European Research Studies Journal
Volume XXIII, Special Issue 3, 2020

pp. 339-359

Internal Whistleblowing Systems – New Standards for Active Security Management and Protection Against Systemic Risks

Submitted 03/09/20, 1st revision 29/09/20, 2nd revision 20/10/20, accepted 15/11/20

Marcin Jurgilewicz[1], Krzysztof Michalski[2], Andrzej Misiuk[3], Jozefína Drotárová[4]

Abstract:

Purpose: *The article analyzes contemporary conditions for the emergence of complex systemic threats resulting from the development of the risk industry. The authors are looking for an answer to the question whether the obligatory incorporation of internal whistleblowing systems in organizations producing dangerous products in dangerous processes with the use of dangerous devices would minimize the systemic risks resulting from organized irresponsibility.*
Design/Methodology/Approach: *The research carried out using the problem analysis method was aimed at the initial structuring of the research field and theoretical and conceptual preparation of tools for detailed exploration.*
Findings: *The conducted analysis revealed surprising constellations of interests in keeping security as low as possible. The mutual interactions between the risk industry, security administration and professional science create conditions that are particularly favorable to disasters and unlimited chains of damage. To disrupt these interactions, all organizations with a security impact should be required to install credible internal whistleblowers systems.*
Practical Implications: *The problems presented in the article will contribute to the increased awareness of the hidden dimensions of threats and the need to change the current security paradigm based on the elementarization of threats, linear-deterministic understanding of causality, Cartesian methodical skepticism, computability as the dominant objectivisation strategy, passive responsibility, crisis response and method learning trial and error.*
Originality: *The article problematizes the hitherto unknown contexts of using internal whistleblowing systems.*

Keywords: *Security management, technical safety research, corporate social responsibility.*

JEL codes: *C51, E31, E37, E64.*

Paper type: *Research paper.*

[1]*Rzeszów University of Technology, Rzeszow, Poland, m.jurgilewicz@prz.edu.pl;*
[2]*Rzeszów University of Technology, Rzeszow, Poland, michals@prz.edu.pl;*
[3]*Military University of Technology, Warsaw, Poland, University of Security Management in Košice, Slovakia, amisiuk@wp.pl;*
[4]*University of Security Management in Košice, Košice, Slovakia, jozefina.drotarova@vsbm.sk;*

1. Introduction

Increasing global competition and contemporary economic determinisms have made technological innovations the main factor of advantage in modern business. Enterprises and economies compete in rashly introducing controversial innovations, before science fully recognizes the resulting consequences, and stakeholders agree on safety requirements and conditions for the protection of people or goods at risk. Fears of the adverse effects of technological innovations and the unequal exposure to the resulting risks are now becoming a cause of violent social conflicts and an important arena for political manipulation. Even more often than fear of the harmful effects of technology, the source of this type of conflict is the growing distrust of the public opinion in the existing security systems, as well as in the reliability and adequacy of professional expertise that support these systems. The development of civic science, which owes the current dynamics to the spread of the Internet, is conducive to questioning the legitimacy of the existing methods of scientific perception and processing of security problems in technical systems.

Despite solemn declarations of concern for safety, dangerous products manufactured in dangerous processes using dangerous devices are released for sale and consumption every day, despite serious doubts as to their harmfulness to humans. How is it possible that increasingly stringent safety regulations, control procedures and thousands of workplaces causally related to security are not able to make the world safer? The analysis of the complex conditions for the implementation, diffusion and exploitation of complex, innovative technical systems reveals surprising synergies and interdependencies that create fertile ground for undesirable impacts and dangerous situations that favor cascades of damage events that are unlimited in time and space, capable of overcoming all protective barriers invented by man.

The analysis of the mutual interactions between the risk industries, professional, commercialized science and the state security administration reveals surprising constellations of interests in keeping the security of such systems as low as possible. How to stop such unwanted synergies that call into question the viability of actions taken to improve safety? People working in such enterprises have the greatest possibilities of early recognition of threats and risks, the source of which are processes, products, or industrial devices. But the employment situation of these people (for example, the lack of regulations to protect whistleblowers - often called whistleblowers - from retaliation by employers) does not make it easier for them to alert the public to the dangers of their own business. The gloomy biographies of people known from history who, in the sense of social responsibility, decided to inform the public about the dangers of running their own company, certainly do not encourage others to follow in their footsteps. Most countries do nothing to force companies that manufacture hazardous products in hazardous processes using hazardous equipment to integrate internal fraud and

threat alert systems and implement whistleblower protection programs into their organizational structures (Michalski 2017). Are properly configured whistleblowing systems really the sought-after new standard for an active, preventive security policy that will protect society from the fatal consequences of an alliance of dangerous technologies, irresponsible business, sluggish administration, and commercialized science?

2. Systemic, Combined, and Cumulative Threats and Risks

The notion of systemic threats and systemic risk is imprecise, does not yet have a universally applicable definition and is still waiting for the theoretical foundation and development of appropriate analytical tools. Systems are understood here as internally coherent assemblies of elements that are also capable of separate existence, dynamic complexes that can be separated from their environment, capable of spontaneous self-organization and autonomous action as a result of mysterious synergies - of action that cannot be understood or explained by means of elementarization, that is to say, decomposition into original components and learning how the individual components operate separately, in mutual isolation.

The systems are governed by an "invisible hand" - even though they often do not have any centralized steering or controlling authority, they have a high degree of self-organization. Systems have a paradoxical constitution: on the one hand, they are super stable super structures, on the other hand, fragile assemblies of elements, which such assemblies are at risk of disintegration. Their durability depends on the ability to neutralize environmental interference (noise) by producing operations that increase internal complexity allowing for increased synergy between components - the use of additional functions and interactions, that are not contained in separate system components. The more intrinsically complex a system is, the greater is usually its autonomy, stability, and resistance to damage.

However, there is an upper limit of complexity which, if exceeded, results in a dysfunctional system and increased vulnerability to destruction or destabilization. Systemic threats are intuitively understood as threats resulting from chaotic behaviours and synergies characterized by complex multi-agent structures. Based on the mathematical theory of chaos, it has been shown that even a simple three-dimensional autonomous square system, with a single stable balance focused on a node, can behave in an unpredictable way (Wang and Chen, 2012). Research on industrial catastrophes has highlighted how, through networks of complex, non-linear interactions and overly rigid connections, exogenous or endogenous disturbances in complex multi-agent systems can spread uncontrollably and create time-temporal and socially limitless damage events' cascades capable of overcoming any protective barriers (Perrow, 1984; Perrow, 1994; Perrow, 2007; Hofmann, 2008). The impulse to undertake research into systemic threats and risks and to reactivate the theory of systems was the Nasdaq index "bump" that occurred between 2002 and 2003 following the Enron and WorldCom scandal.

The first scientific papers on the subject were in the financial and banking sector (Kaufman and Scott 2003), but the focus of research quickly shifted towards security research and infrastructure risk analysis (Hellström, 2007; Renn and Keil, 2008; Helbing, 2009; Hellström, 2009; Rothkegel, Banse, and Renn, 2010; Büscher, 2011; Cleeland, 2011; Orwat, 2011).

Couplings between elements of a system shall be considered to be tight if there is no slacks, buffers, or flexibility between them. Then any change in the behaviour of one element necessarily affects the behaviour of the other element, whereas in the case of loose couplings, individual elements may follow their own separate logic and such peculiar behaviours of the parts do not destabilize the behaviour of the whole system. In the case of too rigid and tight connections between elements of the system there is an increased risk of so-called cascade effects associated with the spread of the disorder. The shorter the links and the stronger the couplings between the individual components of the system, the greater the speed and extent of the spread of the disturbances. Also, too big "slacks" between the components of a system causing them to behave independently of each other can result in dangerous, unpredictable interactions and a loss of ability to cushion and compensate for disturbances by spreading them over multiple security buffers.

Therefore, in the case of highly complex systems based on non-linear interactions of strongly interconnected components, disasters are normal phenomenon (Perrow, 1984; Perrow, 1994; Perrow, 2007), because a small failure of one component due to a domino effect can have serious consequences for the whole system and its surroundings (Homer-Dixon, 2006). Systemic threats and risks arise from surprising synergies, and the resulting disturbances produce either swinging effects causing loss of control of the system's behaviour, or domino effects, and the destabilizations can spread through different channels in a cascade or epidemic-like manner, hitting many components of the system simultaneously. The initiating event is most often an unexpected endogenous change in the behaviour of one of the components, or an exogenous change caused by an external stimulus or environmental pressure that some components do not withstand.

Since the mid-1980s, US disaster researcher Charles Perrow drew attention to the common features of technological and organizational systems responsible for their structural vulnerability to destabilization (Perrow, 1984), there has been a leap in complexity in the systems studied. Previously, the cause of accidents and technical catastrophes was seen only in human error (designer's error, operator's error, disregard for safety and security regulations, etc.). In his analyses, Perrow focused on two mutually independent structural features of so-called high technologies (overly complex, advanced, and innovative technologies) - types of interactions (linear - non-linear) and types of couplings between system components (loose - strong). From the combination of both dimensions a heuristic matrix was created (Perrow, 1984, p. 97) which is useful in technical systems' security analyses and

can also be used to study threats and systemic risks outside the original area of industrial activity.

Threats mean possible exogenous or endogenous deviations from the normal or desired functioning of the system, which such deviations may adversely affect everything within the system's sphere of influence. Many high-risk technical appliances have required by law protection systems to protect them from normal operating risks, such as breakdowns or unwanted events caused by unintentional operating errors. These systems usually have sufficient security "buffers" for random events, but most of these systems do not have the capacity to protect against deliberate destruction or deliberate release of destructive impacts.

Particularly in view of the increase in terrorist and cyber-terrorist threats, new concepts are urgently needed to protect against this type of hybrid, combined threats resulting from potentially highly destructive "human malice - high-risk technology" interactions. Critical, scientific elaboration is required not only by more appropriate ways to identify, perceive, describe and assess such hybrid, combined threats (combi-risk), but also by new, socially agreed concepts for preventing and protecting against such threats, by new risk management concepts (e.g. innovative insurance products), by new needs for politics and administration cooperation with modern science and by new models of public-private security partnerships.

The nature of threats that are beyond simple cause-effect patterns due to the labyrinths of complex structures and properties of systems such as, among others, self-organization capabilities, mysterious synergies, non-linear interactions, inertia, critical thresholds, sudden and unexpected phase changes, bifurcations[5], hysteresis (path dependency), feedback loops, redundancies and self-improving effects, aggregations, "snowballs", disruption cascades or delayed effects (Cleeland, 2011). Weak signals announcing the approach of a critical transition into a new state. In the case of some systems, the signal announcing the approach to a critical point may be a "critical fluctuation" (more frequent and larger disturbances), for other systems it is "critical slowing down" (increasingly slower recovery) (Scheffer *et al.*, 2009). Systemic threats and risks are often referred to in common communication in relation to possible damage which is not linked by a simple, linear, mutually explicit cause and effect relationship with the action of a specific perpetrator or a specific initiating event, which in the existing legal system means that such damages or loss cannot be the subject of claims in legal proceedings.

[5]*Bifurcations are leapfrogged changes in quality properties of a system, caused by small continuous changes in its parameters (Kuznetsov, 1995; Magnitskij, 2018).*

One of the most important factors increasing the vulnerability of modern social systems to disasters are the so-called high technologies[6]. The convergence potentials of modern technologies - including the tendency to merging and uncontrolled interactions with economic processes - combined with the different dynamics of evolution of the individual component technologies, are a source of constant mismatch, which can cause dangerous systemic disturbances.

The research of disaster analysts unanimously confirms that not only do control systems in industrial plants tend to generate hazards and risks, but also, due to internal structural factors, modern industrial infrastructures, based on the convergences of so-called different speed technologies[7], are particularly prone to disasters. A circumstance particularly conducive to the occurrence of system threats in complex systems with high importance of technological components is the frequent mismatch between management structures (organization, regulation, efficiency) and built-in technical systems. This problem is of particular importance for operators of critical infrastructures, i.e. systems on the proper functioning of which other security-critical activities depend[8].

---

[6] *Particular caution is recommended when using the following types of technologies (Michalski, 2019, p. 113):*
- high-risk technologies: high probability of catastrophic events with large numbers of victims and long lasting or irreversible consequences - technologies where disasters are normal (e.g. nuclear energy, GMOs, chemical engineering, civil air transport, hazardous waste dumps, etc.),
- highly invasive technologies, characterized by profound interference with natural processes and, at the same time, high efficiency of such interference (e.g. targeted mutagenesis technologies enabling the production of synthetic organisms that act autonomously and self-replicate),
- technologies with high transformational potential, capable of evoking radical changes in civilization (e.g. IT technologies),
- highly innovative technologies with an indeterminate development and impact potential due to the lack of an extrapolation model,
- organic, post-modern technologies with high self-production and self-organization capacities - technologies with high productivity resulting from instability that limits the possibility of external controlling and steering. Such technologies of the future only need an initial impulse, after which they operate on their own without human intervention. For more on post-modern technologies see Liebert, Schmidt, 2018, pp. 54-57.

[7] *Cyber-physical systems (CPS) connecting infrastructures with different rates of technological changes.*

[8] *The main disadvantage of modern intelligent power generation and supply systems (Smart Grid) from the security point of view is the inappropriate management model based on too rigid connections of components with IT technologies, characterized by, among other things, a large number of attack points, low standards of reliability typical for systems operated from multiple terminals and a feedback dependence on the reliability of the system, whose security they manage (Orwat, 2011).*

In the context of systemic threats, combined (hybrid) and cumulative threats are also increasingly being discussed. Combination threats are the threats that result from the co-incidence or uncontrolled interaction of several elementary threats or factors considered harmless or classified as trivial risks, provided they operate in mutual isolation. In the case of hybrid threats resulting from the coupling between natural threats and high-risk technologies, the problems are often caused by the outdated assumptions made in the past, in the authorization procedure, about the probability and magnitude of the consequences of dangerous natural events (e.g. hurricanes, floods or lack of water for cooling, landslides or seismic phenomena), which are outdated as a result of current climate change, political transformations, economic processes, social changes and other global changes (Rothkegel *et al.*, 2010, p. 156n).

Hybrid threats, which are combinations of two or more impact factors with totally different functional structures, e.g. technical risks and elementary natural threats (e.g. the Columbia space shuttle air catastrophe of February 1, 2003, the largest ever Deepwater Horizon oil disaster of April 20, 2010 or the Fukushima nuclear power plant disaster of March 11, 2011), technical risks and human factors (e.g. the Chernobyl nuclear power plant catastrophe of April 26, 1986, terrorist attacks at the WTC and Pentagon of September 11, 2001, or the Germanwings Airbus A320-211 air crash in the Western Alps of March 24, 2015). Threats which are a combination of social threats such as terrorism, sabotage or cybercrime and technical threats. Many of the problems associated with this phenomenon have not yet been scientifically recognized and explained, and these are threats with great destructive potential, capable even of causing radical political and existential changes.

Cumulative threats are defined as those occurring in areas with a high density of sources of threats with a moderate level of risk, e.g. industrial facilities presenting most often low potential for dangerous impact, but, because of their high density, posing a significant danger due to the so-called cumulative risk potential. These include problems arising, for example, from the close proximity of petrol stations and plants with a high fire risk, or warehouses for hazardous chemicals or pyrotechnics. Each of these facilities may separately have a low level of risk meeting the permit requirements, but the high density of such facilities in a small space may result in very dangerous cross effects and synergies that seriously endanger the life, health and property of many people. Solving this type of problem requires modern legal, political, planning, technical and communication instruments that enable integrated management of the risks accumulated at regional level, instead of the fragmented risk management to date at the level of mutually isolated threats' sources. Legal and ethical issues relating to the sharing of co-responsibility for cumulative risks are also of particular importance in this context.

All three types of complex threats call into question the existing models of security management based on the elementarization of threats, restrictive requirements of

strict proof, methodical scepticism, linear concept of responsibility and division of competences.

3. A "Fertile Ground" for Systemic Threats: Risk Industries, False Security Promises, and Public-Private Partnership of Interests in Keeping Security at the Lowest Possible Level

Growing global competition has made technological innovation the main advantage factor in modern business. In such conditions, enterprises and national economies compete in rashly introducing controversial innovations before science fully recognizes their implications and consequences. Complex conditions for the implementation and operation of innovative technical systems - conditions which, apart from strictly technical factors, also include the interaction of political, economic, environmental, social and cultural factors - combined with the limited predictability of the behavior of complex systems, surprising synergies, cross-influences and accumulations, make technical systems a source of serious threats, social controversy and conflicts.

Despite the political declarations that give security the highest priority, despite the systematic increase in expenditure on security and the introduction of increasingly restrictive regulations and controls on many levels, a surprising convergence of interests in keeping security at the lowest possible level can be observed. The interaction between science, politics, business and public administration creates an interesting cooperative structure consisting of agents who, guided by different strategic interests, show a consistent tendency to favor technological constellations and organizational solutions that guarantee high susceptibility to disasters (Hofmann, 2008, p. 39).

The source of contemporary security problems is not only the activities of the high-margin risk industry, for which the systematic production of threats, means of protection against threats and the liquidation of the effects of disasters is an important source of income, but also badly configured security systems, which - based on inadequate models of scientific knowledge and passive safety management result-oriented - they make false promises of safety by understating the actual level of risk.

Economic determinisms and organized irresponsibility of companies producing threats and risks (dangerous facilities, processes, products, etc.). Many of the threats associated with the undesirable peripheral effects of innovative processes or products only come to light at late stages of development, usually after a company has already incurred significant investment costs which it would like to amortize as soon as possible. This explains the companies' resistance to abandoning dangerous processes or withdrawing dangerous products, especially when there is no compelling scientific and experimental evidence of their harmfulness, which could

be used as a basis for possible legal claims[9]. Also, internal structures in companies that operate dangerous equipment and are the manufacturers that supply dangerous products to the market, combined with the aforementioned factors, contribute to, rather than prevent, catastrophic events.

The dynamic development of the so-called "risk industry" - a strong, high-margin market sector for goods and services, dealing with the effects of disasters and unwanted side-effects "after the fact occurs" is certainly not the best option for managing security, but there are an increasing number of entities that benefit from such activities. The industry benefits from the threats it produces itself, so it only does the cosmetic treatment of threats, really without eliminating their causes. In addition, the risk industry in almost every country can count on the favour of the State/government, which receives considerable revenue from the taxation of cash flows in this sector. When one takes into account the sad fact that in many accidents, potential victims also have little interest in risk and damage prevention in counting on the payment of substantial compensation and reparation, the question arises as to who really cares about safety in these circumstances and how to encourage greater involvement of stakeholders in providing it (Rothkegel *et al.*, 2010, p. 156).

Under the influence of political integration and globalization, the functions of the State/government are changing, as more and more decision-making powers (primarily in the sphere of regulations, economic policy, finance or security and defence) have been taken over by organizations standing above States/governments (e.g. the European Union). Modern countries have been significantly reduced in their functions to the role of fiscal apparatus, whose main focus is on taxing everything and prosecuting tax evaders. Since the State/government benefits from increased investment, increased production and increased sales, since it

[9] *A telling example of the companies' "irresponsibility" motivated by the desire for profit was the mass production and sale of the popular glyphosate herbicide Roundup, which has been suspected of carcinogenic activity for over twenty years. Since, in court proceedings, the manufacturer of this herbicide was able to challenge any scientific expertise confirming the causal link between long-term exposure to glyphosate and the increased likelihood of developing cancer, and to contrast against the above-mentioned expertise its own scientific expertise confirming the harmlessness of its product at the recommended dosage and protective measures, the proceedings went on for years and ended in nothing. The judgement day for the producer of Roundup turned out to be Thursday, March 28, 2019, when the San Francisco Court of Appeal shared the plaintiff's arguments, upheld the ruling of both lower courts and ordered the German company Bayer - owner of the Roundup brand - to pay USD 80.3 million in compensation to a man, for whom contact with the herbicide was considered by the experts to be an important factor that caused him to develop an invasive variety of lymph node cancer (cf. https://biznes.interia.pl/firma/news/bayer-przegrywa-przed-sadem-w-sprawie-glifosatu,2607585,1852?utm_source=paste&utm_medium=paste&utm_campaign=chrome [accessed on: March 30, 2019]).*

scrupulously taxes the resulting money flows, it is not in the fiscal interest of the State/government to prohibit the production of dangerous products in dangerous processes using dangerous equipment[10].

An additional problem is the processes of commercialization of science that force the hasty implementation of innovations before science fully recognizes their impact and understands the potential dangers arising from them. Commercialization also contributes to the growth of corruption in science and a crisis of social trust in scientific expertise (Michalski, 2011), which is clearly illustrated by the controversies surrounding the so-called *safety case* (Eckhardt and Rippe, 2016; Röhling and Eckhardt, 2017).

4. Passive Model of Security Management

Passive security - protection against consequences, crisis management - vs. active safety - influencing the causes: deterrence, prevention and building inviolability, resilience. Everything is connected to everything in a complex and often incomprehensible way, and every change - even the most inconspicuous one - is not without influence on other elements (Büscher, 2011, p. 4). Meanwhile, the current administrative procedures for security management are based on an inadequate picture of reality, an inadequate model of scientific cognition and inadequate theory of operation. Although, due to the spread of knowledge of ecology, more and more people now realize that, above all, there are complex multi-level superstructures with the abilities to act in accordance with their own logic, the abilities to self-organize and self-reproduct, which people do not always understand, yet safety management still seems to be dominated by unjustified cognitive and planning optimism, based on the Aristotelian-Enlightenment conviction of the dominance of reason over the world of the unintelligible things and an the conviction of the fundamental calculability of the world.

Until now, anti-corruption policy has been based on external control mechanisms carried out by specialized, authorized government services and agencies. The importance of internal control mechanisms was generally underestimated, as evidenced by the fact that bottom-up anti-corruption initiatives were treated solely

[10] *The degree of state involvement in confronting threats against their own citizens has been unmasked by the aforementioned global glyphosate scandal. Contrary to protests by environmental organizations, contrary to warnings by the International Agency for Research on Cancer (IARC), part of the World Health Organization (WHO), which already announced in March 2015 that this compound is likely to be carcinogenic, and contrary to calls by the medical community for glyphosate to be banned, the Member States of the European Union, after many months of deadlock, opted in late November 2017 for the renewal of glyphosate licences for five years. Only a few EU countries: France, Italy, the Netherlands and Belgium have decided to restrict the use of glyphosate in their country (see https://biznes.interia.pl/firma/news/bayer-przegrywa-przed-sadem-w-sprawie-glifosatu,2607585,1852 [March 30, 2019]).*

as a gesture of goodwill. However, such measures have had limited practical effectiveness and protected society at most from certain forms of tax or financial crime[11]. However, the abilities to control the security of complex systems based on technological components and complex, multi-agent organizational structures has so far been widely overestimated.

The traditional way to deal productively with uncertainty and indeterminacy and to influence the occurrence of unwanted events in the future is to determine the possible range of future events of this kind, to determine the frequency of their occurrence in similar situations, to draw inductive conclusions about the probability of the repetition of certain events or situations over a defined period of time, to analyse and balance the costs (potential damages and losses caused by these events and the expenditure related to preventing or reducing the probability of their occurrence) and benefits resulting from the elimination of threats, and also to calculate the risk associated with the choice of available options for action. In the context of threats and systemic risks, such a widespread approach to security can be a source of damaging, false promises of security. The widespread belief in the calculability of risk is a trap, which is from time to time reminded of by major technical disasters (Banse, 2013, p. 23).

In particular, due to the rapidly increasing complexity of interconnections in a world of hybrid cyber-physical infrastructures and the mutual mismatch between the dynamics of change at component level, traditional security management and threat protection systems based on threat elementarization, vulnerability analysis and risk calculation, are proving increasingly useless (NIST, 2014; Rossebo *et al.*, 2017).

Reductionism, which attempts to understand, explain or predict the behaviours of the system under consideration by slicing it into elements (breaking down into its original components), can sometimes be useful for some simple, elementary, single-factor threats, but is counterproductive for most complex, multi-factorial threats resulting from synergy, coincidence or accumulation of multiple causative factors.

Inadequate linear-deterministic models of scientific cognition and overstated scientific standards (mathematical evidence) prevailing in most safety-relevant areas of social life. Many of the systemic determinants of the emergence of serious threats and risk production - particularly latent risks that have not yet emerged in the form of actual disasters - cannot be captured in all their potential impacts through the prism of linear-causal assignments, according to the principles of the dominant Newtonian mechanistic model of scientific cognition, just as experimental confirmation of complex cause-effect relationships cannot be provided.

[11] *A comment on the ineffectiveness of the fight against the VAT or junk mafias.*

The Cartesian programme of methodical scepticism is a pillar of Western rationality and legal culture. The widespread presumption of innocence - including with regard to threats - combined with methodical scepticism, recommend doubt if it is not possible to demonstrate a clear cause-effect relationships between a specific action and the disasters that fall on other people. On the other hand, the epistemology of modern science requires that all doubts be resolved... to the detriment of doubts (Hofmann, 2008, p. 29).

If it is not possible to demonstrate clear linear cause-effect chains between the phenomena, the widespread passive safety model requires Cartesian methodical scepticism to be followed. With regard to many modern technologies, this means, in practice, a weighty presumption of innocence. Parcelling complex realities into narrow disciplinary fields of specialization creates favourable conditions for questioning someone else's competence, and the inadequate elementarization of complex phenomena in the positivist model of science makes complex phenomena of key importance for the functioning of modern man elusive for science.

Combined with the widespread presumption of innocence in the Western European legal culture, which recommends that any doubt be resolved ... to the detriment of doubt, this vision of science makes it difficult for people, who are exposed against their own will to serious threats, to defend themselves and makes it easier for people, who are exposing to threats, to deny their own responsibility. Due to the widespread positivist scientific cognitive model, thousands of dangerous products manufactured in dangerous processes using dangerous devices are being released for sale worldwide every day - despite justified doubts about their security, which cannot, however, be supported by laboratory simulations and other experimental evidences. This way, the positivist ideal of science - instead of contributing to the universal happiness of mankind - provides mankind with a high degree of vulnerability to misfortunes and catastrophes, favouring the dynamic development of a high-margin risk industry, which, in addition, can count on the favour of a State/government that earns considerable income from taxing dangerous transfers everywhere.

It is not in the fiscal interest of the State/government to issue bans on the production of dangerous products in dangerous processes using dangerous equipment, all the more so as government supervisory authorities gain only access to information on dangerous processes, equipment and products when the development process is completed and the production system is ready for normal start-up. As a company has already incurred investment costs that it would like to amortize as soon as possible, the resistance of companies to possible State/government bans is understandable - companies demand compelling evidences of the danger of a product, process or appliance, and such evidences - especially in the case of innovative processes or products - usually do not exist.

Due to the lengthiness of administrative proceedings and the increase in bureaucracy, State/government authorities are therefore rarely able to prevent disasters. Martin Jänicke diagnosed this situation extremely aptly: "to the problems of today, produced by the investment decisions of industry from yesterday, basing on innovations from the day before yesterday, the State authorities will react tomorrow and their reaction will have an effect the day after tomorrow" (Jänicke, 1979, p. 32n).

Inefficiency of State/government supervisory authorities. The inability of State/government and international institutions to adequately identify and respond to threats on time, the number of standards and over-regulations, and the myriad of enforcement measures, are essentially due to two reasons. Firstly, the administrative authorities authorizing highly risky or socially worrying projects are usually only given access to information about dangerous processes, equipment and products when the development process is complete, and the production system is ready for normal start-up. As companies have already incurred investment costs and are interested in amortizing those costs as soon as possible, the resistance of companies to possible State/government bans is understandable - companies demand compelling evidences of the danger of a product, process or appliance, and such evidences are usually impossible to be provided. Due to the lengthiness of administrative proceedings and the increase in bureaucracy, State/government authorities are therefore rarely able to prevent disasters.

In view of the clear differences in risk vulnerability, focusing solely on the emergence of threats, anticipating, and counteracting them may result in inappropriate or ineffective risk reduction and the emergence of secondary threats (Cleeland, 2011, p. 19n).

In the traditional passive security management model, a popular way to protect against system threats is to use security engineering solutions. However, without calling into question the sensibility of many applications of such solutions, it is worth rethinking the question of the limits of technical possibilities in ensuring safety or security. In this context, we can speak of a hopeless spiral created by the widespread increase in security of technical systems by building-in further - potentially dangerous - technical systems into them (Banse, 2013, p. 26).

The interaction of these factors creates an interesting cooperative structure composed of actors who, guided by different strategic interests, show a surprisingly consistent tendency to support technological constellations and organizational solutions that guarantee high vulnerability to disasters (Hofmann, 2008, p. 39).

5. Active Model of Security Management

The unpleasant experiences with major economic scandals, economic crises, technological catastrophes and creeping threats related to erosion processes in the

environment, in political life or related to the negative effects of civilization changes, have shaped society's awareness of the inadequacy of traditional, "demarcationist" security systems based on the "episodic" responsibility of specialized State/government bodies and the need to replace them with a modern "systemic" approach based on the post-normal model of scientific cognition[12], social co-responsibility and proactive attitudes. In security management, both at the level of States, public administrations bodies and at the level of industry organizations and companies, there is a need for a profound reorientation of attitudes - replacing the existing passive result-oriented security model (loss reduction) with an active cause-oriented model (probability reduction).

Organizational solutions to limit the destructive influence of the human factor are also urgently needed, for example, to make it more difficult to make mistakes or commit abuses, such as internal notification systems, fraud and irregularities exposing systems and programmes to protect whistle-blowers. Manufacturers and operators of technical systems - especially systems of public interest (critical infrastructures, catastrophic impact potentials, strategically important sectors for national security, etc.) - should be obligated to increase security margins and use proven ways of reducing the risk of adverse effects resulting from the loss of safety buffers, such as "firewalls" preventing the spread of disturbances (e.g. damage) between components of the system or protecting the system against malicious intrusion, constructing system structures with greater redundancy (duplication of important functions) or with greater *resilience* to cascade effects, constructed in such a way that each safety-critical component of the system can, on the one hand, count on the support of other components and, on the other hand, has a degree of self-sufficiency to ensure that functions are maintained even in the event of a serious failure of the whole system.

The proposed change to the scientific cognitive model will facilitate the identification and monitoring of systemic threats, but it will not ensure that those who contribute to such types of threats or who are responsible for protecting against such threats, shall feel responsible and shall be allowed to be held accountable for the consequences of their vulnerability. On the contrary. It is to be expected that the recognition of dangerous situations as a result of systemic impact will open the door to abuses in the form of belittling, "washing hands" and denying responsibility (*blue-washing, green-washing*). In order to prevent this, the issues of responsibility for counteracting systemic threats and responsibility for the consequences of exposing others to such threats need to be redefined by law (see

[12] *The constitutive features of post-normal science are: uncertainty of facts, disputed values, high stakes and the need to make decisions quickly, and the key requirements of this new scientific paradigm are: openness and communication of uncertainties, social authentication and inclusion - participation of all stakeholders in the process of identification, analysis and assessment of threats and in the risk decision making process (see Funtowicz, Ravetz, 1993a; Funtowicz, Ravetz, 1993b).*

Jurgilewicz 2020; Jurgilewicz, Michalski *et. al*., 2020; Jurgilewicz, Kmiotek *et al.*, 2019, Jurgilewicz, 2018).

It is worth promoting proactive attitudes of responsibility for security - so-called active security, i.e., oriented towards the causes of threats and problems - and introducing organizational solutions to encourage such attitudes (e.g. voluntary commitment schemes, CSR, trust rankings, etc.). The increasing complexity and opacity of modern organizational structures in large companies and public institutions and also complexity and opacity of external interdependencies make the existing tools for detecting and combating frauds by external supervisors increasingly ineffective. There is a need to build in mechanisms that will increase the transparency and clearness of activities and ensure a socially credible flow of information, Remedium, whistleblowing systems.

6. Internal Whistle-blowing Systems - from the Ethical Ideal to Transparency Policy to Active Security Management

The greatest potential for early identification of threats and risks arising from industrial processes, products or appliances is available to those working in such enterprises. However, the professional situation of these people (e.g. the lack of regulations guaranteeing the protection of whistle-blowers) does not make it easier for them to warn their environment about the threats arising from the activities of the company. The gloomy biographies of people who have decided to inform the public about the dangers of their own business in a sense of social responsibility, known from history, certainly do not encourage others to follow in their footsteps.

This way, the “dykes” surrounding the high-risk industry act to the benefits of entities exposing to threats, thanks to the uncertain facts, and to the detriment of the potential victims of the products authorized for production, sale and consumption, despite serious doubts about their safety or security.

The term “whistle-blowing” has been in use since 1963, when it was used the first time, following *the Otopeka case*. Whistleblowing definitions (see De Maria 1995; Jubb, 1999). Whistle-blower is a person who alerts his/her superior, a specially appointed internal supervisory or disciplinary body (ethics committee, ethics commissioner, ombudsman, compliance officer), trade unions, external law enforcement agencies or the public opinion - that is, entities that are able to effectively counteract and bring about the cessation of disturbing practices - about abuses in his/her workplace or professional environment, publicising activities that he/she believe are most likely illegal, dishonest, socially irresponsible, dangerous to people’s health and life, harmful to the environment or threatening public security. Recently, a distinction has been made between internal, employee whistleblowing and external whistleblowing (Dworkin and Baucus 1998).

External whistle-blowers are defined as persons from outside the organization alerting to irregularities (e.g. former employees), although the situation of such persons differs significantly from the specific situation of employed persons, who are exposed to "mouth shutting" and retaliatory actions by the organizations. It is widely believed that whistle-blowers are the main source of information about irregularities in companies, institutions, and workplaces of all types. The year 2002 was declared the year of whistle-blowers in the USA (Dwyer *et al.*, 2002). An important feature, the whistle-blower does not act in its own interest or on a personal revenge basis, but is guided by social responsibility, the common good and the public interest.

The most famous scandals unmasked by whistleblowing are ENRON case and WORLDCOM case. Following the disclosure of the scandals in the US, the first ever regulatory initiative to implement whistleblowing: Sarbanes-Oxley Act (SOX 2002) - Objective: To rebuild and maintain investors' confidence. 1. a new structure for the regulation and supervision of the audit industry (PCABO), 2. strengthening the responsibility and imposition of criminal sanctions on boards of directors (audit committee), 3. strengthening the Securities and Exchange Commission (SEC) and extending its authority to regulate the markets 4. establishing ethical programmes and whistleblowing procedures in companies. Protection of whistle-blowers and numerous incentives (Franze, 2002) to break the collusion of silence about corporate malpractices and the threats that arise from their activities.

High penalties, in particular, for accounting fraud, falsification of accounts, tax offences, fraud in connection with the issue of securities - often disproportionate to the seriousness of the abuse committed. The changes implemented by SOX 2002 include the establishment of procedures for whistleblowing in the event of doubts about accounting and auditing matters, the imposition of an obligation on lawyers providing legal services to companies to alert the authorities about abuses and irregularities, the establishment of legal protection for whistle-blowers against retaliation by the employer, and the introduction of severe penalties for retaliatory actions taken against the whistle-blower. The main disincentives to whistleblowing:

- The moral dilemma of the conflict between the ethical requirements of loyalty and the requirements of social responsibility,
- Negative perceptions of whistleblowing by those in the community, who identify it with denunciation, cabbage and the fears of social stigmatization or exclusion,
- Fear of retaliatory actions by the employer[13],
- Fear of losing a job and difficulties in finding it (blacklisting) (Lipman, 2012).

[13] *Retaliatory actions against whistle-blowers and their effects (Near, Miceli, 1986). The demands for their protection also appeared early on (Fox, 1993).*

Previous regulatory initiatives are less well known, such as, among others *the Public Interest Disclosure Act* - a special law implemented in the UK in 1998 to promote exposing and denouncing activity related to fraud and abuse of workers' rights in workplaces, excluding uniformed government services and agencies. In addition to the tangible economic and financial benefits that companies with internal alarming systems obtain (an average of seven times the return on invested capital), whistleblowing can also be a useful tool for deterrence[14] and early threats' identification and early warning of threats on time, so at a time when there are so-called weak signals announcing an impending disaster and it is not yet too late to prevent it or limit its destructive effects.

Transparency is considered to be one of the main pillars of a democratic State of law (Osowski and Wilk, 2016). However, it is usually understood only as the possibility for a citizen to gain access to information about all manifestations of activity (including its lack) in the area related to the functioning of specific public institutions and persons representing them, in accordance with the provisions of the Polish Act on Access to Public Information (Jabłoński, 2018, p. 47).

7. The Realities in Poland

Poland is one of the last European countries where a comprehensive package of statutory regulations ensuring transparency of public life has not yet been implemented, being in line with the standards which have been in force for several years in most countries of the world. This is combined with the controversial - balancing on the verge of constitutionality - actions of the current government and the parliamentary majority, the greatest international repercussions of which are caused by attempts to subjugate the judiciary to the executive, in violation of the constitutional principle of triple power and international standards of power balance between the three kinds of power, the delay of those in power before the implementation of systemic changes which increase citizens' control over the activities of organizations of public interest and improve the effectiveness of internal mechanisms for self-control and counteracting threats in such organizations, is detrimental to Poland's international image, which is increasingly often perceived and presented as the country where democracy is under threat. What kind of damage to the economy is caused in the modern globalized world by such a worsening reputation, which countries competing with Poland consistently

[14] *Internal alarming systems are designed not so much to catch the perpetrators of abuse "in the act" as rather to deter potential perpetrators. In Poland, transportation companies were the first ones to recognize the benefits of deterrence and started to exploit them. In order to temper the bravado of drivers, many such companies use certain elements of external whistleblowing, placing toll-free telephone numbers in visible places at the stern of the vehicles and encouraging other road users to report complaints about drivers who violate regulations, cultural rules or who put other road users at danger. Since awareness of the inevitable consequences discourages people from committing abuses, such weapons have mainly a deterrent function (Michalski, 2017b).*

use to strategically play out their own geopolitical interests - this is a complicated problem for a separate paper.

In Polish labour law there are grounds for exposing activity by whistle-blowers and for protecting whistle-blowers (Wujczyk, 2014; Świątkowski, 2015). The Act on Transparency of Public Life is to replace the Act on Access to Public Information, although experts are critical of subsequent versions of the draft law, indicating that the Act on Transparency of Public Life will restrict certain rights of a citizen in terms of access to information about the activities of State/government bodies and their officers. A problem larger than just defining the scope of public information is the misunderstanding of the need to guarantee the effective realization of a citizen's right to such information in the least formalized procedures, while transparency should be a "knee-jerk" reaction to the production of such information (Jabłoński, 2018, p. 51).

The Polish media are not short of voices of criticism of the draft act on the transparency of public life, which is supposed to embed the institution of whistleblowing in the Polish legal system (Rodzynkiewicz, 2018). The current panorama of problems related to the Polish draft act on transparency in public life was outlined in Wojciechowska-Nowak, 2012.

8. Conclusions

In the face of threats and systemic risks, the current passive security management model, focused on threat elementarization, vulnerability assessment, risk assessment, crisis response (so-called incident handling), error learning and division of competences and responsibilities, is proving increasingly useless. A high level of security for critical infrastructures requires a proactive, preventive approach to security - a cause-oriented approach that takes into account a holistic, complementary systemic perspective in all the complexities of interdependencies, couplings, cross-reactions and synergies between technological components, the biology environment, socio-organizational structures, economic determinants and regulatory-administrative actions. A systemic approach to security allows to understand the causes of dysfunctional behaviours of complex systems, build resilience by designing more adequate security margins, identify in advance "weak signals" of impending disruptions and prepare more adequate ways of dealing with systemic risks that are unremovable.

Effective overcoming of the difficulties preventing the rational handling of threats and systemic risks requires not only interference in system structures for monitoring threats, strengthening reliability and resilience to disturbances, building security buffers and barriers to prevent the spread of disturbances, but also building a security culture based on awareness of the inevitability of risks, increased organizational flexibility, transparency and understanding of prejudices, solidarity and honest communication of risks, and agreeing with the society on the need to

react and how to react. A change in the culture of security is a difficult challenge, but it is a prerequisite for an adaptive approach to the increasingly frequent systemic threats and proactive management of the associated risks (Cleeland, 2011, p. 20).

A key link in such active security management are the internal alarming systems, which act as a deterrent, on the one hand, and, on the other, enable the recognition of weak signals announcing dangerous disturbances. Public interest organizations recognizing social expectations, as well as being aware of the new types of threats and challenges to universal security, in the sense of social responsibility, should outdo each other in implementing internal alarming systems and whistle-blower protection programmes without waiting for this to become a statutory obligation in Poland. Those who do not do so on time will find it difficult to avoid embarrassing social accusations.

References:

Banse, G. 2013. Sicherheit. In: Grunwald, A. (ed.): Handbuch Technikethik, J.B. Metzler, Stuttgart-Weimar, 22-27.

Büscher, Ch. 2011. Systemic Risk as a Perspective for Interdisciplinary Risk Research. Technikfolgenabschätzung – Theorie und Praxis, 3/20, 4-12.

Cleeland, B. 2011. Contributing Factors to the Emergence of Systemic Risks. Technikfolgenabschätzung – Theorie und Praxis, 3/20, 13-21.

De Maria, W. 1995. Whistleblowing. Alternative Law Journal, 20(6), 270-281.

Dworkin, T.M., Baucus, M.S. 1998. Internal vs. External Whistleblowers: A Comparison of Whistleblowing Processes. Journal of Business Ethics, 17, 1281-1298.

Dwyer, P., Carney, D., Borrus, A., Woellert, L., Palmeri, C. 2002. Year of the whistleblower: The personal costs are high, but a new law protects truth-tellers as never before. Business Week, 3, 72-77.

Eckhardt, A., Rippe, K.P. 2016. Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, Zürich.

Fox, R.G. 1993. Protecting the whistleblower. Adelaide Law Review, 15(6), 137-163.

Franze, L.M. 2002. The whistleblower provisions of the Sarbanes-Oxley Act of 2002. Insights: The Corporate and Securities Law Advisor, 16(12), 12-21.

Funtowicz, S., Ravetz, J. 1993a. Science for the Post-Normal Age. Futures, 25/7, 739-755.

Funtowicz, S., Ravetz, J. 1993b. The Emergence of Post-Normal-Science. In: von Schomberg, R. (ed.). Science, Politics and Morality. Scientific Uncertainty and Decision Making, Dordrecht, 85-123.

Helbing, D. 2009. Systemic Risks in Society and Economics, Geneva. http://irgc.org/IMG/pdf/Systemic_Risks_Helbing2.pdf.

Hellström, T. 2007. Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework. Safety Science, 45/3, 415-430.

Hofmann, M. 2008. Lernen aus Katastrophen. Nach den Unfällen von Harrisburg. Seveso und Sandoz, Edition Sigma, Berlin.

Homer-Dixon, T. 2006. The Upside of Down: Catastrophe, Creativity, and the Renewal of Civilization. Routledge, London.

Jabłoński, M. 2018. Jawność działania władz publicznych jako dobro wspólne. Ruch Prawniczy, Ekonomiczny i Socjologiczny, 80(1), 39-52.

Jänicke, M. 1979. Wie das Industriesystem von seinen Miβständen profitiert. Westdeutscher Verlag, Opladen.

Jubb, P.B. 1999. Whistleblowing: A Restrictive Definition and Interpretation. Journal of Business Ethics, 21, 77-94.

Jurgilewicz, M., Michalski, K., Kubiak, M., Grądzka, A. 2020. The implementation of selective passenger screening systems based on data analysis and behavioral profiling in the smart aviation security management - conditions, consequences, and controversies. Journal of Security and Sustainability Issues, 9(4), 1145-1155. https://doi.org/10.9770/jssi.2020.9.4(2).

Jurgilewicz, M. 2020. Legal safety of the Republic of Poland. Journal of Security and Sustainability Issues, 9(3), 869-875. https://doi.org/10.9770/jssi.2020.9.3(12).

Jurgilewicz, M., Kmiotek, K., Dankiewicz, R., Misiuk, A. 2019. Mediation in civil matters as an example of the method used in legal security management and optimization of costs of proceedings. Journal of Security and Sustainability Issues, 9(2), 595-602. https://doi.org/10.9770/jssi.2019.9.2(18).

Jurgilewicz, M. 2018. Environmental security management from the perspective of environmental disputes resolution. Modern Management Review, 25(4), 59-68.

Kaufman, G.G., Scott, K.E. 2003. What is Systemic Risk, and do Bank Regulators Retard or Contribute to it? Independent Review, 7/3, 371-391.

Khazai, B., Daniell, J.E., Wenzel, F. 2011. The March 2011 Japan Earthquake. Analysis of Losses, Impacts, and Implications for the Understanding of Risks Posed by Extreme Events. Technikfolgenanschätzung – Theorie und Praxis, 3/20, 22-33.

Kuznetsov, Y.A. 1995. Elements of Applied Bifurcation Theory. New York.

Lipman, F. 2012. Whistleblowers: Incentives, Disincentives, and Protection Strategies. John Wiley & Sons Inc., New Jersey.

Magnitskii, N.A. 2018. Bifurcation Theory of Dynamical Chaos. In: Mohamedamen Al Naimee K.A. (ed.): Chaos Theory. IntechOpen, DOI: 10.5772/intechopen.70987. https://www.intechopen.com/books/chaos-theory/bifurcation-theory-of-dynamical-chaos.

Miceli, M.P., Near, J.P. 1992. Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees. Lexington Books, New York.

Michalski, K. 2011. Dylemat ekspertowy w ocenie technologii. Zarys problemu. Zeszyty Naukowe Politechniki Rzeszowskiej. Ekonomia i Nauki Humanistyczne, 18, 123-134.

Michalski, K. 2017a. Programy etyczne w instytucjach publicznych i ich znaczenie dla bezpieczeństwa narodowego. In: Oleksiewicz, I. (ed.). Wybrane aspekty bezpieczeństwa państwa w wymiarze zewnętrznym i wewnętrznym. Rambler Press, Warszawa, 137-163.

Michalski, K. 2017b. Programy etyczne w zarządzaniu organizacjami zainteresowania publicznego. Humanities and Social Sciences, XXII, 24 (2/2017), 181-195.

Michalski, K. 2019. Technology Assessment. Ocena technologii – nowe wyzwania dla filozofii nauki i ogólnej metodologii nauk. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów.

Near, J.P., Miceli, M.P. 1985. Organizational dissidence: The case of whistleblowing. Journal of Business Ethics, 3, 72-77.

Orwat, C. 2011. Systemic Risks in the Electric Power Infrastructure? Technikfolgenabschätzung - Theorie und Praxis, 3/20, 47-55.

Osowski, S., Wilk, B. 2016. Jawność jako zasada demokratycznego państwa prawa. Krajowa Rada Sądownictwa, 4(33), 27-34.

Perrow, Ch. 1984. Normal Accidents. Living with High-Risk Technologies. New York.
Perrow, Ch. 1994. The Limits of Safety: The Enhancement of a Theory of Accidents. Journal of Contingencies and Crisis Management, 2/4, 212–220.
Perrow, C. 2007. The Next Catastrophe. Princeton.
Renn, O., Keil, F. 2008. Systemische Risiken: Versuch einer Charakterisierung. GAIA, 17/4, 349-354.
Rodzynkiewicz, M. 2018. Projekt ustawy o jawności życia publicznego, czyli jak utrudnić działanie przedsiębiorcom. Rzeczpospolita.
Röhlig, K.J., Eckhardt, A. 2017. Primat der Sicherheit. Ja, aber welche Sicherheit ist gemeint? GAIA, 26/2, 105-107.
Rothkegel, A., Banse, G., Renn, O. 2010. Interdisziplinäre Risiko- und Sicherheitsforschung. In: Winzer, P., Schnieder, E., Bach, F.W. (eds.): Sicherheitsforschung – Chancen und Perspektiven, Springer, Berlin-Heidelberg, 147-162.
Salinger, L.M. 2004. Encyclopedia of White-Collar & Corporate Crime. Sage.
Scheffer, M., Bascompte, J., Brock, W.A. 2009. Early-warning Signals for Critical Transitions. Nature, 461/7260, 53-59.
Świątkowski, A.M. 2015. Sygnalizacja (whistleblowing) a prawo pracy. Przegląd Sądowy, (116), 6-25.
Wang, X., Chen, G. 2012. A chaotic system with only one stable equilibrium. Communications in Nonlinear Science and Numerical Simulation, 17, 1264-1272.
Wojciechowska-Nowak, A. 2012. Założenia do ustawy o ochronie osób sygnalizujących nieprawidłowości w środowisku zawodowym. Jak polski ustawodawca może czerpać z doświadczeń państw obcych? Fundacja Batorego, Warszawa. http://www.sygnalista.pl/wp-content/uploads/2016/10/AWN-Zalozenia-do-ustawy-o-ochronie-osob-sygnalizujacych-nieprawidlowosci.pdf.
Wujczyk, M. 2014. Podstawy whistleblowingu w polskim prawie pracy. Przegląd Sądowy, 6, 114-121.