCLUSION

We proposed a hierarchical, two-level on-line scheme for the national-level risk assessments, where local entities repetitively prepare their own assessments used by the Center (national CSIRT) to coordinate those assessments and to evaluate the overall risks. Our on-line risk assessment algorithm is predictive, taking into account temporal dependencies of local entities on cyber threats and services provided by other local entities. The iterative scheme which calculates the local forecast expresses interdependencies between different services as a linear combination of local and external components. Due to the truncation function restricting the value of the external components, the resulting mapping is nonlinear and nonsmooth. Fortunately, in quite a natural case, when the sum of the external weights does not exceed 1, this mapping is contractive and the whole algorithm is convergent. That was proved in the paper and confirmed in a numerical case study concerning a system consisting of four entities.

REFERENCES

[1] Y.Y. Haimes, J. Santos, K. Crowther, M. Henry, Ch. Lian and Z. Yan, "Risk analysis in interdependent infrastructures," in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi, Eds. Boston, MA, USA: Springer, 2007, pp. 297–310.

[2] *National-level Risk Assessments An Analysis Report—Executive Summary*, European Union Agency for Network and Information Security, ENISA, Heraklion, Greece, Nov. 2013.

[3] The European Parliament and the Council of the European Union, "Directive (Eu) 2016/1148 of The European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," *Off. J. Eur. Union*, vol. 59, pp. L194/1–L194/30, Jul. 2016.

[4] *Guide for Conducting Risk Assessments, Information Security*, document NIST Special Publication 800–30 Revision, National Institute of Standards and Technology, U.S. Department of Commerce, 2012, vol. 1.

[5] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using Bayesian attack graphs," *IEEE Trans. Depend. Sec. Comput.*, vol. 9, no. 1, pp. 61–74, Jan. 2012.

[6] V. Viduto, C. Maple, W. Huang, and D. López-Peréz, "A novel risk assessment and optimization model for a multi-objective network security countermeasure selection problem," *Decis. Support Syst.*, vol. 53, no. 3, pp. 569–610, 2012.

[7] S. Naumov and I. Kabanov, "Dynamic framework for assessing cyber security risks in a changing environment," in *Proc. Int. Conf. Inf. Sci. Commun. Technol. (ICISCT)*, Nov. 2016, pp. 4854–4863.
[8] M. Kalantarnia, F. Khan, and K. Hawboldt, "Dynamic risk assessment using failure assessment and Bayesian theory," *J. Loss Prevention Process Industries*, vol. 22, no. 5, pp. 600–606, Sep. 2009.
[9] F. Khan, S. J. Hashemi, N. Paltrinieri, P. Amyotte, V. Cozzani, and G. Reniers, "Dynamic risk management: A contemporary approach to process safety management," *Current Opinion Chem. Eng.*, vol. 14, pp. 9–17, Nov. 2016.
[10] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, and S. Huang, "Multimodel-based incident prediction and risk assessment in dynamic cybesecurity protection for industrial control systems," *IEEE Trans. Syst., Man, Cybern.*, vol. 46, no. 10, pp. 1426–1444, Oct. 2016.
[11] D. López, O. Pastor, and L. J. G. Villalba, "Dynamic risk assessment in information systems: State-of-the-art," in *Proc. 6th Int. Conf. Inf. Technol. (ICIT)*, vol. 8, May 2013, pp. 1–9.
[12] K. Malinowski and A. Karbowski, "Hierarchical on-line risk assessment at national level," in *Proc. Int. Conf. Mil. Commun. Inf. Syst. (ICMCIS)*, May 2019, pp. 1–5.
[13] M. D. Mesarović, D. Macko, and Y. Takahara, *Theory of Multi-level Hierarchical Systems*. New York, NY, USA: Academic, 1970.
[14] W. Findeisen, F. N. Bailey, M. Brdys, K. Malinowski, P. Tatjewski, and A. Wozniak, *Control and Coordination in Hierarchical Systems*. London, U.K.: Wiley, 1980.
[15] D. P. Bertsekas and J. N. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods*. Belmont, MA, USA: Athena Scientific, 2015.
[16] A. Karbowski, "Distributed, asynchronous algorithms for data networks control—A state of the art review," in *Artificial Intelligence and Computer Science*, S. Shannon, Ed. New York, NY, USA: Nova Science Publishers, Inc., 2005, pp. 59–82.
[17] A. Karbowski, "Comments on 'optimization flow control.I. Basic algorithm and convergence,'" *IEEE/ACM Trans. Netw.*, vol. 11, no. 2, pp. 338–339, Apr. 2003.