Blokus-Roszkowska Agnieszka

Guze Sambor

Kołowrocki Krzysztof

Soszyńska-Budny Joanna
Maritime University, Gdynia, Poland

Ledóchowski Marek
Maritime Office, Gdynia, Poland

Methodology for ship traffic and Port Operation Information Critical Infrastructures safety and resilience to climate change analysis

Keywords

critical infrastructure, Port Critical Infrastructure, Baltic Sea Region, climate change, safety, resilience

Abstract

The paper presents the terminology of port critical infrastructure including definitions of general terms and definitions of more detailed notions. The European Programme for Critical Infrastructure Protection and the European Critical Infrastructures are introduced. Furthermore, the ship traffic and port operation information critical infrastructure terminology and related climate and resilience terminology are presented. Next, the taxonomy refers to ship traffic and port operation information critical infrastructure network with notions related to climate change and resilience and vulnerability of critical infrastructures to climate change are given.

1. Introduction

To ensure compatibility in this paper and in next papers, concerned with this topic, we start with fixing the "working terminology". The first step is to define the *Critical infrastructure (CI)*. According to the European Commission, it is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters or other threats (terrorism, criminal activity or malicious behaviour), may have a significant negative impact for the security of the EU and the well-being of its citizens.

2. State of art

Before the considerations on port critical infrastructure at Baltic Sea Region taxonomy, we refer to definitions of selected basic notions concerned with critical infrastructures and climate and weather impacts on their safety included in the EU-CIRCLE Report - *Taxonomy* [7].

In the paper we use notation *hazard* in term of natural hazards classified as severe and extreme weather and climate events, while *threats* refer to events coming from human activity and other systems or infrastructures.

The main goal of the EU is reducing the vulnerabilities of critical infrastructure and increasing their resilience. Thus, the *European Programme for Critical Infrastructure Protection (EPCIP)* has been started. This sets the overall framework for activities aimed at improving the protection of critical infrastructure in Europe - across all EU States and in all relevant sectors of economic activity. According to the EPCIP a list of 11 European critical infrastructures based upon inputs by its Member States.

The main goal of the EPCIP functioning is to take higher the level of protection of critical infrastructures in the EU Member States. The protection of critical infrastructure, according to [3] indicates activities whose objective is to ensure functionality, continuous operation and delivery of

critical infrastructure services/goods, as well as to prevent natural hazards and threats to critical infrastructure.

Nowadays, the Directive 2008/114/EC on *European Critical Infrastructures (ECI)* [6] is functioning. There are introduced the definition of

- the ECI as the critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure. [6];
- the *Owners/operators of ECIs* as be the entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part there of designated as an ECI and have to prepare *operator security plans* (advanced business continuity plans) and nominate Security Liaison Officers (linking the owner/operator with the national authority responsible for critical infrastructure protection);
- the *Operator Security Plan* (OSP) should cover the identification of important assets, a risk analysis based on major threat scenarios and the vulnerability of each asset, and the identification, selection and prioritisation of counter-measures and procedures;
- the *cross-cutting criteria* as a compromise of the casualties criterion (assessed in terms of the potential number of fatalities or injuries), economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects) and public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services);
- the *sectoral criteria* shall take into account the characteristics of individual ECI sectors.

Furthermore, the document [6] establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. There is a sectorial scope, applying only to the energy and transport sectors.

2.1. Ship traffic and port operation information critical infrastructure terminology

The basis of human activity is the use of goods that are manufactured in various parts of the world. Because of it, the important thing is *transportation*, which means the conveyance of passengers or goods by the six modes of transportation: aviation, maritime, mass transit, highway, freight rail, and pipeline. [53]. This process is possible according to existing *transportation infrastructure*. It is physical distribution systems critical to supporting the national security and economic well-being of this nation, including the national airspace systems, airlines, and aircraft, and airports; roads and highways, trucking and personal vehicles; ports and waterways and the vessels operating thereon; mass transit, both rail and bus; pipelines, including natural gas, petroleum, and other hazardous materials; freight and long haul passenger rail; and delivery services. [44]. The most effective and relatively inexpensive transportation mode is *maritime transport*. It is defined as the shipment of goods (cargo) and people by sea and other waterways. The safety of maritime transport is providing with i*nformation communication technology (ICT).* It is defined as electronic information-processing technologies such as computers and the Internet, as well as fixed-line telecommunications, mobile phones and other wireless communications, networks, broadband, and various specialised application devices ranging from barcode scanners and Braille readers to global positioning systems (GPS). [6] Very important thing is *cybersecurity* understood as the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 112 or similar communications systems and control systems. [55] The above supports the p*ort operations* defined as a necessary tool to enable maritime trade between trading partners. To ensure smooth port operations and to avoid congestion in the harbour it is inevitable to permanently upgrade the ports physical infrastructure, invest in human capital, fostering connectivity of the port and upgrade the port operations to prevailing standards. Hence, *port operations* can be defined as all policies, reforms and regulations that influence the infrastructure and operations of port facilities including shipping services. [57].

The data exchange between ports and ships usually requires:

- the identification is described as recognizing users on a company's system by using unique names.

- the *authentication* defined as the process of establishing the legitimacy of a node or user before allowing access to requested information.

During the process of data exchange, the user enters a name or account number (identification) and password (authentication). [48].

Both stages have to be done with maintaining the *information security* understood as a preservation of confidentiality integrity and availability of information. [38]

The sea ports and ICT are part of the *critical facilities*, which are defined as the primary physical structures, technical facilities and systems which are socially, economically or operationally essential to the functioning of a society or community, both in routine circumstances and in the extreme circumstances of an emergency. Critical facilities are elements of the infrastructure that support essential services in a society. They include such things as transport systems, air and sea ports, electricity, water and communications systems, hospitals and health clinics, and centres for fire, police and public administration services [50].

Managements of particular ports and the owners of companies operating in the port area make up the *Critical Infrastructure community.* It includes critical infrastructure owners and operators (those entities responsible for day-to-day operation and investment of a particular critical infrastructure entity), both public and private; departments and agencies; regional entities; governments; and other organizations from the private and non-profit sectors with a role in securing and strengthening the resilience of the Nation's critical infrastructure and/or promoting practices and ideas for doing so [57].

Every sea port has to be considered as a separate port critical infrastructure. Thus, there are interconnections and mutually dependencies between particular port critical infrastructures.

Thus, we define the *dependency of CI* as a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other. [40], [47]

According to [47], there are four principal classes of interdependencies: physical, cyber, geographic and logical. The particular definitions are given as follows.

Two infrastructures are *physically interdependent* if the state of each is dependent on the material output(s) of the other.

An infrastructure has a *cyber interdependency* if its state depends on information transmitted through the information infrastructure.

Two infrastructures are *geographically interdependent* if a local environmental event affects components across these infrastructures due to physical proximity.

Two infrastructures are *logically interdependent* if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection [47].

2.2. Climate change terminology

In this paper, we consider events that influence critical infrastructures. In this section we focus on terminology about the natural hazards associated with weather and climate change, i.e. *climate hazards*. It is defined as natural phenomena coming out from climate change. Besides the *natural hazards* are severe and extreme weather and climate events that occur naturally in all parts of the world, although some regions are more vulnerable to certain hazards than others [58]. If people's lives and livelihoods are destroyed, then natural hazards become natural disasters [58]. According to US President's Commission on Critical Infrastructure Protection *natural disaster* is a physical capability with the ability to destroy or incapacitate critical infrastructures. It is a violent, sudden and destructive change in the environment without cause from human activity, due to phenomena such as floods, earthquakes, fire and hurricanes. [58]

Following to this way of thinking, we use the Inter-governmental Panel on Climate Change (IPCC), definition of *hazard*. This is defined as the potential occurrence of a natural or human-induced physical event or trend or physical impact that may cause loss of life, injury, or other health impacts, as well as damage and loss to property, infrastructure, livelihoods, service provision, ecosystems and environmental resources [29]-[31].

According to the IPCC, the *climate change* is defined as a change in the state of the climate that can be identified (e.g., by using statistical tests) by changes in the mean and/or the variability of its properties, and that persists for an extended period, typically decades or longer. Climate change may be due to natural internal processes or external forcing, or to persistent anthropogenic changes in the composition of the atmosphere or in land use [20].

In the other hand, we have the definition proposed by the United Nations Framework Convention on Climate Change (UNFCCC). This is defined as follows, the *climate change* is describing as a change of climate which is attributed directly or indirectly to human activity that alters the composition of the global atmosphere and which is in addition to natural climate variability observed over comparable time periods.

The concept of the climate change is linked with the *climate variability*. It refers to variations in the mean state and other statistics (such as standard deviations, the occurrence of extremes, etc.) of the climate at all spatial and temporal scales beyond that of individual weather events. Variability may be due to natural internal processes within the climate system (internal variability), or to variations in natural or anthropogenic external forcing (external variability) [25]-[31].

Following to these definitions, the *climate change scenario* is a coherent and internally-consistent description of the change in climate by a certain time in the future, using a specific modelling technique and under specific assumptions about the growth of greenhouse gas and other emissions and about other factors that may influence climate in the future [42].

Further, *climate stationarity* refers to the stationarity of extremes of climate and weather i.e. that the frequencies and intensities of extremes observed in the past adequately represent those that will occur in the future. [45]

To facilitate works related to the climate changes, the *climate model* is introduced and defined as a numerical representation of the climate system that is based on the physical, chemical, and biological properties of its components, their interactions, and feedback processes, and that accounts for all or some of its known properties [25], [27], [29]-[31].

Climate-weather change process is the process of the climate-weather states changing considered in time for a fixed area.

Extreme weather event is an event that is rare at a particular place and time of year. Definitions of rare vary, but an extreme weather event would normally be as rare as or rarer than the 10th or 90th percentile of the observed probability density function. By definition, the characteristics of what is called extreme weather may vary from place to place in an absolute sense. Single extreme events cannot be simply and directly attributed to anthropogenic climate change, as there is always a finite chance the event in question might have occurred naturally. When a pattern of extreme weather persists for some time, such as a season, it may be classed as an extreme climate event, especially if it yields an average or total that is itself extreme (e.g. drought or heavy rainfall over a season) [29].

2.3. Resilience terminology

Nowadays, the main goal of the EU is to increase the resilience of critical infrastructures. *Resilience* can be understood as the ability of a system and its component parts to anticipate, absorb, accommodate, or recover from the effects of a hazardous event in a timely and efficient manner, including through ensuring the preservation, restoration, or improvement of its essential basic structures and functions [4], [27], [40]

The resilience of systems is distinguished by following four infrastructural qualities:

- *Robustness*: the inherent strength or resistance in a system to withstand external demands without degradation or loss of functionality.
- *Redundancy*: system properties that allow for alternate options, choices, and substitutions under stress.
- *Resourcefulness*: the capacity to mobilize needed resources and services in emergencies.
- *Rapidity*: the speed with which disruption can be overcome and safety, services, and financial stability restored.

The following terms are connected with these notions.

In the case of critical infrastructure, *secure/security* means reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters [55].

Safety plan from owner/manager of critical infrastructure indicates a plan that ensures confidentiality, integrity and availability of the organizational, human, material, information-communication and other solutions, as well as permanent and graded security measures necessary for the continuous functioning of critical infrastructure [3].

There are many concepts of risk in the literature. One of them presented in [40], defines risk as a combination of the consequences of an event (hazard) and the associated likelihood/probability of its occurrence. Other concepts define risk as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization [5]. Relating to climate and climate change, risk can be also understood as the result of interaction of physically defined hazards with the properties of the exposed systems i.e., their sensitivity or vulnerability.

In Section 2.2., there is introduced the Operator Security Plans. One of their elements can be *critical infrastructure risk management framework* defined as a planning and decision-making framework that outlines the process for setting goals and objectives, identifying infrastructure, assessing risks, implementing risk management activities, and measuring effectiveness to inform continuous improvement in critical infrastructure security and resilience [55].

Furthermore, an overall process consisting of three steps: risk identification, risk analysis and risk evaluation defines *risk assessment* [14], [38]-[39]. Besides, *risk management process* is the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk. [14], [38].

In the next step, there are presented concepts related to vulnerability, adaptation and mitigation.

In the paper [55], vulnerability is defined as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

In terms of reliability, it can be measured as the probability that a system will come to the critical state or worse in time shorter than assumed level, due to some external factors, causing large negative effects that influence on other sensitive systems (consequences above a fixed level). Similar approach has been presented in "*Disaster resilient infrastructure*", where the vulnerability of an infrastructure system is defined as the probability of at least one disturbance with negative societal consequence larger than some large (critical) value, during a given period time.

In fact, the concept of vulnerability can be related to the *adaptation*, which in terms of climate change includes initiatives and measures to reduce the vulnerability or increase the resilience of natural and human systems to actual or expected climate change impacts. There can be distinguished various types of adaptation, such as anticipatory and reactive, private and public, and autonomous and planned.

With the adaptation the following terms can be linked.

Detection of impacts of climate change for a system or infrastructure is defined as the identification of a change from a specified baseline. The baseline characterizes behaviour in the absence of climate change and may be stationary or non-stationary [29].

Potential impacts are defined as all impacts that may occur given a projected change in climate, without considering adaptation. And r*esidual impacts* are the impacts of climate change that would occur after adaptation. [22]

The very close related with terms resilience, vulnerability and adaptation is *mitigation* of disaster risk and disaster can be defined as the lessening of the potential adverse impacts of physical threats, including those that are human-induced, and natural hazards through actions that reduce hazard, exposure, and vulnerability [25]. Mitigation of the climate change effects in relation to critical infrastructures can be implemented through policies and action to reduce potential negative consequences of hazards caused by climate change extreme events.

3. Baltic ship traffic and port operation information critical infrastructure network taxonomy

Considering definitions concerned with critical infrastructures and their networks and the nature and features of the industrial installations at the Baltic Sea Region, we start with the notion of the *complex system* that is defined as a set or group of interacting, interrelated or interdependent elements or parts, that are organized and integrated to form a collective unity or an unified whole, to achieve a common objective.

This definition lays emphasis on the interactions between the parts of a system and the external environment to perform a specific task or function in the context of an operational environment. This focus on interactions is to take a view on the expected or unexpected demands (inputs) that will be placed on the system and see whether necessary and sufficient resources are available to process the demands. These might take form of stresses. These stresses can be either expected, as part of normal operations, or unexpected, as part of unforeseen acts or conditions that produce beyond-normal (i.e., abnormal) conditions and behaviours. This definition of a system, therefore, includes not only the product or the process but also the influences that the surrounding environment (including human interactions) may have on the product's or process's safety performance.

The *system operating environment* is defined as the surroundings in which a system operates, including air, water, land, natural resources, flora, fauna, humans and their interrelations.

The *system operating environment threat* is an unnatural event that may cause the system damage and/or change its operation activity in the way unsafe for the system and its operating environment, for instance: another ship activity in the ship operating environment that can result in an accident with serious consequences for the ship and its operating environment, terrorist attack changing the system operation process in an unsafe way.

The *system inside dependencies* are dependencies within a system itself i.e. relationship between components and subsystems in a system causing state changes of other components and subsystems and in a consequence resulting in changes of the system state.

The system outside dependencies are dependencies coming from the system operating environment (external factors), including changes of the system

state caused by outside this system conditions e.g. climate changes, changes of its functionality, location, other objects, government and human decisions (regulations, economic, public policy).

Now, we can define the *critical infrastructure* as a complex system in its operating environment that significant features are inside-system dependencies and outside-system dependencies, that in the case of its degradation have significant destructive influence on the health, safety and security, economics and social conditions of large human communities and territory areas.

In next step, we define the *critical infrastructure network* as a set of interconnected and interdependent critical infrastructures interacting directly and indirectly at various levels of their complexity and operating activity. Furthermore, the *interconnected critical infrastructures* that are critical infrastructures in mutually direct and indirect connections between themselves and the *interdependent critical infrastructures* that are critical infrastructures in mutually dependant relationships between themselves interacting at various levels of their complexity.

A concept closely related to the above is *CI network cascading effects*. They are degrading effects occurring within an infrastructure and between infrastructures in their operating environment, including situations in which one infrastructure causes degradation of another ones, which again causes additional degradation in other infrastructures and in their operating environment [7].

We define the Baltic Ship Traffic and Port Operation Information Critical Infrastructure Network (BSTPOICIN) composed of 121 AIS base stations, 27 DGPS stations and 21 port/terminal operation systems. The BSTPOICIN interactions with Baltic Sea Environment and Other Critical Infrastructures can be expressed by its strong impact on the proper and the efficient functioning of maritime transport. Mainly, it affects the BSCIN and BPCIN both described in [8]. Moreover, BSTPOICIN cooperates with and depends on land critical infrastructures and systems, i.e. electric power grids, computer and internet networks, etc.

3.1. Critical infrastructure taxonomy

The Baltic Ship Traffic and Port Operation Information Critical Infrastructure is in the class of so called static industry installations. For them, we can define *threats to critical infrastructure or critical infrastructure network* as the occurrence of an unwanted circumstance or event that may cause damage, functioning disruption or service interruption to port critical infrastructures located in the Baltic Sea Region. Considering this critical infrastructure, we have to take into account natural climatic hazards i.e. hazards associated with climate and weather change. In particular, we pay attention to the natural hazards related to climate-weather change. Thus, the following two important definitions.

Critical infrastructure operation process general model related to climate-weather change is defined as the critical infrastructure operation process joint model related to operating environment hazards and climate-weather change extreme events linking the critical infrastructure operation process model and the climate-weather change process model.

Critical infrastructure integrated safety model related to climate-weather change includes modelling the critical infrastructure operation process according to the critical infrastructure operation process general model related to climate-weather change process and modelling the critical infrastructure inside dependencies between its components and subsystems according to the critical infrastructure safety general model.

3.2. Climate change taxonomy

For Baltic Ship Traffic and Port Operation Information Critical Infrastructure Network, the following climatic hazards have influence on its functioning can be distinguish: wind, temperature, humidity, cloudiness, precipitation or solar radiation, hurricanes or storms. It means, that we have to consider the following hazards parameters: wind speed, wind direction, wave height, sea water temperature, air temperature, soil temperature, rainfall level, snowfall level, ice thickness, fog density, flood level, landslide speed and wildfire level. Not all types of hazards and hazards parameters have influence on ship traffic and port operation information critical infrastructure, but have some consequences for particular range of the hazard parameter. Thus, the following basic notions related to climate and weather changes, in particular to climate changes in the Baltic Sea Region, are:

- *Storms* is defined as an atmospheric disturbance involving perturbations of the prevailing pressure and wind fields, on scales ranging from tornadoes (1 km across) to extratropical cyclones (2000-3000 km across). On the Beaufort scale storm refers to wind with a speed between 48 and 55 knots and Beaufort number 10 of wind force [19].
- *Extreme coastal high water*, also referred to as extreme sea level, depends on average sea level, tides, and regional weather systems. Extreme coastal high water events are usually defined in

terms of the higher percentiles (e.g., 90th to 99.9th) of a distribution of hourly values of observed sea level at a station for a given reference period [27].
- *Significant wave height* refers to the average height of the highest one-third of the wave heights (trough to peak) from sea and swell occurring in a particular time period [8].
- The *storm surge* is the temporary increase, at a particular locality, in the height of the sea due to extreme meteorological conditions (low atmospheric pressure and/or strong winds). The storm surge is defined as being the excess above the level expected from the tidal variation alone at that time and place [20], [28].
- *Storm tracks* are regions with a high frequency of storms. The storms tend to have a preference for the north-eastern part of the North Atlantic, but are affected by the NAO.

According to above notions, the important thing is that the *critical infrastructure exposure* is defined as the fact or the condition of being exposed to something (of being subjected to an action or an influence), for instance being exposed to severe weather.

Thus, the climate prediction and climate projection are important terms for climate changes. They are defining as follows.

The *climate prediction* or climate forecast is the result of an attempt to produce an estimate of the actual evolution of the climate in the future, e.g., at seasonal, inter-annual or long-term time scales, while the *climate projection* is the response of the climate system to emissions or concentration scenarios of greenhouse gases and aerosols, or radiative forcing scenarios, often based on simulations by climate models [25], [27].

3.3. Resilience taxonomy

We assume that *resilience* is the sufficient ability of an object to continue its operational objective in the conditions including harmful impacts and the ability to mitigate and/or to neutralize those harmful impacts. Further, we define the *critical infrastructure resilience* to climate change as the ability of a CI to continue providing its essential services when it is exposed to hazards associated with coming out from the climate change harmful events as well as its speed of recovery and ability to return to normal operation after those hazards has receded.

Besides *strengthening critical infrastructure resilience to climate change* means efforts, like policies, procedures and actions, taken to prolong the proper and effective functioning of a critical infrastructure and providing its essential services when it is exposed to threats and natural hazards associated with climate-weather change.

The concept of infrastructure resilience is also closely related to *critical infrastructure vulnerability*, that can be defined as the possibility of a critical infrastructure coming to the safety state subset worse than a critical safety state in time shorter than its fixed value, due to some external factors, causing negative effects on itself, other objects and its operating environment.

Referring to the definition of hazards and threats adopted in this article, we accept the definition of vulnerability given in [3], with a small correction. Then, *vulnerability* can be defined as essential properties of the system, parts of the system, assets, community and the environment which make them susceptible to adverse effects of natural hazards and other threats.

Besides, the resilience strengthening of CI is related to terms: robustness, resourcefulness, redundancy, response and recovery, which definitions are as follows:
- *Robustness*, in climate change context, is the inherent strength or the ability of infrastructure to withstand external demands coming from climate change without degradation or loss of functionality. Hence, robustness signifies that a system/infrastructure will retain its system structure (function) intact (remains unchanged or nearly unchanged), when exposed to perturbations and can be measured as the probability that a system will not go into the critical state or worse in time shorter than assumed level, due to some external factors ("*Disaster resilient infrastructure*").
- Critical infrastructure r*esourcefulness* is the ability of a critical infrastructure to identify problems, establish priorities, and mobilize needed resources and services when threatened by harmful events coming from the climate change.
- *Redundancy* is the properties of a critical infrastructure that allow for use alternate options, choices, and substitutions under stress, in order to satisfy functional requirements in threat situations of disruption, degradation, or loss of functionality coming from climate change. It can be measured as the speed with which disruptions coming from climate change can be overcome, in order to contain losses and avoid future disruption, and with which safety, functionality and stability of critical infrastructure can be restored.
- *Response* means reaction (policies and action) during or immediately after a disaster in order to reduce its impacts, to ensure functioning of basic systems (infrastructures) and to prevent transitions of the system or infrastructure into

crisis situation. It usually includes activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs.

- *Recovery* can be defined as the restoration, and improvement where appropriate, of facilities, livelihoods and living conditions of disaster-affected communities, including efforts to reduce disaster risk factors [49].

Additionally, with resilience there are linked other notions, such as resistance or retrofitting. *Resistance* is the ability of a system to remain unchanged by external events. *Retrofitting* is a reinforcement or upgrading of existing structures to become more resistant and resilient to the damaging effects of hazards [4].

4. Conclusion

In the paper the terminology and methodology on Baltic ship traffic and port operation information critical infrastructures are presented. More detailed description of the Baltic Ship Traffic and Port Operation Information Critical Infrastructure Network, defined in this paper, is given in the report [8] and [15]-[16]. Presented in the paper terminology and taxonomy are also used in the EU-CIRCLE project. Presented methodology and terminology refers to climate-weather change and its impact on critical infrastructures as well as critical infrastructure resilience and resilience strengthening to climate change.

Acknowledgments

The paper presents the results developed in the scope of the EU-CIRCLE project titled "A pan – European framework for strengthening Critical Infrastructure resilience to climate change" that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653824. http://www.eu-circle.eu/.

References

[1] Brodie, P. & Sullivan, E. (1997). *Dictionary of Shipping Terms*, Third Edition.

[2] Committee on the Peaceful Uses of Outer Space. (2014). *Working report of expert group C: space weather*. United Nations. A/AC.105/C.1/2014/ CRP.15.

[3] Croatian Law on critical infrastructures. (2013). *Official Gazette - Narodne novine* 56/13.

[4] Dickson, E., Baker, J. L., Hoornweg, D. et al. (2012). *Urban Risk Assessments, Understanding Disaster and Climate Risk in Cities*. International Bank for Reconstruction and Development/World Bank, Washington, DC.

[5] ENISA, EU. European Union Agency for Network and Information Security. *Glossary*. [available at: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary].

[6] EU. (2008). *Identification and Designation of European critical infrastructures and the Assessment of the need to improve their protection*. Council Directive 2008/114/EC of 8 December 2008

[7] EU-CIRCLE Report D1.1-GMU1. (2015). *EU-CIRCLE Taxonomy*.

[8] EU-CIRCLE Report D1.2-GMU1. (2016). *Identification of existing critical infrastructures at the Baltic Sea area and its seaside, their scopes, parameters and accidents in terms of climate change impacts*.

[9] EU-CIRCLE Report D1.4-GMU3. (2016). *Holistic approach to analysis and identification of critical infrastructures within the Baltic Sea area and its surroundings – Formulating the concept of a global network of critical infrastructures in this region ("network of networks" approach).*

[10] EU-CIRCLE Report D2.1-GMU2. (2016). *Modelling outside dependences influence on Critical Infrastructure Safety (CIS) – Modelling Critical Infrastructure Operation Process (CIOP) including Operating Environment Threats (OET).*

[11] EU-CIRCLE Report D2.1-GMU3. (2016). *Modelling outside dependences influence on Critical Infrastructure Safety (CIS) – Modelling Climate-Weather Change Process (C-WCP) including Extreme Weather Hazards (EWH).*

[12] EU-CIRCLE Report D2.1-GMU4. (2016). *Modelling outside dependences influence on Critical Infrastructure Safety (CIS) - Designing Critical Infrastructure Operation Process General Model (CIOPGM) related to Operating Environment Threats (OET) and Extreme Weather Hazards (EWH) by linking CIOP and C-WCP models.*

[13] European Commission. (2012). Commission staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP). Brussels, 22.6.2012 SWD(2012) 190.

[14] Government of South Australia, Department for Communities and Social Inclusion. (2012). DECS 07/5007, *Framework. Fraud, Corruption, Misconduct and Maladministration Control*.

[15] Guze, S. & Kołowrocki, K. (2016). Joint Network of Port, Shipping and Ship Traffic and Operation Information Critical Infrastructure Networks. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 61-64.
[16] Guze, S. & Ledóchowski, M. (2016). Ship Traffic and Port Operation Information Critical Infrastructure Network. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 65-72.
[17] HELCOM (2009). *Ensuring safe shipping in the Baltic*. Helsinki Commission (HELCOM) - Baltic Marine Environment Protection Commission.
[18] HELCOM. (2013). Climate change in the Baltic Sea Area - HELCOM thematic assessment in 2013. *Baltic Sea Environment Proceedings* 137.
[19] *International Meteorological Vocabulary*, WMO - No. 182. [available at: http://wmo.multicorpora.net/MultiTransWeb/Web.mvc].
[20] IPCC, [available at: https://www.ipcc.ch/publications_and_data/publications_and_data_glossary.shtml].
[21] IPCC (2001). *Third Assessment Report: Climate Change 2001 (TAR)*. [available at: http://www.ipcc.ch/publications_and_data/publications_and_data_reports.shtml].
[22] IPCC (2007). Climate Change 2007: *Working Group I: The Physical Science Basis* [available at: http://www.ipcc.ch/publications_and_data/publications_and_data_reports.shtml].
[23] IPCC (2007). *Climate Change 2007* (AR4). [available at: http://www.ipcc.ch/publications_and_data/publications_and_data_reports.shtml].
[24] IPCC (2007). *Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change*, Parry M. L., Canziani O. F., Palutikof, J. P. et al. (eds.), *Climate Change 2007: Impacts, Adaptation and Vulnerability*. Cambridge University Press, Cambridge, UK, 976
[25] IPCC (2012). *Glossary of terms. In: Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation* [Field, C.B., Barros, V., Stocker, T. F. et al. (eds.)]. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change (IPCC). Cambridge University Press, Cambridge, UK, and New York, NY, USA, 555-564.
[26] IPCC (2012). *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation*. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change [Field, C. B., Barros V., Stocker T. F. et al. (eds.)]. Cambridge University Press, Cambridge, UK, and New York, NY, USA, 582.
[27] IPCC (2012). *Summary for Policymakers. In: Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation* [Field, C. B., Barros, V., Stocker, T. F. et al. (eds.)]. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change. Cambridge University Press, Cambridge, UK, and New York, NY, USA, 1-19.
[28] IPCC (2013). Annex III: Glossary [Planton, S., (ed.)]. In: *Climate Change 2013: The Physical Science Basis. Contribution of Working Group I to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change* [Stocker, T. F., Qin, D., Plattner, G.-K. et al. (eds.)]. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, 1447-1466, doi:10.1017/CBO9781107415324.031
[29] IPCC (2014). Annex II: Glossary [Agard, J., Schipper, E. L. F., Birkmann, J. et al. (eds.)]. In: *Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part B: Regional Aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change* [Barros, V. R., Field C. B., Dokken D. J. et al. (eds.)]. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, 1757-1776
[30] IPCC (2014). Annex II: Glossary [Mach, K. J., Planton, S. & von Stechow, C. (eds.)]. In: *Climate Change 2014: Synthesis Report. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change* [Core Writing Team, Pachauri, R. K. & Meyer, L. A. (eds.)]. IPCC, Geneva, Switzerland, 117-130
[31] IPCC (2014). *Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change* [Field, C. B., Barros, V. R., Dokken, D. J. et al. (eds.)]. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, 1132.
[32] ISO 22301:2012, [available at: http://www.iso.org/iso/catalogue_detail?csnumber=50038].
[33] ISO 31 010, *Risk management Risk assessment techniques.*
[34] ISO Guide 73:2009, *Risk management – Vocabulary.*
[35] ISO/IEC 14001:2004, *Environmental Management.*

[36] ISO/IEC 22301:2012, Business *Continuity Management System.*
[37] ISO/IEC 26000:2010, *Social Responsibility.*
[38] ISO/IEC 27000:2013, *Information Security Management System.*
[39] ISO/IEC 31000:2009, *Risk Management*.
[40] Klaver, M. H. A., Luiijf, H. A. M. & Nieuwenhuijsen, A. H. (2011). *RECIPE project. Good practices manual for CIP policies. For policy makers in Europe*.
[41] Lauge, A., Hernantes, J. & Sarriegi, J. M. (2015). Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *International Journal of Critical Infrastructure Protection* 8, 16-23.
[42] Levina, E. & Tirpak, D. (2006). *Adaptation to climate change: key terms. Organisation for Economic Co-operation and Development (OECD)*, International Energy Agency.
[43] Martin, D. F. et al. (2005). Ecological impact of coastal defence structures on sediment and mobile fauna: Evaluating and forecasting consequences of unavoidable modifications of native habitats. *Coastal Engineering* 52, 1027-1051.
[44] Moteff, J., Copeland, C. & Fischer J. (2003). *Critical Infrastructures: What Makes an Infrastructure Critical?* Report for Congress, January 2003.
[45] Olsen, J. R., (ed.) (2015). ASCE, *Committee on Adaptation to a Changing Climate. Adapting Infrastructure and Civil Engineering Practice to a Changing Climate*, 82-93.
[46] Pederson, P., Dudenhoeffer, D., Hartley, S. et al. (2006). *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Idaho National Laboratory, Idaho Falls, ID) Report INL/EXT-06-11464.
[47] Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 11-25.
[48] Sadowsky, G., Dempsey, J.X., Greenberg, A. et al. (2003). *Information Technology Security Handbook.* The International Bank for Reconstruction and Development / The World Bank, Washington, DC.
[49] United Nations. (1997). Glossary of Environment Statistics. *Studies in Methods*, Series F 67, New York.
[50] United Nations. (2009). *ISDR Terminology of disaster risk reduction, Terminology on Disaster Risk Reduction*, United Nations International Strategy for Disaster Reduction (UNISDR).
[51] US-DHS. (2008). *Infrastructure Taxonomy. Infrastructure Information Collection Division, Office of Infrastructure Protection*. U.S. Department of Homeland Security (ver. 3).
[52] U.S. Department of Transportation, Maritime Administration. (2008). *Glossary of Shipping Terms*.
[53] US EPA, [available at: *http://www.epa.gov/climatechange/glossary.html#C*].
[54] US Homeland Security. (2007). *Transportation System, Critical Infrastructure and Key Resources*.
[55] US Homeland Security. (2013). *National Infrastructure Protection Program. Partnering for Critical Infrastructure Security and Resilience*.
[56] Website of AAPA, [available at: *http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1077*].
[57] Website of GFP. [available at: *http://www.gfptt.org/node/67*].
[58] Website of WMO. [available at: *https://www.wmo.int/pages/prog/drr/resourceDrrDefinitions_en.html*].
[59] WWF. (2010). *A Sea Exposed to Oil Accidents*. [available at: *http://wwf.panda.org/what_we_do/where_we_work/baltic/threats/shipping/*; last accessed: 29th March 2010].
[60] WWF. (2010). *Future Trends in the Baltic Sea*. WWF Baltic Ecoregion Programme.