

Ostrowska, Teresa

## Article

# The resource hazards model for the critical infrastructure of the state emergency management process

Foundations of Management

## Provided in Cooperation with:

Faculty of Management, Warsaw University of Technology

*Suggested Citation:* Ostrowska, Teresa (2013) : The resource hazards model for the critical infrastructure of the state emergency management process, Foundations of Management, ISSN 2300-5661, De Gruyter, Warsaw, Vol. 5, Iss. 3, pp. 49-60, <https://doi.org/10.2478/fman-2014-0019>

This Version is available at:

<https://hdl.handle.net/10419/184561>

### Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

### Terms of use:

*Documents in EconStor may be saved and copied for your personal and scholarly purposes.*

*You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.*

*If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.*



<https://creativecommons.org/licenses/by-nc-nd/3.0>

## THE RESOURCE HAZARDS MODEL FOR THE CRITICAL INFRASTRUCTURE OF THE STATE EMERGENCY MANAGEMENT PROCESS

Teresa OSTROWSKA

Faculty of Management, Warsaw University of Technology, Warsaw, Poland  
e-mail: t.ostrowska@wz.pw.edu.pl

**Abstract:** This paper presents an investigation of the relevant factors related to the construction of a resource model which is designed to be useful in the management processes of the operation of critical infrastructure (CI) for state emergencies. The genesis of the research lay in the perceived need for effective protection of multidimensional CI methodologies, and it was influenced by the nature of the physical characteristics of the available resources. It was necessary to establish a clear structure and well defined objectives and to assess the functional and structural resources required, as well as the potential relational susceptibilities deriving from a number of possible threats and the possible seriousness of a specific range of incidents and their possible consequences. The interdependence of CI stocks is shown by the use of tables of resource classes. The dynamics of the interaction of CI resources are modeled by examining how using clusters of potential risks can at any given time create a class of compounds related to susceptibilities and threats to the resources. As a result, the model can be used to conduct multi-dimensional risk calculations for crisis management CI resource configurations.

**Keywords:** resource, resource features, class of resources, threats and susceptibilities of the class of resource, critical infrastructure system (CI system), positioning resources of CI, hazards cluster.

### 1 Introduction - the genesis

*(...) We assume every day the right to freedom, knowledge and security - not necessarily realizing this fact. Human work related to the environment has accumulated many cultural resources over a number of centuries, including such modern resources such as power plants, banks, universities, insurance, health care, computer networks, databases, plastic cards of various types, markets, subway stations, gas stations ... these are apparently endless, but in fact they are countable sets of surrounding resources, services and opportunities. This is due to the diversity of resources that can be organized in a related administrative infrastructure territorial state (...) [1].*

Part of this infrastructure, which is created to ensure the safety of human life, is known as critical infrastructure (CI)<sup>1</sup>, and can be systematically encapsulated

in specific physical and methodical protection. The purpose of physical protection is to ward off internal and external threats<sup>2</sup> in order to isolate structural and functional CI. The purpose of carrying out methodical systematic risk estimations and the maintenance of CI resources was to assess threats and susceptibilities and to prevent and minimize the level of a single incident, a group of incidents and incidents that turned into a crisis. In the following discussion the focus is placed mainly on methodical protection.

The Act of 26 April 2007 on crisis management, hereinafter referred to as the *Act*, imposes an obligation to draw up plans and reports on national security. One of the most important reports is the report on threats to national security developed to the requirements of the *National Crisis Management Report*<sup>3</sup>, hereinafter referred to as the *Report*, wherein

<sup>1</sup> The Act of 26 April 2007 on crisis management (Journal of Laws of 2013 pos. 1166) defines critical infrastructure (CI) as follows: "Art 3 Whenever in this Act: (...) 2) critical infrastructure - should be understood as systems and their constituent functionally interrelated objects, including building structures, equipment, installations, services essential to the security of the state and its citizens required to ensure the smooth functioning of the public administration, as well as institutions and entrepreneurs. Critical infrastructure includes: a) the supply of energy, raw materials and energy consumption, b) communication, c) ICT networks, d) the financial, e) the provision of food, f) water supply, g) the protection

*of health, h) transport i) rescue, j) ensuring the continuity of the public administration, k) the production, storage, handling and use of chemicals and radioactive materials, including pipelines containing hazardous substances (...)."*

<sup>2</sup> The threat is a phenomenon caused by the interaction of human, material objects or phenomena, leading to increased risk of adverse events, and in the case of a significant worsening of their well, to an emergency.

<sup>3</sup> Council of Ministers of 30 April 2010 on the report of threats to national security (Journal of Laws of 2010 No. 83, item. 540).

the coordination of the preparation is provided by the Director of the Government Security Centre (GSC)<sup>4</sup>.

The main objectives of the *Report* are to identify the most important national security threats and assess their risks. The document contains strategic objectives and projects that should be implemented in order to minimize the possibility of hazards and their effects.

After analyzing all of the information in the *Report*, it appears to be necessary to develop a model of CI information for possible risks in order to provide a single, multi-dimensional and objective description of them. Model information risks CI could be used to support decision-making in crisis management. Information Model CI threats could also be useful for the construction of the so-called system of methodical CI resource protection, as they cover all the stages of crisis management, including:

- collection and aggregation of operational data about the state of the CI,
- analyzing and reporting the status of threats to the CI,
- operational management of a crisis,
- planning and strategic management to ensure the safety of the state.

## 2 Purpose and structure of the research

To make methodical resource protection IK possible, it is necessary to conduct systematic modeling and analysis of the structural-functional compounds which appear in a CI and its environment. For this purpose, the administrative structure of the state creates a virtual network of nodes and relationships administrative, whose task is to monitor the resources required for CI, on the basis of systematic analyses of threats, susceptibilities and risks of impacts (events). Virtual nodes are divided into: operational nodes (representing physically separate resources CI), intermediate nodes corresponding to the administrative structure of the state (municipalities, counties, provinces) and the central node.

In order to test the effectiveness of methodical protection, it is necessary to prepare a unified conceptual and algorithmic apparatus which can be used to:

- describe the dynamics of the characteristics of resource sharing in relation to the characteristics of risks and susceptibilities in the nodes of the operating networks,
- calculate the potential risks and potential susceptibilities in the operational, intermediate and central nodes,
- calculation of the risk of incidents, groups of incidents and crisis events,
- build a simulation model of a virtual network of nodes and links to assess various administrative issues, in order to monitor and consolidate the characteristics of the potential risks and potential susceptibilities of online network nodes,
- build a model of decision-making for virtual networks of nodes and create administrative links which are capable of supporting hierarchical decision-making CI administrators in the minimization of the risk of incidents and the liquidation of the consequences of their occurrence.

The main objective of the study is to prepare a methodology for assessing the risk of a crisis, in particular the destruction or disruption of CI. During a detailed analysis of risk assessment issues emergencies, one of the most difficult problems turned out to be developing comprehensive procedures that:

- enable the collection, aggregation and processing of data about threats in all the distinguished systems of CI,
- take into account the interaction of the threats posed by CI and their consequences in the form of a domino effect in the relationship between CIs and CI relationships with the environment,
- allow for modeling and generating forecast threats which may be spread in internal and external CI environments,
- are consistent methodically at all levels of crisis management CI,
- can be used for the development of planning documents and reports of research internships for crisis management CI.

In order to achieve this objective, there needs to be:

- an assumption that the areas of critical infrastructure are created by class resources that are vulnerable to threats from other resources and are themselves a threat to the resources in their environment,

<sup>4</sup> The Act of 26 April 2007 on crisis management (Journal of Laws of 2007 No. 89, item. 509, Art. 5a).

- a listing of the characteristics of the classes of resources on the basis of their susceptibility, and of the risk they create for the CI resources of their surroundings and the proposed positioning of the resources in time and space, taking into account the geographical distribution of resources and their destructive effects on other resources, as the threats and, consequently, the risks depend on the configuration of resources and their potential impact.

In order to develop comprehensive crisis management tools, CI is necessary to formulate guidelines to construct a model based on dynamically developing interactions (incidents) within and between CIs. It was assumed that the proposed model would be based on the decomposition of CI resources, taking into account the correlation (coincidence and synergy) of the relationship between CIs in the event of a threat. Such an approach should enable the modeling and analysis of the spread of incidents in and between CIs, and may be relevant to the overall assessment of the risk of a crisis in a functioning CI.

A model based on dynamically developing interactions (events) between CI resource approach was applied [7], involving the decomposition of CI in clearly distinguishable classes of stocks including:

- proposed repertoires characteristics (attributes) of resources,
- the criteria for the selection of the characteristics of resources,
- proposed principles of mutual positioning of resources in the CI, which are important to indicate the impact of a full or partial loss of the resources to threats in other resources belonging to CI.

This approach allows for the identification and assessment of susceptibilities and threats to CIs, the identification and analysis of interdependencies of a geographic nature, and between CI systems. It is anticipated that the model will be used to prepare the system at any level of crisis management to enable the collection of operational data about the state of CI, the aggregation of the data collected and the analysis and to report the status of threats and emergencies related to CI.

In work is intended to:

- present selected elements of the theory of resources (Section 3), as a basis for the interpretation of the classes and the critical infrastructure of resources,
- clarify the concept of CI and the CI system (Section 4),

- formulate guidelines for the construction of a CI model, assuming that CIs are created by class resources that are vulnerable to threats from other resources and are themselves a threat to the resources in their environment,
- identify the characteristics of the classes of resources offered by the specification of the characteristics of their susceptibility to hazards and dangers,
- propose the positioning of resources in time and space by taking into account the geographical distribution of resources and timing their destructive impacts on other resources, assuming that the consequent risk depends on the configuration of resources and timing of their interactions,
- specify an initial proposal for a repertoire of attributes that can be harmonized for all critical infrastructures, which would allow the development and use of the same tools for collecting operational data, the reporting and aggregation of data and the conduct of analytical and decision support.

### 3 Elements of the theory of resources

The concept of a resource is regarded as a universal term, in the place of which the name of the highlighted item (real or abstract) of the modeled reality is substituted. A resource can be “something” or “someone”. Resources can have a structure can be described as a set of attributes (features) which overlap between specific compounds. It is possible to specify the class of resources to which they belong and the sets of attributes of their individual values for each resource belonging to their specific class. The analysis conducted in this part of the article reflects on the trading of resources, the dynamics of the processes carried out by the resources and decision-making processes, the associated resources and their interaction processes.

The aim of the analysis is to identify structural-functional phenomena for the effective implementation of and management of their resource decision-making processes. The efficiency of particular resources is evaluated based on the criteria of balance, ensuring the desired states of structural-functional relationships in distinguished categories of critical infrastructure.

The considerations are carried out from three perspectives: *resources*, *processes* and *decisions*. These perspectives are interwoven in order to allow their mutual interpretability and coherence in the course of analyzing the results of the theoretical and practical aspects

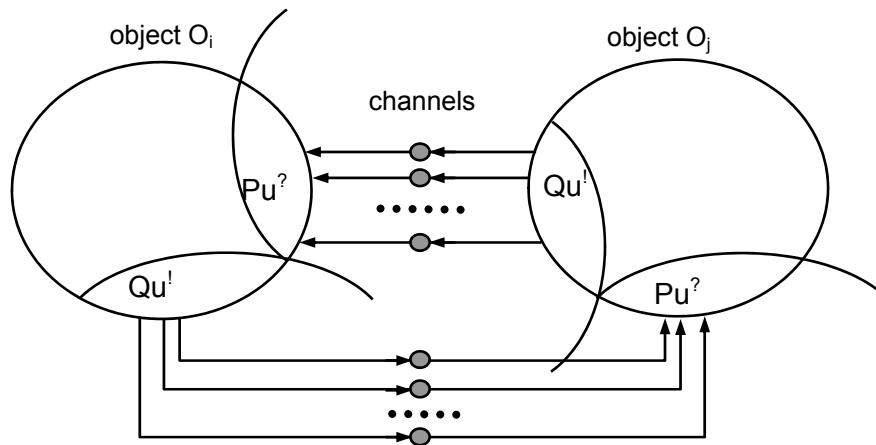


Figure 1. Mutual activities of the two resources - output channels of threats and input channels of susceptibility objects  $O_i, O_j$

of the structural-functional phenomena being observed. Other research perspectives on integral assessments of potential impacts (e.g. risk factors), risk assessment and situational management (crisis management) will be included, using unconventional operating systems, game theory, semiotics, Pavlovian networks, theories of catastrophe and other research methods.

The key assumption is that of the methodological coherence of models, guaranteeing their co-operation in specific technological layers of a crisis management system.

The prospective “resources” make possible a resource-oriented (static and dynamic) interpretation of interacting fragments of physical reality and information. The task here is to identify all the objects in this reality which are essential for maintaining the desired balance.

The prospective “processes” show the dynamic processes of recognition of objects in the course of their interactions. The construction and analysis of the processes taking place in the objects and between objects can be used to define and solve decision problems related to the maintenance of the desired objects in a state of equilibrium.

The prospective “decisions” relate to the definition and decomposition of decision problems, which should lead to the determination of the trajectory of the desired parametric resource states in the process of the setting up and interaction of objects.

The material presented is the result of the selection of a group of systemic issues that can be presented in a form that does not seem to be too simple and also does not require the use of excessive abstract notation. Among the topics were selected elements of an engi-

neering and utility that can be used for modeling and designing systems and the nature of organizational and technical information, in order to help define the roles of people and resources.

The condition of effective coordination of resource interaction is necessary to recognize the morphological characteristics, and above all the functions, structure and transformation of these characteristics. Well-constructed ontology area interactions can significantly affect the architecture (spatial structure) and function (efficiency) crisis management system.

For the purpose of resource configuration, the analysis is treated as a collection of object related channels, wherein the channels play a key role by which the objects communicate with each other. Channels correspond to those objects, and the values of their states correspond to the current values of the attributes of the resources. An illustration of the mutual activities of the two resources is Fig. 1, which shows two related object channels.

The susceptibility of objects  $O_i$  and  $O_j$  is modeled by susceptibility function systems (observation)  $P_u$ . Threats of objects  $O_i$  and  $O_j$  are modeled by functions threats systems (extortion)  $Q_u$ .

Channels act as storage facilities - and if detailed description is necessary - they can be interpreted as objects, thus creating a multi-layered model of resource configuration. The phenomena occurring in the channels of the object are treated as processes of risks and susceptibility. It is assumed that any operation of the object can be described by sequences of discrete events that enforce and control the repertoires of finite state channels.

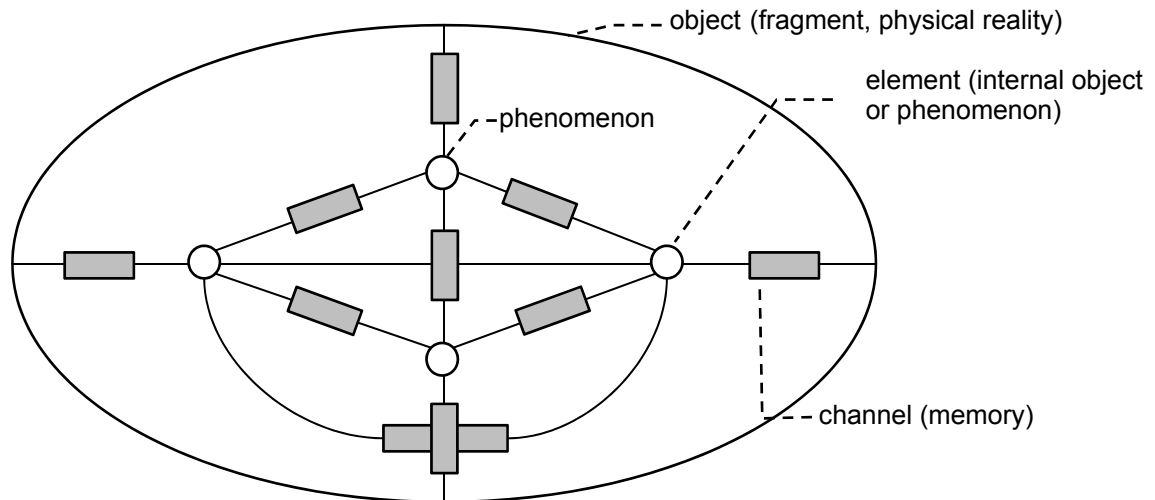


Figure 2. Object and its elements connected with channels as a model of particulars and phenomena

The concept of the object can also be used to describe physical reality, and in rare cases to the description of the corresponding unstable virtual reality. The facts are also used to describe phenomena (interactions) in them or between them occurring. The concept of the object is used to model the structure constant during each of the interacting fragments of material reality. The concept of phenomenon is used to describe the effects of the interaction of objects.

The discussion may include occasions when the concrete can take the form of material - for example, highlighting the physical condition of the channel or information form - such as a data record stored in the buffer memory.

With such facilities, *class invariants* (invariants) and meta-language descriptions of physical reality can be constructed. Fig. 2 illustrates the three levels of modeling (object - element - impact) and analyzing fragments of physical reality. Processes occurring in physical reality may be presented at the level of meta-language descriptions of the particulars and phenomena, if the only concrete fact assigns the element related channels into a single object. In this description, the channels are used to model the interaction of particulars. In this interpretation, the impact of particulars are presented by the relationship of mutual threats and susceptibilities recorded on the channel connecting material objects (particulars) and other related phenomena.

#### 4 Positioning resources - the interdependence of CI

The use of the resource approach makes it possible to define critical infrastructures as systems including their constituent functionally interrelated objects, such as building structures, equipment, installations, services crucial to the security of the state and its citizens and to ensure the smooth functioning of the public administration, as well as institutions and entrepreneurs.

As stated in the National Programme for Critical Infrastructure Protection (NPCIP): “*Identification of facilities, equipment, installations or services whose destruction or disruption of the operation would cause a crisis, is a key step in the process of protecting CI.*” Part of NPCIP’s proposed method for identifying critical infrastructure uses identification criteria for each CI system, describing them as criteria for the systems. These criteria quantitatively or subjectively characterize parameters (functions) resources (objects, devices, systems or services), which are suitable for resource allocation to critical infrastructure. This approach allows for a definition of the critical infrastructure of the simultaneous decomposition of CI systems and constituent resource classes, which can also be considered as part of the CI in the system, as illustrated in Fig. 3.

The CI system is built in accordance with the representation of the concept. For each operational area R (e.g. municipalities) are specified as real property, equipment, installations, and other systems belonging to various classes of CI and their resources (Fig. 4).

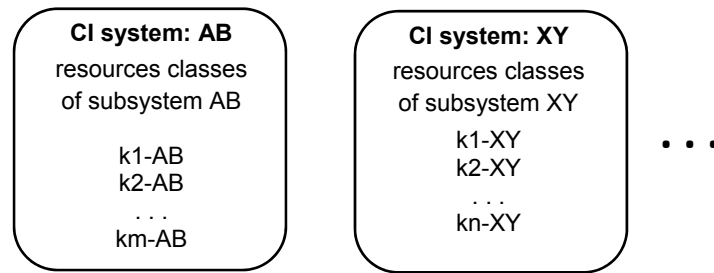


Figure 3. The decomposition of CI systems and their constituent classes of resources

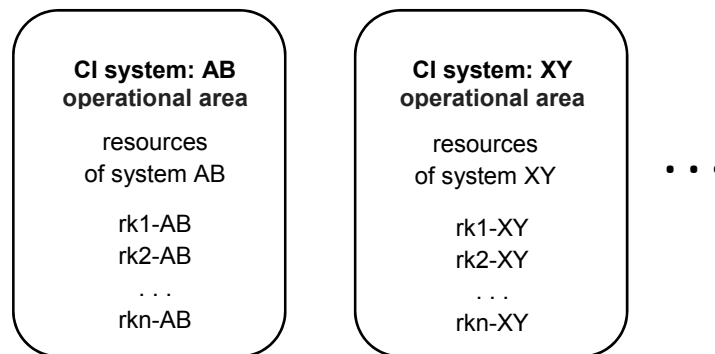


Figure 4. The resource features in the operating areas  $r_{ki}$  of CI systems

Table 1. Classes of resources in the CI systems

resource	CI system (CIS) in operational area R									
	AB	BC	CD	DE	EF	FG	GH	.....		XY
rk1-AB	1		0,5		0,1		0,2			
rk2-AB	1			0,1						
...	1									
rkn-AB	1	0,4								
rk1-BC		1	0,2			0,2				
rk2-BC		1								
...		1								
rkn-BC		1								
...	...	...	...	...	...	...	...	...	...	...
rk1-FG		0,2				1				
rk2- FG						1				
...						...				
rkn- FG						1				
rk1-GH				0,2			1			
rk2- GH	0,1				0,3		1			
...							...			
rkn- GH							1			

Table 2. Classes of resources in the CI systems

	AB ↓↓	BC ↓↓	CD ↓↓	DE ↓↓	EF ↓↓	FG ↓↓	GH ↓↓	....
AB								
BC	0,4					0,2		
CD	0,5	0,2						
DE	0,1						0,2	
EF	0,1						0,3	
FG		0,5						
GH	0,2							
....								

Individual CI systems are interrelated and interdependent. Many CI systems realize their functioning due to the availability of resources contained in other systems of CI. This relationship can be represented as a table: CI resource systems (Table 1).

Resources belonging to a particular CI system are represented by the value 1.

The estimated impact of a resource on the functioning of the other CI systems is indicated by parameter values in the range of 0 to 1. An analysis of parameter values and their distribution, as presented in Table 1, is used to determine the resource position of critical infrastructures, both in terms of scope and strength of their impact on other CI systems.

Analyses of parameter values and their distribution in Table 1 are used to determine resource positions in critical infrastructure, in terms of both the scope and strength of its impact on other systems CI.

Based on the data entered into Table 1 it is possible to determine the interdependence of CI, including the extent of mutual dependence.

In Table 2, the rows and columns of the table refer to the individual CI systems. The values entered in the table cells indicate the degree of impact of the CI system as indicated in the column header whereby CI systems are placed in the rows on the table. It can be seen, for example, that the CI system AB is indicated as the impact on the functioning of the BC, CD, DE, EF, and GH, but that it is not itself susceptible to disturbances caused by the reduction or absence of the operation of the other systems. The BC may cause harmful interference to systems CD and FG, but is prone to interference from both the AB and FG.

Information about the mutual interdependence of CIs can be useful when making decisions during crisis management.

## 5 Resources and hazards clusters

Resource taking (in a “more or less” controlled) way of the effects of threats in the coming months from resources with regard to location, processing, remembering and communicating in the form of further threats (extortion) and adjacent resources.

An analysis of this process may be important for understanding the phenomenon of pyramidal dominos in the spreading of threats and emergencies.

Fig. 5 shows two models of hyper graph clusters resulting in risks of structural transformation of resources that have moved relative to each other (stock-components are shown as hatched circles) and which initiated the creation of negative interactions within these clusters.

Hyper graph arcs indicate the direction of the threats (negative interactions) between resources. One of the arcs illustrates the risk-return “self-destruction”. Some of the arcs indicate the risks posed by the resources deployed in the interior of the structure of other resources.

In situations of real threat, the nature of CI resources and CI systems interdependence should be considered by taking into account the dynamics of movements of resources (direction, time, and potential threats or susceptibilities). For this reason, each distinguishable resource belonging to the CI system should be interpreted as “a cluster of risks”.



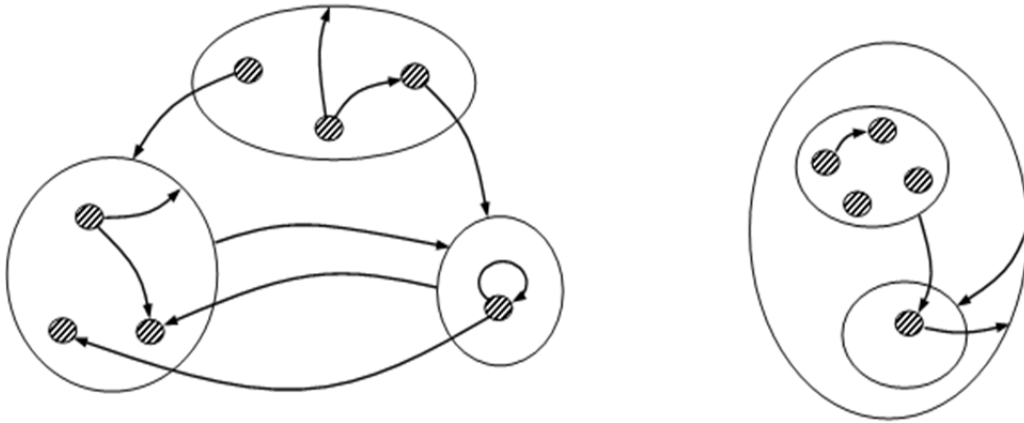


Figure 5. Hyper graphs clustering models of risk

In Fig. 6 the configuration of the cluster resource risks is shown. It is possible that each resource  $R_i$  may contain in its distinguishable structure other CI resources which should be treated as a cluster risks. Resource

interactions  $K_{i,j}$  are represented and transformed in the form of channels in which threats and susceptibilities are processed and balanced.

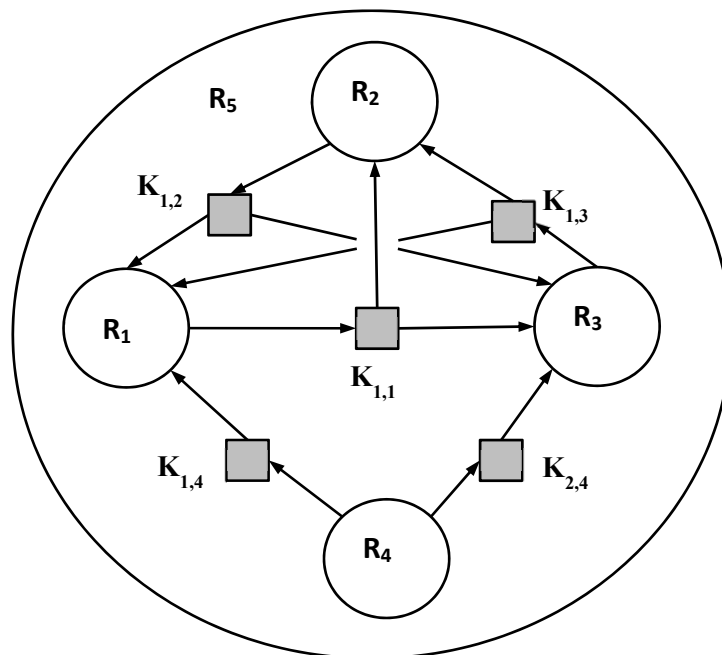


Figure 6. The cluster resource configuration

## 6 Susceptibilities

Concepts of susceptibility and susceptibility analysis usually arise in the context of IT technology. Information resources, including data often strategically located in the IT infrastructures of organizations, are susceptible to a number of internal and external risks. Identification of critical resources and analysis of their susceptibility makes it possible to evaluate the effectiveness of current safeguards and formulate proposals for solutions to improve their safety.

Topic susceptibility has been taken in many environments after 11 September 2011, when a terrorist attack highlighted the susceptibility of many systems at risk, which were not expected, using procedures that would allow for reducing the effects of hazards.

The analysis of critical resources and potential threats seems to be insufficient. The effects of the same risks in relation to the resources of the same class may be very different due to the varying susceptibilities of resources to the same threat.

Conclusions from the analysis based on risk and susceptibility to the threat of resources:

- 1) Resources of a particular class, included in the critical infrastructure have established repertoire of already differentiated features (Fig. 7).

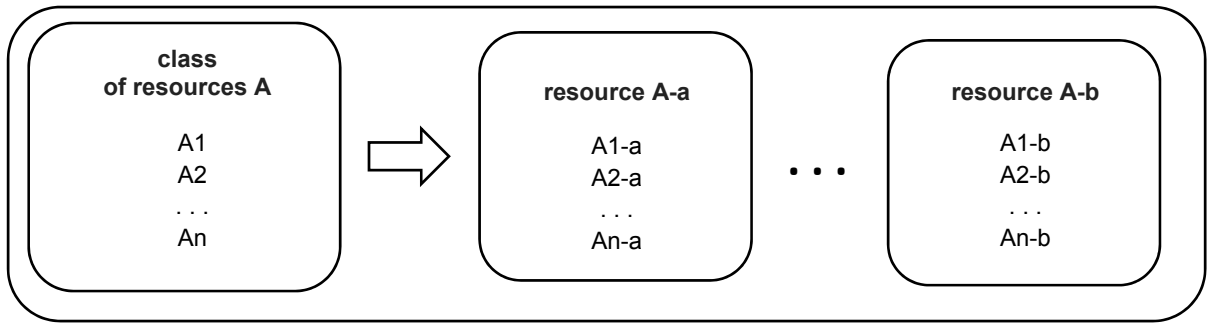


Figure 7. Class of resources

- 2) A fixed subset of a class of resources determines their susceptibilities to the threat to specific resources (Fig. 8).

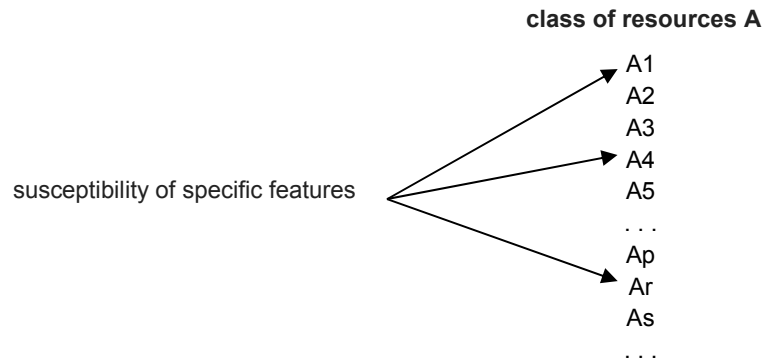


Figure 8. Susceptibilities of class of resources A expressed by the values of the features

- 3) With each threat a resource assesses susceptibilities to it, so each class of resources will also have a corresponding list of susceptibilities (Fig. 9).

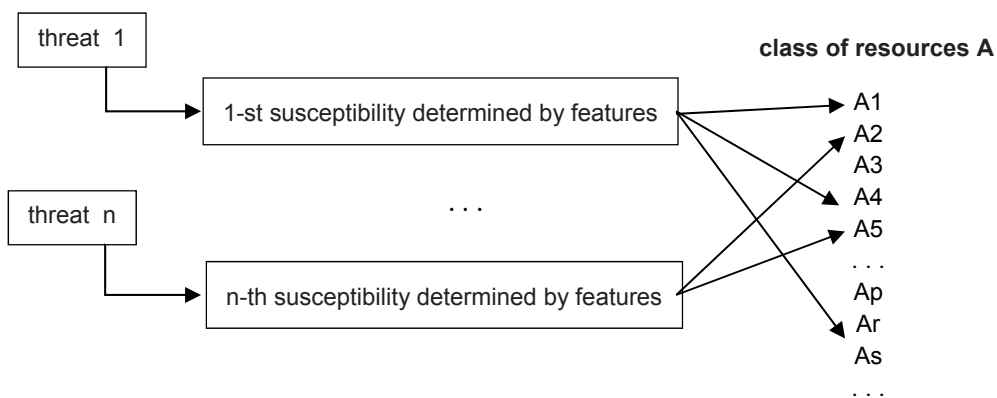


Figure 9. Threats and susceptibilities of the class of resource A expressed by the values of the features

- 4) It seems that susceptibility is a function of the features and will be distinctive and individual for each resource in terms of its value - and does not use the same class of resources with different characteristics (Fig. 10).

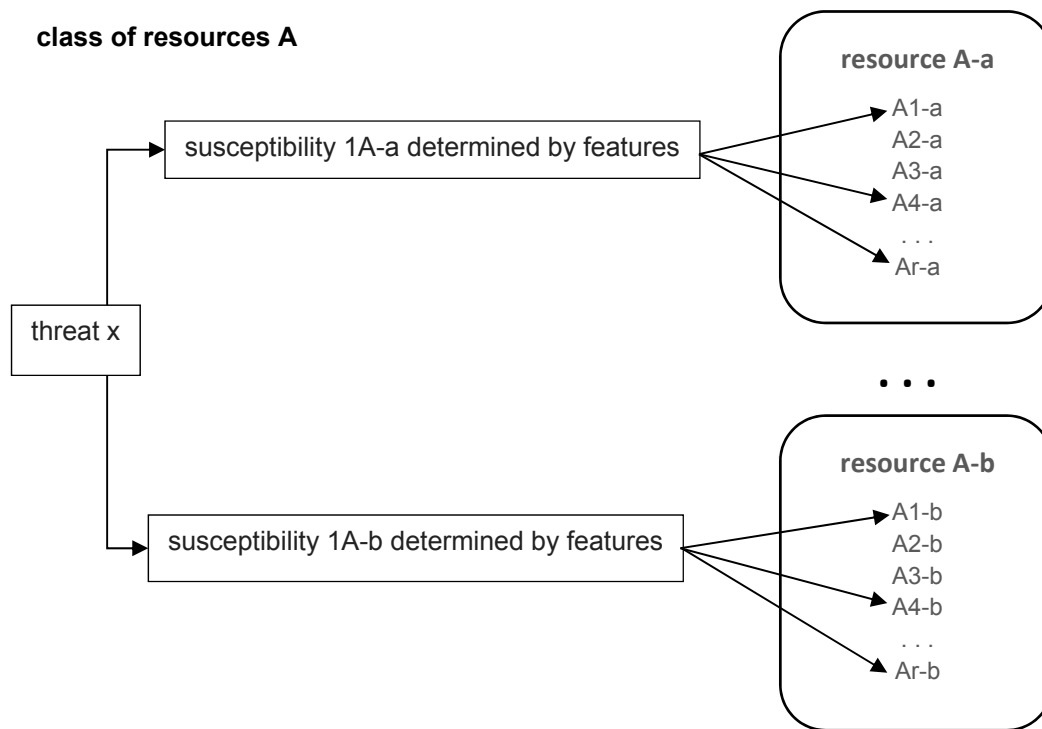


Figure 10. Relationship "threat x - susceptibility class resources" expressed in the values of the features

- 5) The specific features of the object determine its susceptibility to risk and their impact on the susceptibility can vary considerably. It thus seems necessary to position the characteristics of resources in terms of their susceptibilities to risk (Fig. 11). It may be that susceptibility analysis procedures assume that the sum of the weights should be 1 - similar to modeling problems, decision areas and decision-making processes [3, 4, 6].

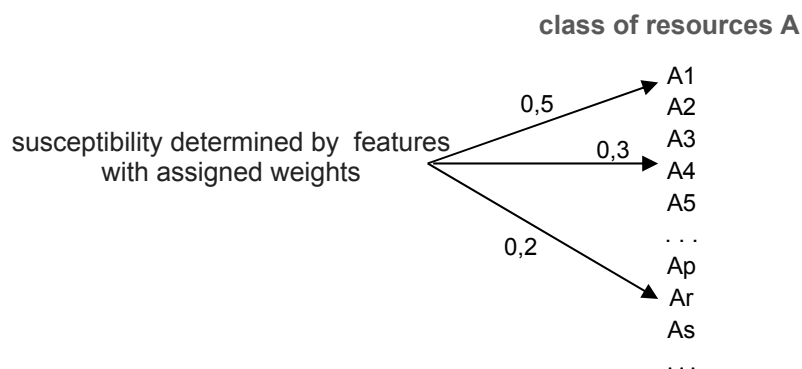


Figure 11. Susceptibility of the resource expressed using weights assigned to groups of features

6) The values of the resource attributes can change over time, which makes it possible to change the susceptibility of resources to a threat by means of established policy changes to its characteristics. It should, however, be noted that changes in the value of certain features associated with different resource

susceptibilities may cause a reduction of one form of susceptibility while increasing others. With the change in the value of individual features, adjustable sensitivity class share resources can be weighted assigned to groups of features (Fig. 11 and Fig. 12).

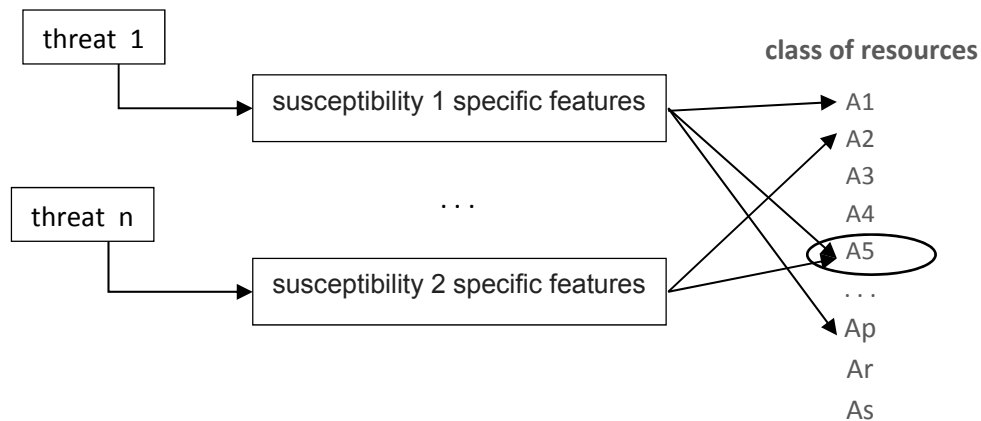


Figure 12. Illustration relationship threats and susceptibility Class A resource expressed in the values of the features and weights are assigned to groups of features

- 7) Since the values of various characteristics may vary over time as a result of threats or due to business resources of the owners, the changes may involve additional susceptibility. Such values may change rapidly, and should be determined in real time, which is only possible with the support of IT tools.
- 8) Susceptibility to risk may also arise from the interdependence of resources as a result of the overlapping of critical infrastructures and mutual threats posed by the domino effect.

## 7 Summary

The interpretation of critical infrastructure in terms of resources allows the use of a simple conceptual apparatus to describe the complex question of the identification of CI systems, which is the basis of specific actions related to national security. In the course of further work this provides a critical analysis of infrastructure systems in terms of their resources. Test specification attributes are required in the process of reporting, analysis and decision-making as well as activities related to the provision of national security.

The proposed approach allows the interpretation of all the data required to prepare the report on the dangers

in the category of resource characteristics of critical infrastructure. This includes data on resources and data, from which information about mutual interdependencies of resources can be obtained, as well as data about the dynamics of changing times under the threat of deliberate action by the owner or resources including, for example, changes in the characteristics of the resources that reduce susceptibility.

The inclusion in the model of the characteristics of resource susceptibility to hazards can be used to:

- assess the effectiveness of current security and of possible changes in reducing susceptibility to specific risks and increasing safety parameters in the area of critical infrastructure,
- assess risks in the form of a risk account for which various features contribute to the increasing susceptibility of resources at risk.

In the course of further work a multidimensional information model of CI is planned, combining a description of the dynamics of susceptibility and threats to CI systems.

The expected result will be the ability to conduct effective risk calculation for crisis management of CI resource configurations.

## 8 Bibliography

- [1] Domański J., Kotarba W., Krupa T. – *W pryzmatach zarządzania* [in] *Klasyczne i współczesne koncepcje zarządzania. Aspekty teoretyczne i praktyczne*. Wyd. Uniwersytetu Ekonomicznego, Poznań 2014 (w druku).
- [2] Zawila-Niedźwiecki J. - *Zarządzanie ryzykiem operacyjnym w zapewnieniu ciągłości działania organizacji*. Wyd. edu-Libri, Kraków - Warszawa 2013.
- [3] Krupa T., Ostrowska T. - *Decision Making in the Flat and Hierarchical Decision Problems* [in] *Foundations of Management - International Journal*, Vol. 4, No. 2, 2012, pp. 23-36.
- [4] Krupa T., Ostrowska T. - *Metoda wielopoziomowego bilansowania zasobów w procesie zarządzania projektami* [in] *Komputerowo zintegrowane zarządzanie* (red. R. Knosala). PTZT, Opole 2011, s. 605-6015.
- [5] Krupa T. - *Events and Events Processes* [in] *Foundations of Management - International Journal*, Vol. 1, No. 2, 2009, pp. 143-158.
- [6] Krupa T., Ostrowska T. - *Multilayer Decision Support Model for Value and Cost Analysis of IT Solutions – Hierarchical Approach* [in] *Managing Worldwide Operations and Communications with Information Technology*. IGI Publishing, IRMA Int. Conf., Vancouver Canada 2007, pp. 86-90.
- [7] Krupa T. - *Elementy organizacji, zasoby i zadania*. WNT, Warszawa 2006.
- [8] Krupa T. - *O pewnej specyfikacji procesu decyzyjnego* [in] *Problemy Zarządzania*. Wydawnictwo Naukowe WZ UW, Nr 1 2005, s. 79-88.
- [9] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r. nr 89 poz. 590, z późn. zm.)  
<http://isap.sejm.gov.pl/DetailsServlet?id=WDU20070890590> (odczyt: 2013.09.16).
- [10] Narodowy Program Ochrony Infrastruktury Krytycznej 2013 – dokument główny.  
<http://rcb.gov.pl/wp-content/uploads/NPOIK-dokument-glowny.pdf> (odczyt:2013.09.16).
- [11] Załącznik 1 – Charakterystyka systemów infrastruktury krytycznej.  
<http://rcb.gov.pl/wp-content/uploads/NPOIK-załącznik-1.pdf> (odczyt: 2013.09.16).
- [12] Załącznik 2 – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje.  
<http://rcb.gov.pl/wp-content/uploads/NPOIK-załącznik-2.pdf> (odczyt: 2013.09.16).

Material developed for the project: “Methodology of risk assessment for the purposes of crisis management system RP”. Agreement No. DOBR/077/R/ID3/2013/03. The project is financed 100% of the budget of the National Center for Research and Development. Consortium member: Faculty of Management - Warsaw University of Technology.