NEW CHALLENGES FOR SECURITY MANAGEMENT

KRZYSZTOF MICHALSKI

DOI: 10.26410/SF_4_2/21/6

ABSTRACT

The article is of an overview and conceptual character. It presents a wide panorama of cognitive and operational problems that, for the management of the safety of technical systems and protection of the population against the effects of technical failures and catastrophes, result from the rapidly growing complexity of such systems. On the basis of the general characteristics of technical-structural, economic-organizational, political-administrative and cognitive safety & security conditions of modern technical systems, which are undergoing transformation into semi-autonomous cyber-physical systems, the author reveals surprising constellations of factors that guarantee high vulnerability of such systems to disasters. Based on the latest research on technical safety using the tools of general systems theory and system analysis, the author shows that traditional safety management systems based on inadequate, mechanistic-deterministic models of scientific cognition, limit values, external control, passive security and risk privatization are misconfigured and will not protect society against the organic, combination and cumulative risks posed by modern technology, which is increasingly working without humans. As a remedy, the author proposes a systemic, synergistic approach to security management, enabling the mobilization of all social resources to shape a safe and human-friendly technosphere. The pillar of the new model of safety management should be the popularization of knowledge about systems and system analysis, imposing on operators of dangerous technical systems the obligation to have transparent and reliable internal whistleblowing systems that guarantee protection of whistleblower against retaliation by employers, as well as complementing exclusive laboratory and expert procedures – dominant in most areas of security research – with post-normal, inclusive, interactive models of knowledge processing (Mode-2-Science), guaranteeing reflectivity, social integrity and credibility of the processes of safety assessment and risk acceptance thanks to openness to alternative points of view and thanks to the participation of stakeholders who bear the consequences of such decisions.

KEY WORDS

Systems theory, safety engineering, risk assessment, systemic (organic) threats, combination (hybrid) threats, cumulative threats.

KRZYSZTOF MICHALSKI, PHD
e-mail: michals@prz.edu.pl
ORCID: 0000-0002-2089-2160
Rzeszów University of Technology

Introduction

Most of the problems of effective protection of the population against technical threats resulting from the activities of private business producing dangerous products in dangerous processes using dangerous devices have not yet been successfully solved, and the rapidly growing complexity of systems with an

increasing share of technological components puts modern security systems against new, unknown challenges so far. The pervasive digitization, the computers being so common and the progressive networking of technological components at "different speeds" – components that previously functioned independently of one another – have caused a leap in the number of interconnections and interactions that are difficult to control with the help of previously proven cognitive and operational tools. The rapid increase in the complexity of technical systems, on which a person is irreversibly dependent on the simplest of life activities, causes dramatic changes in the security environment, to which traditional security systems have not yet adequately responded. Starting from a discussion of the current security conditions of technical systems – conditions resulting from mutual interactions between private business, politics, administration and the so-called normal science, as well as surprising constellations of interests in maintaining security at the lowest possible level – the author of the article introduces the reader to a new problem situation created by organic, combination and cumulative threats, escaping cognitive and operational control, responsible for the growing vulnerability of systems with a large share of components technological disruptions with the risk of large-scale disasters and unlimited chains of damage in space and time. As a remedy, the author proposes a reconfiguration of security systems based on internal systems of unmasking abuses and alerting about threats in enterprises conducting technological and industrial activity potentially dangerous to the environment, and replacing inadequate, scientistic models of recognition modeled on post-laboratory sciences, widely popular in most areas of security management. normal, inclusive research and consultation procedures involving stakeholders who bear the consequences of incorrect safety assessments.

Technical and structural safety limitations of complex technical systems

The digital revolution, the promotion of computers, the Internet, artificial intelligence and wireless connectivity have given technological transformations in the last quarter of a century new dynamics and caused a rapid increase in the complexity of systems based on technological components. The increase in the complexity of such systems results primarily from the interconnection of technologies of "different speeds" into complex, multi-component cyber-physical systems. Differences in the length of the life cycle of individual components and the different pace of innovation change in the industries serving them require constant structural adjustments and reorganization. The increasing structural complexity of technical systems is also the result of positive feedback loops. The growing number of connections and operations requiring security control forces the incorporation of more and more technological components into such systems (e.g. controllers, security layers, firewalls, protective barriers, failover systems, etc.), causing a hopeless spiral of increasing dependence on mutual reliability. In particular, the progressive convergence of physical and ICT infrastructures is currently the source of serious threats related to unlawful interference made possible by the openness of network-based infrastructure operated from multiple terminals. The rapidly growing number of cyber-attacks – combined with the

increasing structural complexity of technical systems increasing the risk of unwanted interactions, synergies and accumulation, favoring the emergence and spreading of disorders and limiting the possibilities of cognitive and operational control – puts humanity in front of the specter of disasters that in the case of highly complex systems with large the involvement of technological components should be regarded as perfectly normal (see Perrow 1984). Research by analysts of technical disasters and insurance statistics showing a constant increase in the number of catastrophes, accidents and various types of loss events involving technical systems (see Schweizerische Rückversicherungsgesellschaft 2008) confirm that the possibilities of cognitive and operational safety control of complex systems based on technological and complex components, multi-agent organizational structures have so far been widely overrated. The structural complexity of such systems, which is growing under the influence of the progressive cross-linking, causes that they acquire the ability to self-organize and to spontaneously behave in an unpredictable manner in accordance with their own logic, which is incomprehensible to humans. A model example of a relatively simple mechanical system behaving in an unpredictable manner is the double pendulum. Contemporary technical systems, on the other hand, are incomparably more complicated. The tendency of such complex technical systems to engage in unplanned or unpredictable behavior that can seriously threaten anything that comes within their reach, combined with the structural factors governing modern industrial activity and corporate governance systems, creates a fertile ground for disasters and calls into question the effectiveness of the security procedures commonly used in such systems.

Where does the constant increase in the complexity of technical systems come from and what are its consequences for the security of their environment will not be understood by someone who does not have at least a basic knowledge of the general theory of systems, especially synergetic (see Haken 1982). Despite the popularization of ecology, which, as the first discipline of natural sciences, broke with the 17th-century mechanistic-reductionist image of the world still dominant in other branches of natural science and focused on a holistic, "systemic" understanding of phenomena in nature without the need to disassemble them, still only a small part of society is aware of existence of systems, is aware of the capabilities of the systems and properly understands their meaning. The shaping of „systemic" consciousness is certainly not fostered by the widespread inflationary use of the word "system", which has now become "chewing gum" used to denote a variety of complex objects that are not systems. According to the classical theory, systems are dynamicinterdependent and cooperating elements that can be distinguished from the environment, showing self-preservation tendencies, having the ability to spontaneously self-organize and act autonomously thanks to the efficiency derived from mysterious internal synergies (cf. Bertalanffy 1950: 143). Despite the lack of a control center, some mysterious, invisible force (invisible hand) binds individual interactions into a harmonious whole and keeps such a variable system in dynamic equilibrium (stability through constant change), so that it is able to survive even violent exo- or engogeneous disturbances, these will not exceed a certain critical level.

The mysterious integrity of such complex systems and their extraordinary productivity cannot be understood or explained by their elementarization – breaking the whole down into its original component parts in order to know how they function separately in isolation from one another. From the knowledge of the properties and operation of individual components in isolation, it is also impossible to deduce what the final effect of their interaction will be when these components enter into complex interactions. The systems have in many respects a paradoxical living constitution. On the one hand, they are fragile assemblies that are permanently threatened with decay and react rapidly to even minor disturbances, and on the other hand, they are super-stable structures that can adapt to changes in the environment thanks to the ability to spontaneously reorganize and high productivity derived from synergy. The durability of systems depends on their ability to neutralize disturbances. Systems acquire this ability by spontaneously producing random operations that continuously increase internal complexity and increase the specialization of individual components. The increase in complexity and specialization enables the generation of new or more efficient synergies between components and the emergence of additional functions that system components do not have when operating separately. The more intrinsically complex a system is, the more autonomous, stable, and resilient it shows, until these exceed a certain critical level. However, there are upper limits of complexity, the exceeding of which makes the system dysfunctional and increases its susceptibility to destabilization (cf. Michalski 2020: 206). Due to the ability to spontaneous self-organization and the synergy of additional productivity, which enables the mutual enhancement of the effects of individual components and the emergence of new, unpredictable functions and interactions, complex systems tend to exhibit surprising behaviors that can seriously threaten everything they can influence.

The variability to which complex systems owe their ability to adapt to changes in the environment is mostly random, consisting in learning by trial and error. However, in addition to the randomness of changes, complex systems share many other structural features that increase the risk of unpredictable behavior, making them a source of serious threats to the environment. Charles Perrow – an American researcher of industrial disasters who uses systems analysis tools to identify the causes of actual accidents – already in the 1980s identified structures in complex technical and organizational systems that could threaten their own functions and everything within their range of influence. Perrow focused in his analyzes on two mutually independent structural features of complex systems: types of interactions (linear – nonlinear) and types of connections between system elements (loose – rigid). The combination of both dimensions resulted in the creation of a heuristic matrix (cf. Perrow 1984: 97) useful in the analysis of the security of technical systems, also suitable for the study of threats and systemic risks outside the primary area of industrial activity. Based on an analysis of real accidents, Perrow showed that complex systems based on non-linear interactions and rigid couplings are particularly prone to accidents and disasters, which in the case of systems such as manned space missions, nuclear energy, air transport, chemical industry or hazardous waste

landfills should be considered for something perfectly normal. Perrow's works constitute a breakthrough in research on technical safety, in which the cause of accidents and technical disasters was previously seen only in human errors (designer errors, operator errors, disregard of safety regulations, etc.). Since, in the mid-1980s, Perrow drew attention to the common features of technological and organizational systems responsible for the structural vulnerability of these systems to destabilization, there has been a rapid progress in complexity in the systems studied. First of all, due to the IT revolution, which transformed traditional, analog technical infrastructures into cyber-physical systems (CPS), there was a rapid increase in threats and systemic risks resulting from the interconnection of technologies of "different speeds", subject to different protection standards, e.g. against unauthorized interference and malicious attacks (see Michalski 2020a: 215f). Perrow's work provided an impetus to undertake more systematic, broadband research into systemic threats and risks. The first systematic scientific works on systemic threats and risks concerned the finance and banking sector (see Kaufman, Scott 2003). They were undertaken under the influence of the financial crisis that occurred in the US in 2002-2003 as a result of the Enron and WorldCom scandal. Soon, similar studies were undertaken in the field of technical and infrastructure security management, see Hellström 2007; Renn, Keil 2008; Helbing 2009; Hellström 2009; Rothkegel et al. 2010; Büscher 2011; Cleeland 2011; Orwat 2011. Thanks to the intensification of research, it has been possible to identify, on the basis of general systems theory, a number of interdependent structural factors common to complex technical systems, increasing the likelihood of surprising, unpredictable behavior or hindering the control of the processes of dissemination of disturbances, and thus creating "fertile ground" for threats and risks. systemic nature (see International Risk Governance Council, IRGC 2010; 2011).

The unexpected, undesirable behavior and interactions of complex systems are primarily favored by the aforementioned ability to generate internal synergies for increasing resource efficiency, with the limits of additional productivity generally not being inferred from the productivity analysis of individual components. The behavior of the systems is also characterized by bifurcations, i.e. abrupt changes in the qualitative properties of the system caused by small and continuous changes in its parameters. Due to nonlinear interactions between components and non-linear relationships between the behavior of individual components and the behavior of the entire system, the causes and effects of disturbances as well as the strength of stimuli and the strength of the reaction are not mutually proportional. Consequently, imperceptible changes in the parameters of a single component can have surprisingly serious effects on the behavior of the entire system, and vice versa: large changes in the parameters of individual components may, under certain conditions, not affect the behavior of the entire system. The spread of disturbances is favored by a tendency to too rigid connections between components. It is the lack of "backlash" that plays an important role in safety margins, which means that even very inconspicuous disturbances in the behavior of a single component can cause cascades of disturbances in other components, threatening with destabilization of the entire system and its tran-

sition to a different, less desirable state. Loose couplings allow individual components to operate freely according to their own logic, providing internal cushioning of disturbances that does not destabilize the operation of the entire system. However, excessive "backlash" increasing the mutual independence of component operation may adversely affect synergies between them and threaten with dangerous, unpredictable interactions or loss of the ability to cushion and compensate for disturbances by spreading them over too many safety buffers. Complex systems show a particular tendency to phase and threshold behaviors, consisting in sudden abrupt changes in state only when a certain critical threshold is exceeded. Although it is extremely difficult to recognize an impending abrupt state change early, phase transitions need not be completely unpredictable. There are both universal and specific for certain classes of systems weak signals announcing the approach of the critical threshold and the imminent transition of the system to a new state. In some systems, such a signal is "critical fluctuation" (more frequent and greater disturbances), in others it can be a "critical slowdown" (slower recovery from disturbances) (see Scheffer et al. 2009). The propensity of systems to phase behavior is related to a certain inertia, which means that disturbances do not usually result in an immediate reaction of the system. Since changes in state often require a deep reorganization of the internal structure, complex systems "postpone" shifting to a new equilibrium until the current equilibrium reaches a critical state. The length of the reaction delays is unpredictable. Complex systems have memory (hysteresis) and path dependency, which means that when a system under the influence of a stimulus or disturbance changes to a new state, after the stimulus is removed or the disturbance ceases, it does not return to the previous state along the same path, if such a return at all is possible. They are also characterized by the occurrence of feedback loops, the frequent effect of which is positive feedback amplification. Such systems react to primary disturbances by amplifying them additionally, which means that an apparently small disturbance can completely destabilize the system due to positive amplification. In this context, "positive" term has nothing to do with the assessment of changes in terms of usefulness, as they only mean the compliance of the direction of changes. How much feedback potential a system offers depends primarily on how closely its components are interconnected, not the degree of complexity. There are simple systems with strong feedback gain. The indicators of positive feedback dynamics are surprisingly radical changes in the system's behavior under the influence of disproportionately weak stimuli (cf. Michalski 2020a: 20-23). A factor that significantly limits the ability to predict the behavior of complex systems is the different susceptibility of such systems to disturbances of the same type. The same stimuli affect different systems or system elements unequally, which, due to the lack of extrapolation patterns, makes it difficult to identify early possible damage events and to estimate their probability, consequences and ailments. The susceptibility of complex dynamic systems to disturbances is constantly changing over time. The overlooking of significant differences in susceptibility or changes in susceptibility over time may result in a fateful overestimation or underestimation of the risk of specific events and erroneous forecasts of its trends

(increasing risk, decreasing risk). In addition to structural factors, an important role in generating systemic threats is also played by social factors, such as constellations and conflicts of interest, economic determinisms, technological progress and related socio-civilization changes or collective behavior – organizational and corporate, collective or mass – as well as subjective factors determining personal or institutional decisions relevant to security (cognitive or communication limitations, "perverse temptations", "malicious attacks", etc.) (Cleeland 2011: 13). Due to the interdependence of the effects of the above-mentioned factors, in the case of complex systems – especially systems based on non-linear interactions and too rigid connections of components – one should take into account the sudden occurrence of unknown, unexpected, dangerous events and situations that are difficult to rationally and responsibly manage at any time. due to cognitive limitations resulting mainly from excessive complexity and too much data requiring processing (the so-called real-time challenges). The occurrence of critical disturbances in such systems is usually diagnosed only after the fact, when such cognition has already limited practical usefulness.

Economic and organizational safety limitations of complex technical systems

The processes of economic globalization that enable drastic reductions in production costs through offshoring, combined with sharp gains in productivity through automation and robotization, have led to a radical increase in competition between enterprises and economies. In the conditions of increasing competition, innovation has become the main factor of strategic advantage. The demands of competitiveness force enterprises, industries and national economies to outdo each other in hasty implementation of innovations before science fully recognizes the resulting consequences. At the same time, the same economic determinisms force enterprises to make radical savings by limiting safety margins, often even to levels below the minimum required by law. As many of the risks and undesirable side effects of innovative processes or products do not become apparent until later in their life cycle, usually after the enterprise has already incurred certain investment costs, it is understandable that companies are reluctant to abandon unsafe processes or recall unsafe products because they fear financial losses and loss of market share. The temptation to be irresponsible is all the greater the less there is firm scientific evidence of harm that could form the basis of a lawsuit. The creators and operators of technical systems know very well what the real cognitive capabilities of modern science are, so instead of engaging ideas, forces and resources in increasing the level of security of their own activities for the environment of the management of companies, they make every effort to ensure that the possible impact of their facilities is dangerous or harmful to people and the environment, processes or products were undetectable by science. Distraction is a popular strategy. Apart from internal unmasking systems, nobody and nothing can force private businesses to take an interest in the undesirable effects of their own activity on the environment and to resign from externalization of costs. In such conditions, the expectation that commercial operators of technical systems, in a sense of social responsibility or fearing the legal consequences of their own carelessness,

will decide to give up profitable activities that are risky for people and the environment, or to incur additional expenditure on improving safety, is a manifestation of naivety.

Enterprises' care for the security of their own technical systems is less and less favored by the organizational structures of multinational corporations which, using the advantage offered by the economies of scale, have successfully dominated the most dangerous sectors of modern industry. The structures for managing the activities of such agents do not respect national borders and legal systems, which places them above the law in many ways. Despite the use of anti-monopoly mechanisms, the progressive expansion of capital results in the emergence of ever larger conglomerates gathering interdependent types of activities in one portfolio, enabling effective circumvention of the law, externalization of costs, masking abuses and dispersing liability. The unequal position of local administrations authorized to supervise territorially limited parts of cross-border operational networks (production, logistics, commercial, etc.) ensures that the applicable safety standards will not be enforced in practice.

The industrial production of risks raises new security needs for those exposed. In response to them, the risk industry is dynamically developing – a new, high-margin segment of the goods and services market, which is not afraid of catastrophes and crises. There are manufacturers of technical security, rescue equipment, specialist medical equipment, drugs, protective measures, as well as insurance companies, companies providing security services, law firms specializing in extorting damages, and companies that profit from removing damage and reconstruction. Stakeholders' propensity to take risk has increased rapidly since modern insurance products have emerged on the market that can spread risk. Insurance products generate a paradoxical compliance of interests in keeping security at the lowest possible level, giving those who risk a guarantee that they will not bear the costs of their own bravery or carelessness, and the exposed ones hope for a payment of generous damages. In this situation, an obvious question arises who, in such conditions, may still care about the safety of technical systems, prevention of disasters and damage incidents (Rothkegel et. Al. 2010: 156). Insuring against various types of risks resulting from technical activities, crisis management and disaster recovery is certainly not the best strategy for managing the security of technical systems, but there are also entities that profit from disasters and are interested in maintaining the security of such systems at the lowest possible level. As the industry ultimately benefits from the risks it generates, it should not be expected to increase its commitment to safety. As long as competition mechanisms force enterprises to limit safety margins to the absolute minimum, and as long as the industry profits from the systematic production of risk, private technological and industrial business – instead of counteracting threats – will be limited only to their cosmetics.

Political and administrative limitations of security of complex technical systems

In any market economy country, industries profiting from the production of hazardous products in hazardous processes with hazardous equipment can rely on the favors of the state gaining revenues

from the sale of permits and the taxation of cash flows in these thriving sectors. The plague of lobbying and corruption ensures special protection of the state for dangerous industries. Big concerns have long discovered that the fate of innovation depends much more on political conditions than on market power, and the success or failure of investment in innovation depends on whether the appropriate political conditions have been prepared in advance for innovation to have a secure outlet by virtue of laws that will force consumers to buy them. Lobbying and corruption guarantee risk-free introduction of innovative products and processes to the market with minimal own capital investment (see Karapiperis, Ladikas 2004). Instead of spending a lot of money on the research and development process, optimization and advertising of a new product, companies prefer to spend relatively small amounts on remuneration for lobbyists, PR and gifts for sympathetic politicians who will legislate to guarantee the success of even the most useless innovation.

A smaller and smaller part of the public believes that the applicable legal regulations, security standards and administrative supervision procedures will effectively protect citizens from exposure to threats resulting from technological and industrial activities of private business. This is because administrative authorities that issue permits or exercise official supervision over the security of technical systems have, as a rule, limited possibilities of accessing up-to-date information on the condition of facilities, devices and processes used by private enterprises and on their impact on the environment. Institutions usually obtain such information with a long delay, when the development or investment process is completed and the problematic production system is ready for commissioning and operation. As operators of innovative technical systems are vitally interested in amortizing their capital expenditure as quickly as possible, their reluctance against possible administrative operating bans is understood. In such situations, companies demand compelling scientific evidence to prove the harmfulness of a product or process, and in the absence of such evidence, they are ready to sacrifice to defend their interests in lengthy, multi-instance court proceedings. Whistleblower activities are often the only source of information about what is happening behind the walls of private companies, in view of the ineffectiveness of state oversight of complex technical systems. As companies are aware of the dangers of their own employees' whistleblowing activities, they keep the dark truth about the security of their facilities, processes and products secret through confidentiality obligations and retaliation against employees who dared to break their silence (see Near, Miceli 1986; Lipman 2012). Despite the introduction of legal regulations in the world to provide such people with better and better protection, the sad lives of most employees who, in a sense of social responsibility, decided to testify against their own employers, do not encourage others to follow in their footsteps (cf. Michalski 2020b: 37f.).

The inadequacy of regulations resulting from the growing mismatch between the pace of legislative processes and the dynamics of technological progress and the requirements of enforceability, combined with excessive formalization and bureaucratization of administrative proceedings and noble minimalism characterizing the involvement of public officials in the performance of their profession,

means that state authorities are rarely able to effectively prevent catastrophes or crisis situations. resulting from the increasing complexity of technical systems in the hands of private businesses. The enforceability requirements force the legislator to precisely define the limit values of harmful doses or hazardous impacts, which in practice means limiting the supervision to direct, measurable, physical effects on humans and the environment, which may be the subject of claims in court proceedings, and excluding the risks resulting from long-term exposures outside the limits difficult to model under the time constraints of laboratory experiments, but above all, irrational, cumulative and diffuse interactions, the origin of which cannot be reconstructed by means of mutually unambiguous cause-effect relationships. The necessity to enforce selective and incomplete safety standards is not facilitated by the slowness of state authorities, which in most countries usually react to the problems identified yesterday and resulting from the innovations introduced the day before yesterday only tomorrow, and their reaction is effective the day after tomorrow (Jänicke 1979: 32f.). Because the lack of compelling scientific evidence of harm – perfectly normal in the case of non-measurable or cumulative effects that cannot be precisely separated and attributed to a specific source – guarantees the failure of any litigation, rather than a comprehensive, active, creative and intelligent confrontation with the risks of commercial activities based on complex technical systems (airports, chemical engineering, landfills, radars and cell phone masts, transmission infrastructure, biotechnology laboratories, etc.), the main attention of the services responsible for security and civil protection is focused on reacting"wise after the event" for producing procedures and observing them without reflection (Michalski 2020b: 40). Administrative safety oversight systems are improperly configured, they are based on excessive allocation of tasks favoring mutual questioning of other people's competences and hindering harmonious cooperation between institutions, which are skilfully used by private businesses conducting technical activities that are dangerous to people and the environment, diversifying the risks of their own operations in such a way that accumulated highly harmful impacts were within official limits established for single agents. Regardless of the above-mentioned political and organizational conditions, the key condition for the possibility of effective protection against the dangerous or harmful effects of more and more complex technical systems is undoubtedly the cognitive control of this complexity. However, the situation in the world of professional science is not conducive to achieving this goal.

Cognitive security limitations of complex technical systems

Private business conducting dangerous technological activities can count not only on the favor of the state, but also on reliable support from professional science, whose processes of progressive commercialization involve increasing financial dependence on private capital and "dangerous relations" with the risk industry. The organic, combinational and cumulative hazards arising from the complexity of technical systems are a blind spot in the field of laboratory science, which has a monopoly on security in many areas. These sciences operate with inadequate, mechanistic-reductionist models of cognition based on elemen-

tarisation, ever narrower specialization, and excessively inflated requirements of accuracy imposed on scientific evidence. The Cartesian, mechanistic model of cognition that considers the reduction of complex phenomena to elementary component parts and simple linear causal relationships as the right way to understand reality, and an in-depth study of how these parts work in mutual isolation, combined with methodical skepticism, which recognizes quantifiability as the only valid objectivization strategy, results in the exclusion of complex, immeasurable and incalculable aspects of reality beyond the area of scientific interests and recognizing them as the domain of uncertain facts and "conspiracy theories" (Jurgilewicz, Michalski 2020: 16). The possibility of arbitrarily omitting immeasurable impacts in risk analysis and assessment under the pretext of "objectification" is commonly used to artificially lower the actual levels of risk in order to build public acceptance for controversial projects. As a consequence, normal science more or less deliberately erects walls around the dangerous industrial activities of private business in the form of factual uncertainty that gives rise to a "presumption of innocence" and allows open-ended contestants to challenge the claims of vulnerable and injured parties. Scientific evidence not only dispels doubts related to the safety of projects, facilities, processes and technological products less and less often, but due to the acceleration of technological changes, the waiting time for such evidence is definitely too long to effectively protect the population from exposure to damage and dangers resulting from the activity technological and industrial private business.

Expert studies on the safety of the impacts of industrial installations or technical infrastructure facilities conducted from the perspective of an uninvolved observer – often "from behind a desk" – do not take into account many conditions and safety aspects relevant to local stakeholders who perceive many dangers from the perspective of a participant who will be hit by the effects of incorrect risk assessment and wrong decisions made on their basis. The overly complicated language of scientific safety research reports means that many stakeholders are considered incompetent to form their own opinion on their basis. The lack of faith of local communities concerned about the vicinity of dangerous installations in the truth and sincerity of scientific promises of their safety is often due to the awareness of what fields for abuse and the possibility of manipulating the results are opened by the objective and functional complexity of security research, which is certainly one of the most complex phenomena that have ever been the subject of scientific cognition. Many scientists involved in researching the safety of objects, processes or products treat the critical attitude of stakeholders to scientific expertise as a refusal to confront the current state of scientific knowledge resulting solely from unfounded prejudices (cf. Röhling, Eckhardt 2017: 105). Such an arrogant approach to the concerns of people concerned about the vicinity of dangerous industrial installations or exposed to unknown influences of objects or products is certainly not conducive to eliminating possible prejudices.

The falsity of scientific promises of security is destructive primarily on two levels: it increases the tendency of industry to take more and more risks and is a source of increasing confusion and violent social

conflicts over technological ventures and innovations. The uncertainty of facts and information chaos create fertile ground for manipulation and broadband disinformation operations, which, thanks to the dissemination of social media, have now become a cheap, effective and easily masked combat means that allows for interfering in the internal affairs of states, inciting social unrest, destabilizing political processes and causing threatening crises internal security and continuity of development (see Singer, Brooking 2018). It is widely believed that among the countries that use fake news on a large scale as a disinformation weapon to cause information chaos and confusion in other countries, undermine trust in the institution of legitimate power and incite social unrest, internal divisions and conflicts, no country can match Russia in the game of a social media keyboard (see Kettemann 2019: 1).

In view of the growing importance of innovation in the internal security policy, neoliberalism has become widespread, which, instead of limiting the risks resulting from the complexity of technical systems growing under the influence of constant changes, consistently strives to privatize these risks. Instead of forcing responsibility for the undesirable effects of one's own activity on others, the liberalization strategy forces every citizen to be a manager of his own life risks and to insure himself against the unpleasant consequences of someone else's carelessness (cf. Clausen 2003: 60). In an egoistic, neoliberal society driven by an economic calculation of purely personal gains or losses – a society whose members fear nothing more than being the last link in a chain in which one pushes the costs, risks and undesirable side effects of their own ventures onto one another – understandably NIMBY becomes a self-defense strategy (Stankiewicz 2017: 289f.). The growing opposition of local communities to technological ventures, capable of stopping the implementation of even very advanced projects of strategic importance for the development of countries or regions, makes us aware, however, of the dire consequences of such a security policy.

Conclusions

Organic threats resulting from the increasing structural complexity of modern technical systems, related to the ability of complex technical systems to self-organize and operate without human knowledge and participation, combination (hybrid) threats related to uncontrolled coincidences and cross-effects of various factors, which are themselves relatively harmless under provided that they operate in mutual isolation, and the cumulative risks associated with the concentration of hazardous impacts, each of which – considered separately – are within the limits of tolerable risk, pose new challenges to security management in enterprises and public administration. The fact that in complex systems based on technical components, disasters and undesirable behavior become something more and more normal does not mean that prevention, anticipation, monitoring, error elimination and caution are completely useless in such systems (see Büscher 2011: 10). The awareness that such actions in the context of complex systems do not guarantee 100% security will facilitate the understanding that the existing ways of protecting society against threats from increasingly destructive technical systems are insufficient and in the face of the great challenges faced by modern societies, a thorough revision and recon-

figuration of traditional societies is needed. security systems. Limiting "systemic" risk resulting from the power of synergy requires "systemic" action, based on the power of synergy. For this purpose, the security systems must be reconfigured so that, instead of being a random cluster of autonomous, mutually incompatible elements, they create a healthy organism capable of spontaneous self-organization and producing surpluses thanks to internal synergies. A prerequisite for success is the harmonious combination of technical optimization with the reorganization of social hazard monitoring systems. Many of the self-organizing and adaptive abilities of complex technical systems mentioned above can be used to reduce systemic risk (see Helbing 2009). The identification and analysis of systemic threats should begin with determining whether the system in question is complex in the sense discussed above. Then, internal, endogenous factors that may be involved in the occurrence of uncontrolled adverse events should be identified. When designing technical systems, particular attention should be paid to leaving sufficiently wide margins of safety in the form of reserves, stocks and "clearances" protecting the technical system against unpredictable overloads, as well as against the effects of inaccuracies resulting, for example, from simplifications necessary to perform static calculations. Such actions result not only from the fear that in theory there may always be some error in the calculation, but also from the fear of uncontrolled interactions, synergies, cross-effects or accumulation between technical systems or their components and elements of the environment. In the case of already existing systems, it is necessary to check on an ongoing basis whether the built-in safety margins are still sufficient. A sudden loss of such margins resulting from e.g. excessive complexity, overloading, shortening and over-stiffening of connections or strengthening of interdependencies between components may significantly increase the susceptibility of systems to destabilization, additionally limiting the low predictability of their future behavior. Leaving or rebuilding appropriate safety margins (buffers, reserves, gaps, flexibility, etc.), using "firewalls" to prevent the spread of disturbances (e.g. damage) between system components, using barriers to protect systems against errors or malicious human interference, and building system structures with greater redundancy (duplication of important functions) or greater resistance, which make each component of the system important from the point of view of safety supported by other components, and at the same time it has adequate self-sufficiency guaranteeing the preservation of functions even in the event of a serious failure of the entire system (cf. Cleeland 2011: 17) are proven methods of reducing the risk of undesirable behavior in complex systems offered by modern security engineering. However, security engineering providing a wide range of increasingly advanced technical security measures will allow only a small shift of security boundaries, if technical improvements are not combined with forcing producers of goods and operators of dangerous installations to care more about the safety of their own operations and greater responsibility for its consequences for the environment. In view of the ineffectiveness of traditional administrative oversight procedures, a statutory obligation should be imposed on companies engaged in potentially hazardous technology activities to embed credible

whistleblowing and whistleblower protection mechanisms into their internal management systems (see Jurgilewicz et al. 2020).

Bibliography

Bertalanffy L. von (1950): An Outline of General System Theory, „The British Journal for the Philosophy of Science" 1, 2 (Aug. 1950): 134-165.

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

Clausen, L. (2003): Reale Gefahren und katastrophensoziologische Theorie, [in:] Clausen, L., Geenen, E.M., Macamo, E. (eds.): Entsetzliche soziale Prozesse. Theorie und Empirie der Katastrophen, Münster: LIT Verlag: 51-76

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

Haken H. (1982): Synergetik, Berlin-Heidelberg-New York: Springer.

Helbing, D. (2009): Systemic Risks in Society and Economics, Geneva: International Risk Governance Council (IRGC)(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 (2007): 415-430.

Hellström, T. (2009): New Vistas for Technology and Risk Assessment? The OECD Programme on Emerging Systemic Risks and beyond, „Technology in Society" 31, 3: 325-331.

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

IRGC – International Risk Governance Council (2010): The Emergence of Risks, Geneva.

IRGC – International Risk Governance Council (2011): Improving the Management of Emerging Risks: Risks from New Technologies, System Interactions and Unforeseen or Changing Circumstances, Geneva.

Jänicke, M. (1979): Wie das Industriesystem von seinen Mißständen profitiert, Opladen: Westdeutscher Verlag.

Jurgilewicz, M., Michalski, K. (2020): Teoretyczno-metodologiczne podstawy nauki o bezpieczeństwie, [in:] Jurgilewicz, M., Michalski, K., Krztoń, W. (eds.): Badania nad bezpieczeństwem. Wybrane aspekty, Rzeszów: Oficyna wydawnicza Politechniki Rzeszowskiej: 13-48.

Jurgilewicz, M., Michalski, K., Misiuk, A., Drotárová, J. (2020): Internal Whistleblowing Systems – New Standards for Active Security Management and Protection Against Systemic Risks, „European Research Studies Journal", 23 (3): 339-359.

Karapiperis, T., Ladikas, M. (2004): Organised Interests in the European Union`s Science and Technology Policy – The Influence of Lobbying Activities, [in:] Decker, M., Ladikas, M. (eds.): Bridges between Science, Society and Policy. Technology Assessment – Methods and Impacts, Berlin-Heidelberg-New York: Springer: 129-142.

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

Kettemann, M.C. (2019): Internationale Regeln für soziale Medien. Menschenrechte wahren und Desinformation bekämpfen, Bonn: Global Governance Spotlight, Stiftung Entwicklung und Frieden.

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

Michalski, K. (2020a): Ochrona infrastruktur elektroenergetycznych przed zagrożeniami i ryzykami systemowymi – nowy paradygmat w zarządzaniu bezpieczeństwem energetycznym, "Rocznik Bez-

pieczeństwa Międzynarodowego", 14, 1: 200-220.
Michalski, K. (2020b): Ochrona przed zagrożeniami systemowymi jako nowy obszar badań i zadań dla polityki bezpieczeństwa, [in:] Delong, M., Puacz-Olszewska, J. (eds.): Współczesna polityka bezpieczeństwa w Europie Środkowo-Wschodniej. Uwarunkowania – Wyzwania – Zagrożenia, Rzeszów: Oficyna Wydawnicza Politechniki Rzeszowskiej: 9-54.
Michalski K. (2020c): Metodyka analizy ryzyka i oceny bezpieczeństwa, [in:] Jurgilewicz, M., Michalski, K., Krztoń, W. (eds.): Badania nad bezpieczeństwem. Wybrane aspekty, Rzeszów: Oficyna Wydawnicza Politechniki Rzeszowskiej: 49-86.
Near, J.P., Miceli, M.P. (1986): Retaliation against Whistle Blowers: Predictors and Effects, „Journal of Applied Psychology", 1 (71): 137-145.
Orwat, C. (2011): Systemic Risks in the Electric Power Infrastructure?, „Technikfolgenabschätzung – Theorie und Praxis", 3/20 (2011): 47-55.
Perrow, Ch. (1984): Normal Accidents. Living with High-Risk Technologies, New York: Basic Books.
Renn, O., Keil, F. (2008): Systemische Risiken: Versuch einer Charakterisierung, „GAIA" 17/4 (2008): 349-354.
Röhlig, K.-J., Eckhardt, A. (2017): Primat der Sicherheit. Ja, aber welche Sicherheit ist gemeint?, „GAIA" 26/2 (2017): 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, Berlin-Heidelberg: Springer: 147-162.
Scheffer, M., Bascompte, J., Brock, W.A., Brovkin, V., Carpenter, S.R., Dakos, V., Held, H., van Nes, E.H., Rietkerk, M., Sugihara, G. (2009): Early-warning Signals for Critical Transitions, „Nature" 461, 7260: 53-59.
Schweizerische Rückversicherungsgesellschaft (2008): Natur- und Man-made-Katastrophen im Jahr 2007: hohe Schäden in Europa, sigma Nr. 1/2008, Zürich.
Singer, P.W., Brooking, E.T. (2018): LikeWar: The Weaponization of Social Media, Boston: Mariner Books.
Stankiewicz, P. (2017): Gra w atom. Społeczne zarządzanie technologią w rozwoju energetyki jądrowej w Polsce, Toruń: Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika.

About the Author

Krzysztof Michalski, PhD., Assistant Professor at the Department of Project Management and Security Policy, Faculty of Management, Rzeszów University of Technology (Poland). He specialize in Philosophy of Science and General Methodology of Science, Technology Assessment, Foresight & Forecasting, Methodology of Safety & Security Sciences, Risk Assessment & Management, Interdisciplinary Safety & Security Research in selected areas (technical safety, industrial safety&security, health & safety in work environment, security and protection of facilities, disaster resilience & protection, security of local communities, crisis management).