Int. J. Appl. Math. Comput. Sci., 2020, Vol. 30, No. 3, 597–609
DOI: 10.34768/amcs-2020-0044

REAL–TIME HIERARCHICAL PREDICTIVE RISK ASSESSMENT AT THE NATIONAL LEVEL: MUTUALLY AGREED PREDICTED SERVICE DISRUPTION PROFILES

KRZYSZTOF MALINOWSKI [a], ANDRZEJ KARBOWSKI [a,b,*]

[a]Centre for Research and Technology Transfer
Research and Academic Computer Network—State Research Institute (NASK PIB)
ul. Kolska 12, 01-045 Warsaw, Poland

[b]Institute of Control and Computation Engineering
Warsaw University of Technology
ul. Nowowiejska 15/19, 00-665 Warsaw, Poland
e-mail: andrzej.karbowski@pw.edu.pl

We present a real-time hierarchical approach to an on-line risk assessment at the national level taking into account both local risk analyses performed by key service operators and relevant interdependencies between those services. For this purpose we define mutually agreed predicted service disruption profiles and then propose a coordination mechanism to align those profiles. A simple, four-entity example is provided to illustrate the coordination.

Keywords: risk assessment, cyber security, hierarchical approach, service disruption profiles, coordination.

1. Introduction

This paper aims to address several crucial issues concerned with developing an approach to performing a dynamic real-time risk assessment at a national level or just a district level, taking into account, first, cyber threats and vulnerabilities as identified at the local level of essential (key) service operators (KSO) and digital service providers (DSP), and then relevant interdependencies between various KSOs and DSPs. It will be shown that at a national or a district level the cyber risk assessment cannot, in fact, be made without taking account, whenever necessary, of other than cyber threats, like, in particular, extreme atmospheric conditions or possible terrorist attacks. It will also be shown that a hierarchical approach is needed to coordinate local, i.e., institution (service) level risk estimates, in particular those concerning mutual interdependencies of the essential services considered.

From now on the term "national level" refers both to the truly national or to the district (regional) level, concerned with a number of interacting key services and data providers.

*Corresponding author

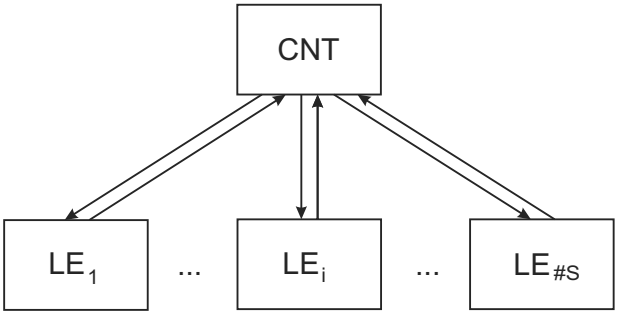

Fig. 1. Architecture of the hierarchical system for predictive risk assessment countrywide. CNT: center, LE_i, $i \in S$: local entities.

KSOs and DSPs, as well as any other institutions being important for the national-level risk assessment (NLRA) and for the dynamic national-level risk assessment (DNLRA) will be further related to as the local entities (LE) while the entity responsible for the national-level risk assessment itself will be related to as the Center (CNT) (Fig. 1).

It should be observed that there are practically

no proposals, at least in the available published literature (Haimes *et al*., 2007; Lian and Haimes, 2006; Poolsappasit *et al*., 2012; Naumov and Kabanov, 2016; Kalantarnia *et al*., 2009; Khan *et al*., 2016; Zhang *et al*., 2016; López *et al*., 2013; Rausand, 2011; Szwed and Skrzyński, 2014), concerning approaches to national level risk assessment, in particular to dynamic (on-line) assessment. According to the ENISA Analysis Report, made available in November 2013 (ENISA, 2013), NLRA can be performed either "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." From this document it can be also conceived that NLRA methodologies being considered are of an off-line type, being either "scenario-based approaches where actors are gathered together to consider scenarios in the round; such scenarios describe risks as narrative and label them by applying simple categories of likelihood and impact (low, medium, high)" or "quantitative approaches which apply ordinal thresholds ...", or, finally, "approaches which combine elements of all of the above (for example, using scenarios and then qualitative and quantitative methods)."

The term 'likelihood' is used in this paper to refer to a subjective numerical representation of a belief regarding the possibility of an event, based on the knowledge of the threat—unlike frequentist probability, which is estimated empirically from data (Zwikael and Smyrk, 2019). Risk assessors do not define a likelihood function in the statistical sense. Instead, they assign a score (or likelihood assessment) based on available evidence, experience, and expert judgment (NIST, 2012).

The mentioned ENISA report does not, however, describe any approach in detail, while it contains a recommendation that "a practical step-by-step guide on how to perform National-Level Risk Assessments should be developed, tested and maintained." As far as NLRA is concerned, it is also recommended to achieve "greater stakeholder involvement and information sharing."

It is important to note that the Directive (EU) 2016/1148 of 6 July 2016 (EU, 2016), concerning measures for a high common level of security of network and information systems across the European Union, to be referred to as the NIS Directive, requires the national Computer Security Incident Response Teams (CSIRTs) to provide, in particular, "dynamic risk and incident analysis and situational awareness."

In view of the above, two approaches may be adopted. The first of them would be to build an aggregated model of an overall national cyberspace, encompassing all relevant entities and taking into account their mutual dependencies, in order to perform a dynamic national level risk assessment (DNLRA). This approach, based, for example, on introducing aggregated states representing various services at various situations and their interdependencies, and leading to a Markovian model (Karbowski *et al*., 2019), must hinge upon the Center being able to estimate the required aggregated probabilities, in general the aggregated risk factors, concerned with possible mutual interactions of the various institutions. This, in particular, might appear very difficult, if not impossible, at the Center level, where not sufficient experience and/or data related to the risks encountered, or anticipated, at the level of the local entities might be available.

An alternate approach is to propose a decentralized or, rather, a hierarchical dynamic scheme for real-time DNLRA, where the local entities (LEs) would repetitively prepare their own assessments to be then used by the Center (e.g., a national CSIRT) to coordinate those assessments and to evaluate the overall risks.

This paper is concerned with the latter possibility, i.e., with the hierarchical dynamic national level risk assessment (HDNLRA).

The first, preliminary, version of such approach was proposed by us earlier (Malinowski and Karbowski, 2019).

The research on hierarchical methods and coordination has a long history (Mesarović *et al*., 1970; Findeisen *et al*., 1980; Haimes, 2016)). Such an approach can be also successfully used to modeling and management of modern computational systems (Kołodziej and Xhafa, 2011).

It is 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 on the services provided by other interacting LEs. A static off-line model to calculate the resilience of the Critical Infrastructure (understood as the ability to "resist" the consequences of an incident), where several (given) scenarios with their likelihoods to occur are considered, was recently presented by König *et al*. (2019). In our work we assume that the risk assessment is to be performed on-line in a repetitive mode, say at times t_k, where $k = 1, 2, \ldots$, and the scenarios are not given *a priori*, but changed as the time goes on. Moreover, we take into account the postulate expressed by Settanni *et al*. (2017) that "organizations need to cooperatively exchange security-relevant information to obtain a broader knowledge on the current cyber threat landscape and subsequently obtain new insights into their infrastructures and timely react if necessary" (Skopik *et al*., 2016), assuming that they share

- information about recent or ongoing incidents,
- information about service dependencies,
- information about the technical service status.

For the time being it is assumed that full DNLRA (or HDNLRA) may be performed at the beginning of each time period $[t_k, t_{k+1}]$ in such a fast mode that the time required for this analysis is small compared with the duration of this inter-analysis interval. We shall come back to this issue later when discussing a modification to the proposed hierarchical assessment scheme when such an assumption cannot be made.

2. Predicted service disruption profiles and mutually agreed predicted service disruption profiles

Let us now identify and then elaborate upon the first of several important factors that may contribute to shaping the central level analysis of risks leading to an overall risk assessment. It will be best achieved with the help of an example infrastructure.

Consider a simple example of four key service providers located in a given area (district):

(i) a power company (or a suite of companies) being in charge of both local electricity generation facilities and of power transmission and distribution grid (E),

(ii) a local railway transport company (T),

(iii) a major hospital (H),

(iv) a digital service provider in the form of a data center (D).

Both the hospital and the data center depend upon the electricity provided by the power company, while some of the health services offered by the hospital depend also upon an access to the data center. The power company, namely, the electricity generating facility, assumed to be coal fired, is dependent upon the railway transport, while the transport operations depend upon the supply of electricity.

The graph of services and connections between them is presented in Fig. 2.

Now assume that each local entity (LE) has its own information system that may be vulnerable and subject to various cyber threats, leading, possibly, to deterioration or even total disruption of a particular service provided by this entity to its clients and, also, to the other entities. For example, corruption of the SCADA system controlling power generation and/or power distribution may lead to power outages in townships and rural communities in the area served by the power company and, in particular, to breaks in power supply to the hospital, the transport company and to the data center.

Consider now the hospital and assume that the management there is concerned with both its own cyber related threats and with possible future breaks in the energy supply. Assume that at a given time the risk

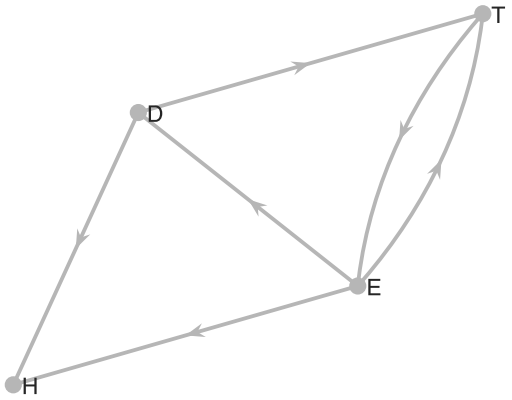

Fig. 2. Graph of services from the example. E: power company, T: transport company, H: hospital, D: data center.

assessment concerning future deterioration or disruption of health services as provided by the hospital involves a defined time period, say, time interval Θ^H composed of a number of, let us say P^H, sub-intervals Θ_p^H, where $p = 0, 1, \ldots, P^H - 1$; i.e., $\Theta^H = \Theta_0^H \cup \Theta_1^H \cup \cdots \cup \Theta_{P^H-1}^H$. The current time, at which the risk assessment is to be performed, say, time t_k, is formally associated with the beginning of the sub-interval Θ_0^H. The predicted service disruption profile (PSDP) of the hospital services may then be defined as

$$D^{A,H} = (D^{A,H}(p);\ p = 0, \ldots, P^H - 1), \qquad (1)$$

where $D^{A,H}(p)$ represents information concerning the predicted status related to the availability of the hospital services during time sub-interval Θ_p^H. In the simplest case this information might be expressed by a single number related to the predicted likelihood of stopping the hospital services during sub-interval Θ_p^H; this number might be normalized to interval [0,1] or expressed in some other scale, for example, as $D^{A,H}(p) \in \{0, 1, \ldots, 10\}$, i.e., in a scale related to a risk assessment technique used at the LE level. $D^{A,H}(p)$ can, in a more elaborate case, be defined as a set of numbers representing, for example, a probability distribution of failure during sub-interval Θ_p^H as well as some measure related to possible degree of failure.

The predicted service disruption profile (PSDP) of the hospital can be defined by choosing the number and the lengths of subintervals of which Θ^H is composed as well as the way in which $D^{A,H}(p)$ is expressed, as is considered proper for the risk assessment performed at the Center and related to possible disruptions or even a full break down of health services provided by the hospital. Yet, since it was assumed that the state of the

services offered by the hospital had no direct influence on other services, the definition of $D^{A,H}$ is not relevant for risk analysis and the assessment performed by operators of the other services. Thus, $D^{A,H}$ may be referred to as just the predicted disruption profile (noninteracting or internal) of the hospital services. This profile may be essential to estimate the level of risk associated with possible degradation or disruption of future services.

In fact, such a profile, as considered within the sphere of interest of a given service operator, may be defined for each key service provider. For example, $D^{A,E}$ can be introduced for the power company and be related to its clients other than the suite of key services. Yet, in the case of this entity all other services are dependent upon the deliveries of electricity. Consequently, we may now ask the question concerning a proper definition of the PSDP of this company. It can be observed that different representations of such a profile or profiles might be relevant for the concerned dependent entities. For example, a failure to deliver electricity to the railway system (transport company) will have immediate result in breaking this system operation. On the other hand, both the hospital and the data center might not be concerned too much about an immediate failure of electricity power delivery, due to available power backup facilities. Instead, the operators of those services might be much more troubled by the contingency of a long term and lasting disruption of power supply since their backup facilities may not be able to satisfy full requirements for power over the prolonged periods. Generation of electricity within a power company may depend upon only a long-term breakdown of the railway transport, say, on a breakdown lasting more than a day or two days. This leads us to define, when required, for a given pair of services, of which the first is the provider and the second is the user, the mutually agreed predicted service disruption profile (MAPSDP). In the case of the pair consisting of the electricity company (E) and the transport company (T) the related MAPSDP can then be defined in a similar way as the PSDP in Eqn. (1), yet being specialized for this particular pair of services, on the agreed interval $\Theta^{ET} = \Theta_0^{ET} \cup \Theta_1^{ET} \cup \cdots \cup \Theta_{P^{ET}-1}^{ET}$:

$$D^{A,ET} = (D^{A,ET}(p);\ p = 0, \ldots, P^{ET} - 1), \qquad (2)$$

where $D^{A,ET}(p)$ represents information concerning the predicted availability of electricity supply for railway operations during time sub-interval Θ_p^{ET}. For example, the length of Θ_0^{ET} could be 5 minutes, the length of Θ_1^{ET} could be 11 hours and 55 minutes, and, finally, the length of Θ_2^{ET} could be 60 hours ($P^{ET} = 3$). In the simplest case $D^{A,ET}(p) \in \{0, 1\}$, where $D^{A,ET}(p) = 0$ means that the service is provided within Θ_p^{ET} and $D^{A,ET}(p) = 1$ means that the electricity supply is disrupted. Otherwise, $D^{A,ET}(p) \in [0, 1]$ can represent the likelihood of a possible breakup of electricity supply to the railway network within the subinterval Θ_p^{ET}. Alternatively, $D^{A,ET}(p) \in \{0, 1, \ldots, 10\}$ can represent the magnitude of the perceived future possible disruption (disruptions) on yet another scale.

Now, as far as the pair consisting of the electricity company (E) and the data center (D) is considered, the MAPSDP, defined accordingly to the needs of both entities on the interval $\Theta^{ED} = \Theta_0^{ED} \cup \Theta_1^{ED} \cup \cdots \cup \Theta_{P^{ED}-1}^{ED}$, will be

$$D^{A,ED} = (D^{A,ED}(p);\ p = 0, \ldots, P^{ED} - 1) \qquad (3)$$

with information $D^{A,ED}(p)$ related to the availability of power supply for the data center over subinterval Θ_p^{ED}. For example, the sub-intervals could be Θ_0^{ED}, 12 hours in length, and Θ_1^{ED}, 60 hours in length ($P^{ED} = 2$). Let again $D^{A,ED}(p) \in \{0, 1\}$, where 0 denotes the service being available and 1 means that the service is disrupted, or $D^{A,ED}(p) \in [0, 1]$ representing the likelihood of the electricity delivery to the data center being disrupted. It is also possible for profile $D^{A,ED}$ to be identical to $D^{A,E}$, i.e., the mutually agreed predicted service disruption profile for the pair E–D may be the same as the internal predicted service disruption profile.

It should be noted that both the number and the lengths of time sub-periods Θ_p^{ET} and Θ_p^{ED} as well as the setup of information sets/vectors $D^{A,ET}(p)$ and $D^{A,ED}(p)$ can vary according to changing circumstances. For example, in the case of the pair E–T the first time subinterval Θ_0^{ET} could be assumed to be equal to five, ten or fifteen minutes, with $D^{A,ET}(0)$ representing the likelihood of a failure of the power supply during this period. At the same time the first subinterval Θ_0^{ED} may be set as equal to three up to twelve hours with $D^{A,ED}(0)$ containing a vector of numbers describing the predicted likelihood or the probability distribution of a breakdown of electricity supply over this subinterval.

3. Cyber threat related risk assessment versus global risk assessment

At this point another important issue has to be discussed. So far we have been concerned with the cyber related risk assessment; i.e., the primary sources of possible losses and disruptions of service availability (in the case of the DSP, like a data center, also confidentiality and integrity of data) were assumed to be threats to network and information security, that is to be the cyber related threats. However, let us assume now, referring to our example, that at a given time the power company operator calculates the MAPSDP (for the pair P–T, i.e., power company (supplier)–transport company (user)) while, for example, the estimated likelihood of a failure of power supply to the local railway network due to a possible cyber attack on the

power company SCADA system within next twelve hours (Θ_1^{ET}) is, say, equal to 0.1 (or 1 on a one-to-ten scale), i.e., it is very small. However, at the same time the actual very extreme weather conditions may result in a power supply breakdown during Θ_1^{ET} with the likelihood equal to 0.8 (or 8, i.e., high) on the same scale. Now, what information should be sent then to the railway network operator? It would seem rather strange to inform her/him that the likelihood of a power supply failure during Θ_1^{ET} is very small, as induced by the cyber threats only, while actually it is high due to other reasons.

The above dilemma can be solved by introducing and using simultaneously, for each pair of the related entities, two mutually agreed predicted service disruption profiles: the first MAPSDP$_{cyber}$ (or just MAPSDP) related only to cyber induced threats and ignoring risks related to other threats and the second MAPSDP$_{global}$ concerned with the general dynamic risk assessment involving all identifiable threats.

It may still be possible for a given entity to concentrate only on its internal cyber threats while taking into account both versions of MAPSDPs, i.e., MAPSDP$_{cyber}$ (MAPSDP) and MAPSDP$_{global}$, as provided by operators of those services on which this entity is dependent upon.

4. General approach to hierarchical dynamic national level risk assessment (HDNLRA): Iterated mutually agreed predicted service disruption profiles

Assume now that the current risk analysis, done at the Center level at time t_k, is concerned mainly with an assembly of service predicted disruption profiles for their clients, like, for example, $D^{A,H}(p)$ $p = 1, \ldots, P^H - 1$, representing information concerning the predicted status related to the availability of the future hospital services, and with the MAPSDPs related to all relevant service pairs, structured as service s (provider)—service g (user), involving future time intervals Θ^{sg}, each of them composed of a number of subintervals Θ_p^{sg}, where $p = 0, 1, \ldots, P^{sg} - 1$; i.e.,

$$\Theta^{sg} = \Theta_0^{sg} \cup \Theta_1^{sg} \cup \cdots \cup \Theta_{P^{sg}-1}^{sg}.$$

Let the information concerning the predicted possible disruption or degradation of service s affecting service g in terms of confidentiality (C), integrity (I) and availability (A), within subinterval Θ_p^{sg}, be defined as the triple

$$D^{CIA,sg}(p) = (D^{C,sg}(p), D^{I,sg}(p), D^{A,sg}(p)).$$

In the case when the discussed LE s is not a digital service provider, only the availability component $D^{A,sg}(p)$ of $D^{CIA,sg}(p)$ is relevant and may assume a nonzero value. In the simplest case this can be a real number, i.e., $D^{A,sg}(p) \in [0, 1]$ or a "likelihood" level belonging to set $\{1,2,\ldots,10\}$, and, likewise, for the remaining components of $D^{CIA,sg}(p)$. The mutually agreed predicted service disruption profile (MAPSDP) for the service pair *s–g* is then defined as

$$D^{CIA,sg} = (D^{CIA,sg}(p);\ p = 0, \ldots, P^{sg} - 1).$$

The current time, at which the iterative process to be described is to be performed, is associated with the beginning of the sub-interval Θ_0^{sg}.

Assume now that we allow for any risk assessment and forecasting method to be used at the local entity (LE) level, being possibly specialized for each service s, provided that this method is capable of performing the required risk assessment whilst using the internally observed or anticipated threats and vulnerabilities as well as the currently available MAPSDPs associated with all pairs *u–s*, such that the provision of service u is relevant to the operation of service s. The method must also be able to produce its own "output" MAPSDP (MAPSDP$_{cyber}$) and MAPSDP$_{global}$ for all relevant pairs *s–g*, associated with all services g that can be affected by disruption or degradation of service s. Further on in this paper we will not differentiate between MAPSDP$_{cyber}$ and MAPSDP$_{global}$, as both exclusively cyber threats related and global MAPSDPs can be iterated in the same way.

As stated above, assume now that at a given time we initiate the analysis that should provide an overall risk assessment, under current conditions, over the assembly of future time intervals Θ^{sg}, for all relevant pairs *s–g* of services, as defined above. At the Center level we may propose to adopt the iterative approach, following the concept of the interaction prediction method (Mesarović *et al.*, 1970).

One may begin with a set of initial MAPSDPs, for all pairs *s–g*. The initial profiles can be defined in, at least, three ways:

(a) all set to zero levels,

(b) resulting from local static risk assessment, based upon an audit of security protection of information system of a given entity,

(c) resulting from the analysis performed previously.

Case (a) refers to the initial assumption by each local entity that at the current time all relevant supporting services are supposed to be fully available over the defined intervals Θ^{sg}. This may be a rather optimistic assumption as there are always at least static levels of risk always present. In Case (b) those static risks are used to compute the MAPSDP profiles, possibly using the procedure described below. Actually, iterative static analysis at the Center level may be initiated with zero MAPSDP profiles

and then lead to computing the profiles resulting from local static risks. Case (c) would be a typical situation when the risk assessment is done repetitively on a periodic basis.

4.1. Coordination. Suppose then that we define the set of initial MAPSDP profiles, denoted as $D^{CIA,sg,(0)}$, for all relevant pairs *s*–*g*. This allows us to initiate the iterations, i.e., to start the coordination process.

At iteration i, where $i = 0, 1, 2, \ldots$, the set of MAPSDPs consisting of the actual profiles $D^{CIA,sg,(i)}$ for all pairs *s*–*g* is to be modified as follows. Let us define for each entity s the set of those entities on which this entity is dependent as U^s, while W^s is defined as the set of those entities that may be affected by the failure of service s. The profiles $D^{CIA,us,(i)}$ for $u \in U^s$ are used, together with all currently available information at the LE level (likelihoods of cyber threats, local vulnerabilities, observed incidents, etc.), to perform local risk analysis and, in particular, to compute at a given s-th service level a new value $D^{CIA,sg,(i),new}$ of the MAPSDP for each pair *s*–*g*, such that $g \in W^s$, i.e., to compute new predicted (output) profiles of entity s as perceived by this entity. After this local analysis is done by all entities and the information about the new "output" profiles $D^{CIA,sg,(i),new}$ computed by those entities is received at the Center, a suite of new predicted profiles $D^{CIA,sg,(i+1)}$ to be distributed and used for the next iteration $i + 1$ must be proposed by the Center. For this purpose many coordination algorithms can be used. The simplest of them is the direct re-injection strategy, whereby

$$D^{CIA,sg,(i+1)} := D^{CIA,sg,(i),new} \tag{4}$$

for all pairs *s*–*g*. In some cases it might be better to use the relaxation based, smoothing, algorithm for computing $D^{CIA,sg,(i+1)}$ as

$$\begin{aligned} D^{CIA,sg,(i+1)} := {} & \rho D^{CIA,sg,(i),new} \\ & + (1-\rho) D^{CIA,sg,(i)}, \end{aligned} \tag{5}$$

where $0 < \rho \leq 1$ is the relaxation coefficient; if $\rho = 1$ then (5) reduces to (4). In both the algorithms the substitutions are made component-wise.

The iterations are terminated when convergence is obtained with respect to all pairs, i.e., when $D^{CIA,sg,(i),new} \approx D^{CIA,sg,(i)}$ for all pairs *s*–*g*. The stopping criterion must be specified for each application of the above approach. For example, assuming that $D^{CIA,sg,(i)}$ is a vector of real numbers, a typical stopping criterion would be to require that

$$\| D^{CIA,sg,(i+1)} - D^{CIA,sg,(i),new} \| \leq \varepsilon_{sg},$$

where $\varepsilon_{sg} > 0$, for every pair *s*–*g*.

Other algorithms for iteration of MAPSDPs may be proposed, in particular when more information is received at each iteration by the Center, i.e., an additional information on top of the value of $D^{CIA,sg,(i),new}$, for example, information regarding the sensitivity of $D^{CIA,sg,(i),new}$ with respect to changes in the relevant profiles $D^{CIA,us,(i)}$, where $u \in U^s$. It can be expected, however, that in most practical cases such information will be not available and so the algorithm (4) or (5), or similar, will have to be used.

As noted above, the iterations defined by the coordination algorithm are performed until satisfactory convergence is obtained. It might happen that during those iterations, each of them taking some time, the information available at the LE level may change due to, for example, new incidents being observed or/and new vulnerabilities being identified. Then the iterative process as described above may be disturbed and the stopping criterion may be not satisfied. Also, time intervals Θ^{sg} can be modified between the iterations if there is a need to do so. It must be then assumed that the above iteration process would be in such circumstances perceived as an ongoing activity. Properties of this process should be examined in view of the relevant factors involved, in particular the details of the LE level analysis procedures and the dynamics of the changes concerned.

The MAPSDPs of key services may well represent crucial information at the Center level and may be used, in particular, for graphical threat presentation and for risk assessment (analysis) performed at this level, for example in a case when the Center can assign numerical values, e.g., in monetary units, to compute expected losses in view of those MAPSDPs.

An alternative, perhaps complementary, approach would be to use local risk evaluations (like Eqn. (10)) and, then sum them up (Eqn. (12)).

5. Example approach to risk analysis at the LE level

To complete the picture, consider now the risk assessment at the local entity level, leading, in particular, to the computation of MAPSDPs, being the "outputs" of a given entity s, while given as inputs predicted disruption profiles of the services this entity is dependent on. It should be stressed that the mechanism presented below is only an example. It is inspired by the risk assessment method at the institutional level proposed by Viduto *et al*. (2012). In fact, any approach to such assessment at the local level can be used and various entities may use different methods. The only requirement is that all methods should, as stated above, be compatible concerning mutually agreed time and information details as far as the usage of related MAPSDPs is concerned.

For the sake of simplicity assume first that we are

concerned here only with the availability component of the service profiles as being relevant to the functioning of other services being dependent upon this service and that data $D^{A,sg}(p)$ is just a single number describing the likelihood of service s availability disruption as affecting the entity g.

Let us assume that the information system of LEs suffers from a number of vulnerabilities (weaknesses) that can be exploited by a suite 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 entity considered. When this vulnerability is exploited, it impacts the service provided by LE s, which may be degraded or disrupted (service failure) within the subinterval Θ_p^{sg}, affecting a given service g; assume that this impact can be described by a number $I_v^{sg}(p)$. These impacts may be, in particular, expressed as Low, Medium or High, with appropriate numbers attached. These numbers may belong to interval [0,1] or be expressed on another scale, as, e.g., Very Low (0–4 or 0), Low (5–20 or 2), Moderate (21–79 or 5), High (80–95 or 8), Very High (96–100 or 10) as in the report by NIST (2012). The likelihood of vulnerability v being exploited may be described as related to possible cyber threats, where, say, threat j may affect the entity s when $j \in J^s$. With each threat it would be then required, while using this approach to the local risk assessment, to associate the level of the likelihood that this threat may exploit the vulnerability $v \in V^s$, namely, $L_{vj}^{A,sg}$, within subinterval Θ_p^{sg}.

In addition to these internal cyber threats it may happen that services external to the entity s, on which this entity is dependent, can be substantially degraded or disrupted for certain time periods, as discussed above. The set of those entities is U^s, while I_u^{sg} represents an impact of the failure of service u upon the service s affecting the entity g. The likelihood of service s to fail within the sub-interval Θ_p^{sg} and to affect the availability of service g can be then defined as

$$L^{A,sg}(p) = \sum_{v \in V^s} I_v^{sg}(p) \sum_{j \in J^s} L_{vj}^{sg}\, T_j^{sg}(p) + \sum_{z \in Z^{sg}(p)} \sum_{u \in U^s} I_u^{sg}(p) D^{A,us}(r_{sg,z}^{us}(p)), \tag{6}$$

where $p = 0, 1, \ldots, P^{sg}-1$ and the mapping $r = r_{sg,z}^{us}(p)$ indicates the subinterval Θ_r^{us} such that $D^{A,us}(r_{sg,z}^{us}(p))$ is relevant for the estimation of $L^{A,sg}(p)$. $Z^{sg}(p)$ is, for given p, the set of such relevant periods associated with pair *u–s*.

The threat activation function can be defined as

$$T_j^{sg}(p) = \begin{cases} 1 & \text{when threat } j \text{ is present} \\ & \text{within } \Theta_p^{sg}, \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

It is assumed that $L^{A,sg}(p)$ is dependent on the internal cyber threats associated with subinterval Θ_p^{sg} (the first term on the right hand side of (6)), while this likelihood may also depend upon the threat of possible disruptions of other services related properly to the appropriate future subintervals (the second term on the right hand side of (6)). It is possible, of course, to introduce a similar dependence of $L^{A,sg}(p)$ on earlier internal threat occurrences.

In the simplest case, the output disruption profile value $D^{A,sg}(p)$, related to service s affecting service g, may be defined as

$$D^{A,sg}(p) = \begin{cases} 1 & \text{when } L^{A,sg}(p) \geq L_{thres}^{A,sg}, \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

for $p = 0, 1, \ldots, P^{sg} - 1$.

Otherwise, as it seems also very natural, $D^{A,sg}(p)$ may be set as equal to $L^{A,sg}(p)$, assuming that $L^{A,sg}(p) \in [0, 1]$. One may then define the MAPSDP as

$$D^{A,sg}(p) = \min\left(1, L^{A,sg}(p)\right) \tag{9}$$

for $p = 1, \ldots, P^{A,sg} - 1$. A modified definition of $D^{A,sg}(p)$ may be appropriate when the service provider s becomes capable, as it should be expected, of restoring the service to normal or simply an acceptable level after some known recovery period. For example, assume that for a given p, $D^{A,sg}(p) = 1$, then $D^{A,sg}(l) = 0$ for $l \geq p + \mu^s$, even if $L^{A,sg}(p + \mu^s) \geq L_{thres}^{A,sg}$.

Similar formulas can be used to define and evaluate "internal" predicted service disruption profiles like given by (1) in the case of the hospital services.

Risk evaluation at the local level can be related both to the possibility of service s entering the failure mode and to the individual impacts of the local vulnerabilities exploited on the performance of the information system of this entity. The risk formulas may be proposed, for example, as follows:

$$R^s(p) = \tilde{I}_s^s\, D^{A,s}(p) + \sum_{g \in W^s} \tilde{I}_s^{sg} D^{A,sg}(p), \tag{10}$$

where $\tilde{I}_s^s$ denotes the internal (perceived internally) impact of possible failure of service s and $\tilde{I}_s^{sg}$ denotes the impact of the failure of service s on the g-th service operator. Remember that W^s is defined as the set of those entities that may be affected by the failure of service s.

It should be noted that the computation of the second term in (10), i.e., the external consequences of the failure of service s on other entities, that is,

$$\sum_{g \in W^s} \tilde{I}_s^{sg} D^{A,sg}(p), \tag{11}$$

may be transferred to the Center or to the concerned entities themselves; this would be in fact necessary in the

case when the s -th LE is not able to determine the values of impact factors $\tilde{I}_s^{sg}$ for $g \in W^s$.

It can be observed immediately that we need to know the disruption profiles of services affecting LE s to compute $L^{A,sg}(p)$ (Eqn. (6)) and the disruption functions of services depending upon this service to compute $R^s(p)$ (Eqn. (10)), for $p = 0, 1, \ldots, P^s - 1$, and $D^{A,sg}(p)$ may be computed (Eqns. (8) or (9)) only after $L^{A,sg}(p)$ is known. Therefore, for computing $L^{A,sg}(p)$ from (6), and, when needed, $R^s(p)$ from (10), at iteration i of the center level coordination step one should use $D^{A,us,(I)}$, while $D^{A,sg}(p)$ computed then from Eqn. (8) or from Eqn. (9) becomes a component of $D^{A,(i),new}$.

5.1. Data services providers. Consider now the s-th LE to be data services provider. Then the likelihood of failure, as defined by (6), can be a vector with components related to confidentiality $L^{C,sg}(p)$, integrity $L^{I,sg}(p)$ and availability $L^{A,sg}(p)$. The disruption profile has then components $D^{C,sg}(p)$, $D^{I,sg}(p)$ and $D^{A,sg}(p)$. In such a case impact factors I_v^{sg} and I_u^{sg} will be, respectively, vectors and matrices.

6. Coordination

After CNT considers the coordination terminated, it may then compute the required risk estimates at this level, in particular using the formulas

$$R(p) = \sum_{s \in S} R^s(p), \tag{12}$$

where $R^s\,(t)$ is computed at the local level from Eqn. (10) or both at the local and the central level (Eqns. (10) and (11)) and S is the set of the entities (services) considered.

The convergence of the coordination process should be examined. The best known sufficient condition to assure it is the absolute weighted dominance of the main diagonal in the Jacobian matrix resulting from the set of equations (6) for $p = 0, 1, \ldots, P^{sg} - 1$ (Frommer, 1991). It may be also useful to provide a choice of a proper value of the relaxation coefficient ρ when using the algorithm (5) or for choosing, if possible, an even more efficient coordination strategy (Bertsekas and Tsitsiklis, 1989).

6.1. Coordination under changing local estimates of local factors. Now consider the situation, which may happen to be more realistic, when some of the actual factors are updated, when appropriate, at the local level, at subsequent iterations of the coordination routine. This concerns parameters such as vulnerabilities, threats, likelihoods L_{vj}^{sg} and impact values as well as time delays used in the local risk analyses. Then this routine becomes an ongoing process, providing for continuously adjusting the dynamical risk assessment at the Center level. It would be of interest to study the dependence of such an assessment on both the convergence characteristics of the coordinating strategy and on the dynamics of on-line changes in the multiple data used. Assuming, from the point of view of the convergence analysis, that the evolution of parameter values over time can be modeled as sequences of random quantities, the coordination process can be then viewed as a stochastic approximation process.

Remark 1. The likelihood of the s-th service failure affecting service g, as given by (6), may be bounded from above in order to make that indicator better aligned and therefore easier to compare with those of other entities. In this case (6) can be modified as follows:

$$\begin{aligned} L^{A,sg}(p) &= \max\Bigg[L^{A,sg}_{\max}(p), \sum_{v \in V^s} I_v^{sg}(p) \sum_{j \in J^s} L_{vj}^{sg}\, T_j^{sg}(p) \\ &\quad + \sum_{z \in Z^{sg}(p)} \sum_{u \in U^s} I_u^{sg}(p) D^{A,us}\left(r^{us}_{sg,z}(p)\right)\Bigg]. \end{aligned} \tag{13}$$

Remark 2. The above hierarchical approach to perform risk assessment can be extended to the case when the Center may recommend specified risk mitigation actions, especially when the global resources required for such actions are limited and have to be allocated in the most efficient way.

7. Example of a four-entity system

To better illustrate the ideas introduced above and the coordination strategies, let us come back to the previously introduced four-entity system consisting of the power company (E), the transport company (T), the hospital (H) and the data center (D) (see Fig. 2). Assume that in the case of each entity s and each relevant pair of the entities s–g we consider the predicted disruption profile components concerned with service availability $D^{A,s}(p)$ and $D^{A,sg}(p)$, for every possible value of p, as defined in (9), where

$$D^{A,sg}(p) = \min\left(1, L^{A,sg}(p)\right) \tag{14}$$

for $p = 1, \ldots, P^{A,sg} - 1$ and $D^{A,sg}(p) \in [0, 1]$.

In all cases of the example entities considered it is assumed that the formulas given by (6) are used together with (14) to compute the predicted service disruption profiles, while the first term in (6), related to internally assessed threats, is represented by a given number. The process of risk analysis at the local level is not detailed.

Now let us start with the electricity company (E) and assume the following timing and formulas defining the relevant profiles, assuming that we differentiate between the case with cyber related threats only (CT) and the case

where we consider global threats, in particular related to cyber and weather issues (GT):

$\boldsymbol{D^{A,ET}(p),\ p=0,1,2;}$

$$\Theta^{ET}=[0,5\text{ min}]\cup[5\text{ min},\ 12\text{ h}]\cup[12\text{ h},\ 72\text{ h}],$$
$$L^{A,ET}(0)=0.02\quad(CT),$$
$$L^{A,ET}(1)=0.1\quad(CT),$$
$$L^{A,ET}(2)=0.07+0.2\cdot D^{A,TE}\left(0=r^{TE}_{ET,1}(2)\right)+0.5\cdot\ D^{A,TE}\left(1=r^{TE}_{ET,2}(2)\right)\quad(CT),$$

and

$$L^{A,ET}_{global}(0)=0.1\quad(GT),$$
$$L^{A,ET}_{global}(1)=0.5\quad(GT),$$
$$L^{A,ET}_{global}(2)=0.3+0.2\cdot D^{A,TE}_{global}\left(0=r^{TE}_{ET,1}(2)\right)+0.4\cdot D^{A,TE}_{global}\left(1=r^{TE}_{ET,2}(2)\right)\quad(GT);$$

$\boldsymbol{D^{A,ED}(p),\ p=0,1;}$

$$\Theta^{ED}=[0,\ 12\text{ h}]\cup[12\text{ h},\ 72\text{ h}],$$
$$L^{A,ED}(0)=0.05\quad(CT),$$
$$L^{A,ED}(1)=0.03+0.2\cdot D^{A,TE}\left(0=r^{TE}_{ED,1}(1)\right)+0.4\cdot D^{A,TE}\left(1=r^{TE}_{ED,2}(1)\right)\quad(CT),$$

and

$$L^{A,ED}_{global}(0)=0.5\quad(GT),$$
$$L^{A,ED}_{global}(1)=0.2+0.1\cdot D^{A,TE}_{global}\left(0=r^{TE}_{ED,1}(1)\right)+0.4\cdot D^{A,TE}_{global}\left(1=r^{TE}_{ED,2}(1)\right)\quad(GT);$$

$\boldsymbol{D^{A,EH}(p),\ p=0,1,2;}$

$$\Theta^{EH}=[0,3\text{ h}]\cup[3\text{ h},\ 12\text{ h}]\cup[12\text{ h},\ 72\text{ h}],$$
$$L^{A,EH}(0)=0.1\quad(CT),$$
$$L^{A,EH}(1)=0.15\quad(CT),$$
$$L^{A,EH}(2)=0.12+0.3\cdot D^{A,TE}\left(1=r^{TE}_{EH,1}(2)\right)\quad(CT),$$

and

$$L^{A,EH}_{global}(0)=0.5\quad(GT),$$
$$L^{A,EH}_{global}(1)=0.8\quad(GT),$$
$$L^{A,EH}_{global}(2)=0.3+0.6\cdot D^{A,TE}_{global}\left(1=r^{TE}_{EH,1}(2)\right)\quad(GT);$$

$\boldsymbol{D^{A,E}(p),\ p=0,1,2;}$

$$\Theta^{E}=[0,3\text{ h}]\cup[3\text{ h},\ 12\text{ h}]\cup[12\text{ h},\ 72\text{ h}],$$
$$D^{A,E}(p)=D^{A,ET}(p),\ p=0,1,2;$$

i.e., the internal profile $D^{A,E}=D^{A,ET}$ and $\Theta^{E}=\Theta^{ET}$. Then define relevant likelihood and disruption profiles of the other services.

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

$\boldsymbol{D^{A,TE}(p),\ p=0,1;}$

$$\Theta^{TE}=[0,\ 24\text{ h}]\cup[24\text{ h},\ 72\text{ h}],$$
$$L^{A,TE}(0)=0.05+0.2\cdot D^{A,ET}\left(0=r^{ET}_{TE,1}(0)\right)+0.1\cdot D^{A,DT}\left(1=r^{DT}_{TE,1}(0)\right)+0.4\cdot D^{A,ET}\left(1=r^{ET}_{TE,2}(0)\right)\quad(CT),$$
$$L^{A,TE}(1)=0.08+0.7\cdot D^{A,ET}\left(2=r^{ET}_{TE,1}(1)\right)\quad(CT),$$

and

$$L^{A,TE}_{global}(0)=0.4+0.2\cdot D^{A,ET}_{global}\left(0=r^{ET}_{TE,1}(0)\right)+0.1\cdot D^{A,DT}_{global}\left(1=r^{DT}_{TE,1}(0)\right)+0.4\cdot D^{A,ET}_{global}\left(1=r^{ET}_{TE,2}(0)\right)\quad(GT),$$
$$L^{A,TE}_{global}(1)=0.6+0.2\cdot D^{A,ET}_{global}\left(2=r^{ET}_{TE,1}(1)\right)\quad(GT),$$

$\boldsymbol{D^{A,T}(p),\ p=0,1;}$

$$\Theta^{T}=[0,\ 24\text{ h}]\cup[24\text{ h},\ 72\text{ h}]$$

and $D^{A,T}=D^{A,TE}$.

The likelihoods and profiles of data center (D) are specified as

$\boldsymbol{D^{A,DH}(p),\ p=0,1,2;}$

$$\Theta^{DH}=[0,3\text{ h}]\cup[3\text{ h},\ 12\text{ h}]\cup[12\text{ h},\ 72\text{ h}],$$
$$L^{A,DH}(0)=0.1\quad(CT),$$
$$L^{A,DH}(1)=0.7+0.1\cdot D^{A,ED}\left(0=r^{ED}_{DH,1}(1)\right)\quad(CT),$$
$$L^{A,DH}(2)=0.7+0.3\cdot D^{A,ED}\left(1=r^{ED}_{DH,1}(2)\right)\quad(CT),$$

and

$$L^{A,DH}_{global}(0)=0.2\quad(GT),$$
$$L^{A,DH}_{global}(1)=0.1+0.2\cdot D^{A,ED}_{global}\left(0=r^{ED}_{DH,1}(1)\right)\quad(GT),$$
$$L^{A,DH}_{global}(2)=0.1+0.4\cdot D^{A,ED}_{global}\left(1=r^{ED}_{DH,1}(2)\right);\quad(GT),$$
$$D^{A,DT}=D^{A,DH},\quad D^{A,D}=D^{A,DH};$$

Finally, for the hospital (H) we define the likelihoods and disruption profile as

$\boldsymbol{D^{A,H}(p),\ p=0,1,2;}$

$$\Theta^{H}=[0,3\text{ h}]\cup[3\text{ h},\ 12\text{ h}]\cup[12\text{ h},\ 72\text{ h}],$$
$$L^{A,H}(0)=0.15+0.2\cdot D^{A,EH}\left(0=r^{EH}_{H,1}(0)\right)$$

$$+0.15 \cdot D^{A,DH}\left(0 = r_{H,1}^{DH}(0)\right) \quad (CT),$$

$$L^{A,H}(1) = 0.15 + 0.2 \cdot D^{A,EH}\left(1 = r_{H,1}^{EH}(1)\right)$$
$$+0.2 \cdot D^{A,DH}\left(1 = r_{H,1}^{DH}(1)\right) \quad (CT),$$
$$L^{A,H}(2) = 0.2 + 0.6 \cdot D^{A,EH}\left(2 = r_{H,1}^{EH}(2)\right) \quad (CT),$$

and

$$L_{global}^{A,H}(0) = 0.4 + 0.05 \cdot D_{global}^{A,EH}\left(0 = r_{H,1}^{EH}(0)\right)$$
$$+0.3 \cdot D_{global}^{A,DH}\left(0 = r_{H,1}^{DH}(0)\right) \quad (GT),$$
$$L_{global}^{A,H}(1) = 0.3 + 0.3 \cdot D_{global}^{A,EH}\left(1 = r_{H,1}^{EH}(1)\right)$$
$$+0.1 \cdot D_{global}^{A,DH}\left(1 = r_{H,1}^{DH}(1)\right) \quad (GT),$$
$$L_{global}^{A,H}(2) = 0.2 + 0.5 \cdot D_{global}^{A,EH}\left(2 = r_{H,1}^{EH}(2)\right) \quad (GT).$$

It can be seen that both the number of time periods and their duration vary between different profiles, while it is assumed that the overall time horizon is equal to 72 hours.

The objective now is to demonstrate the coordination process at the central level, for both cyber threats related analysis (CT) and the analysis where we consider other threats, in particular related to cyber and weather issues (GT), while using the coordination strategy (5) with various relaxation coefficients.

The results of computations when the direct re-injection strategy (4) ($\rho = 1$ in algorithm (5)) was used are presented in Figs. 3–8. For the termination condition $\varepsilon_{sg} = 10^{-6}, sg \in \{ET, ED, EH, TE, DH, DT\}$ we needed 24 iterations to obtain the convergence in the case of cyber disruption profiles and 14 iterations in the case of global ones.

It can be observed that, as it was described in Section 2, 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 in few hours we can see the same effect for the data center and the hospital. Since the disruption of power supply prolongs over next days, both global and cyber threats remain on higher levels for all services.

The results of computations of the $D^{A,TE}$ profile (for other profiles we observed the same effects) when the relaxation strategy was used are presented in Fig. 9. We used $\rho = 0.5$ in the algorithm (5). 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 $\varepsilon_{sg} = 10^{-6}, sg \in \{ET, ED, EH, TE, DH, DT\}$ the calculations took more time: to obtain the convergence in the case of cyber disruption profiles 50 iterations were needed and in the case of global profiles 34 iterations were required.

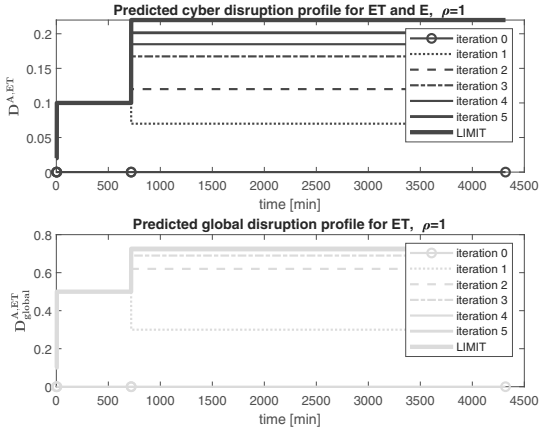

Fig. 3. Predicted disruption profiles between the power plant (E) and the transport company (T) as well as for the power company itself when the direct re-injection strategy was used.

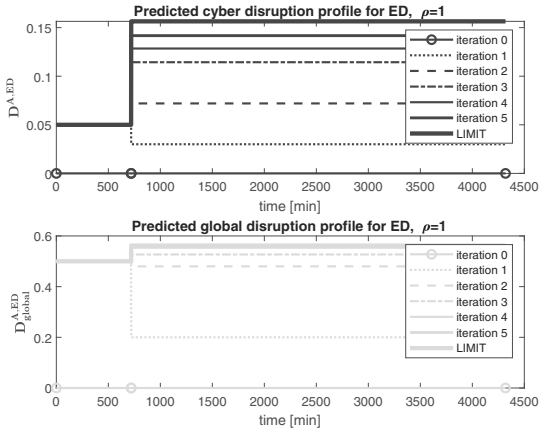

Fig. 4. Predicted disruption profiles between the power plant (E) and the data center (D) when the direct re-injection strategy was used.

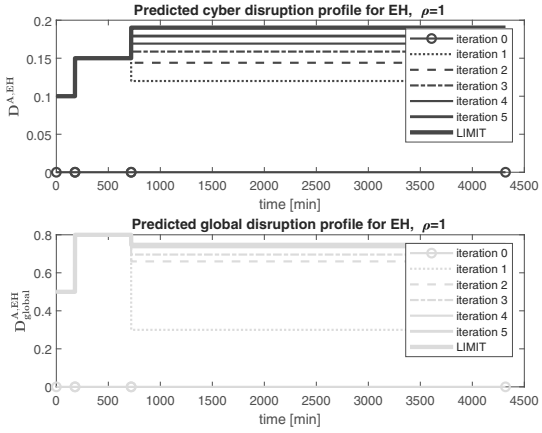

Fig. 5. Predicted disruption profiles between the power plant (E) and the hospital (H) when the direct re-injection strategy was used.

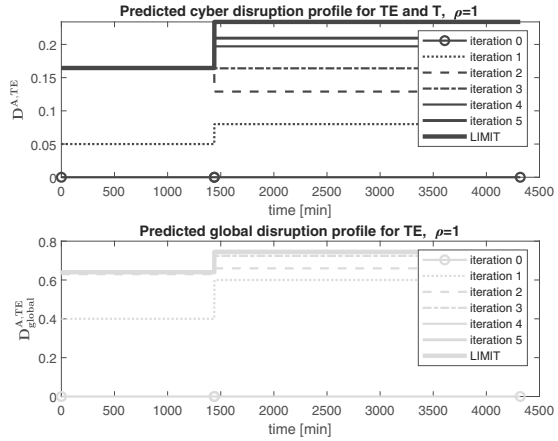

Fig. 6. Predicted disruption profiles between the transport company (T) and the power plant (E) as well as for the transport company itself when the direct re-injection strategy was used.

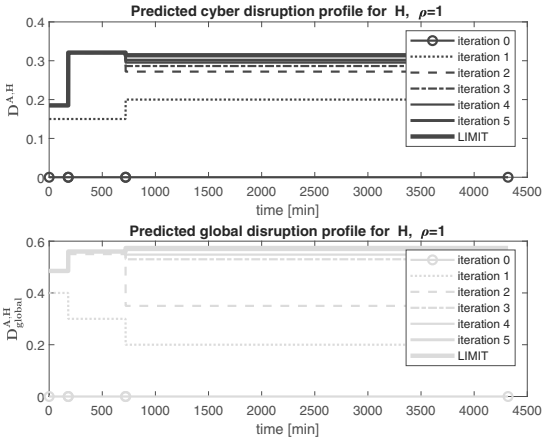

Fig. 8. Predicted disruption profiles of the services delivered by the hospital (H) when the direct re-injection strategy was used.

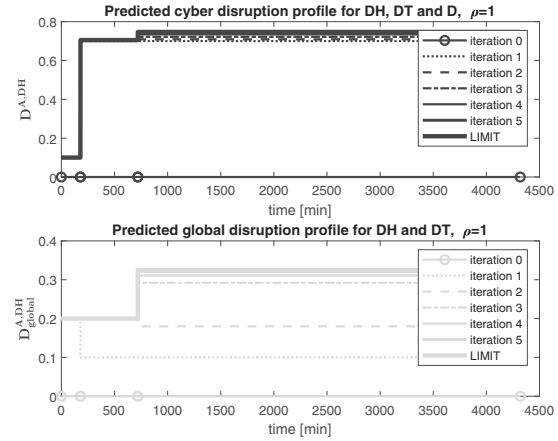

Fig. 7. Predicted disruption profiles between the data center (D) and both the hospital (H) and the transport company (T) as well as and for the data center itself when the direct re-injection strategy was used.

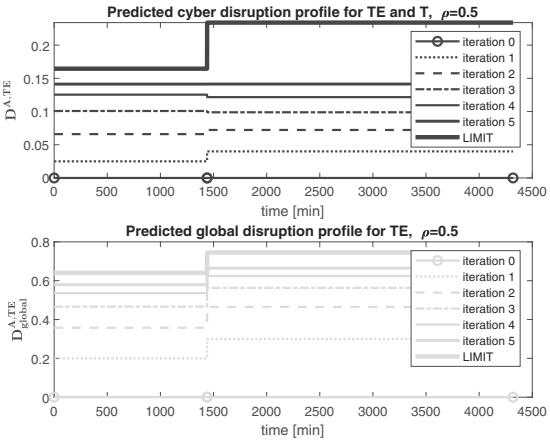

Fig. 9. Predicted disruption profiles between the transport company (T) and the power plant (E) as well as for the transport company itself when the relaxation algorithm with $\rho = 0.5$ was used.

8. Conclusions

We proposed a hierarchical on-line scheme for 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 above hierarchical approach to perform the risk assessment can be extended to the case when the Center may recommend specified risk mitigation actions, especially when the global resources required for such actions are limited and have to be allocated in the most efficient way.

The proposed approach to the risk analysis at the central (national or district) level requires investigation of several aspects. The main task would be to develop a real life case study (studies) involving a number of operators of existing key services, possessing and using their own risk analysis tools, and then to find and examine a procedure for defining relevant predicted service disruption profiles, and, finally, to try various coordination strategies.

Another important aspect, mentioned only in this paper, is to consider time variability of local analyses, especially when the changes in local risk factors (threats, vulnerability impacts, etc.) occur during the coordination of PSDPs and MAPSDPs.

Acknowledgment

This work was done as part of the CYBERSECIDENT/369195/I/NCBR/2017 project supported by the National Center of Research and Development in Poland in the framework of the CyberSecIdent Programme.

References

Bertsekas, D. and Tsitsiklis, J. (1989). *Parallel and Distributed Computation: Numerical Methods*, Prentice Hall, Englewood Cliffs, NJ.

EU (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of the European Union of 6 July 2016 concerning measures for a high common level of security of network and information systems across the union, *Official Journal of the European Union* **59**: L194/1–L194/30.

ENISA (2013). National-level risk assessments an analysis report—Executive summary, *Technical report*, European Union Agency for Network and Information Security, Heraklion.

Findeisen, W., Bailey, F.N., Brdyś, M., Malinowski, K., Tatjewski, P. and Woźniak, A. (1980). *Control and Coordination in Hierarchical Systems*, Wiley, Chichester.

Frommer, A. (1991). Generalized nonlinear diagonal dominance and applications to asynchronous iterative methods, *Journal of Computational and Applied Mathematics* **38**(1): 105–124.

Haimes, Y. (2016). *Risk Modeling, Assessment, and Management (4th Edition)*, Wiley, Hoboken, NJ.

Haimes, Y., Santos, J., Crowther, K., Henry, M., Lian, C. and Yan, Z. (2007). Risk analysis in interdependent infrastructure, *in* E. Goetz and S. Shenoi (Eds), *Critical Infrastructure Protection*, Springer, Boston, MA, pp. 297–310.

Kalantarnia, M., Khan, F. and Hawboldt, K. (2009). Dynamic risk assessment using failure assessment and Bayesian theory, *Journal of Loss Prevention in the Process Industries* **22**(5): 600–606.

Karbowski, A., Malinowski, K., Szwaczyk, S. and Jaskóła, P. (2019). Critical infrastructure risk assessment using Markov chain model, *Journal of Telecommunications and Information Technology* **2019**(2): 15–20.

Khan, F., Hashemi, S.J., Paltrinieri, N., Amyotte, P., Cozzani, V. and Reniers, G. (2016). Dynamic risk management: A contemporary approach to process safety management, *Current Opinion in Chemical Engineering* **14**: 9–17.

Kołodziej, J. and Xhafa, F. (2011). Modern approaches to modeling user requirements on resource and task allocation in hierarchical computational grids, *International Journal of Applied Mathematics and Computer Science* **21**(2): 243–257, DOI: 10.2478/v10006-011-0018-x.

König, S., Schaberreiter, T., Rass, S. and Schauer, S. (2019). A measure for resilience of critical infrastructures, *in* E. Luiijf *et al.* (Eds), *Critical Information Infrastructures Security*, Springer, Cham, pp. 57–71.

Lian, C. and Haimes, Y.Y. (2006). Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input–output model, *Systems Engineering* **9**(3): 241–258.

López, Pastor, D. and Villalba, L.J.G. (2013). Dynamic risk assessment in information systems: State-of-the-art, *Proceedings of the 6th International Conference on Information Technology (ICIT 2013), Amman, Jordan,* pp. 1–9.

Malinowski, K. and Karbowski, A. (2019). Hierarchical on-line risk assessment at national level, *International Conference on Military Communications and Information Systems (ICMCIS 2019), Budva, Montenegro*, pp. 1–5.

Mesarović, M., Macko, D. and Takahara, Y. (1970). *Theory of Multi-Level Hierarchical Systems*, Academic Press, New York, NY.

Naumov, S. and Kabanov, I. (2016). Dynamic framework for assessing cyber security risks in a changing environment, *Proceedings of the 2016 International Conference on Information Science and Communication Technologies (ICISCT 2016), Tashkent, Uzbekistan,* pp. 1–4.

NIST (2012). Guide for conducting risk assessments, information security, NIST special publication 800-30, Revision 1, *Technical report*, US Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD.

Poolsappasit, N., Dewri, R. and Ray, I. (2012). Dynamic security risk management using Bayesian attack graphs, *IEEE Transactions on Dependable and Secure Computing* **9**(1): 61–74.

Rausand, M. (2011). *Risk Assessment; Theory, Methods, and Applications*, Wiley, Hoboken, NJ.

Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., Boettinger, K., Gall, M., Brost, G., Ponchel, C., Haustein, M., Kaufmann, H., Theuerkauf, K. and Olli, P. (2017). A collaborative cyber incident management system for European interconnected critical infrastructures, *Journal of Information Security and Applications* **34**(2): 166–182.

Skopik, F., Settanni, G. and Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing, *Computers & Security* **60**: 154–176.

Szwed, P. and Skrzyński, P. (2014). A new lightweight method for security risk assessment based on fuzzy cognitive maps, *International Journal of Applied Mathematics and Computer Science* **24**(1): 213–225, DOI: 10.2478/amcs-2014-0016.

Viduto, V., Maple, C., Huang, W. and López-Peréz, D. (2012). A novel risk assessment and optimization model for a multi-objective network security countermeasure selection problem, *Decision Support Systems* **53**(3): 569–610.

Zhang, Q., Zhou, C., Xiong, N., Qin, Y., Li, X. and Huang, S. (2016). Multimodel-based incident prediction and risk assessment in dynamic cybesecurity protection for industrial control systems, *IEEE Transactions on Systems, Man and Cybernetics* **46**(10): 1426–1444.

Zwikael, O. and Smyrk, J. (2019). *Project Management: A Benefit Realisation Approach*, Springer, Cham.

Krzysztof Malinowski, DSc, PhD, MEng, is a professor of technical sciences and a *professor emeritus* of control and information engineering at the Warsaw University of Technology. He has once held the position of the director for research of NASK and of the NASK CEO. He is the author or a co-author of four books and over 160 journal and conference papers. For many years he had been involved in research on hierarchical control and management methods. Professor Malinowski is a member of the Polish Academy of Sciences.

Andrzej Karbowski received his PhD (1990) and DSc (2012) in automatic control and robotics from the Warsaw University of Technology, Faculty of Electronics and Information Technology. Currently he is an associate professor at the Institute of Control and Computation Engineering of the Warsaw University of Technology and at the Research and Academic Computer Network (NASK). He is the editor and a co-author of two books (on parallel and distributed computing), the author and a co-author of two e-books (on grid computing and optimal control synthesis), as well as over 130 journal and conference papers. His research interests concentrate on optimal control, data networks management, cybersecurity, decomposition and parallel implementation of optimization algorithms.

Received: 27 December 2019
Revised: 1 June 2020
Accepted: 5 June 2020