



Publisher

<http://jssidoi.org/esc/home>



THREATS AND THEIR TRIGGERS IN THE GLOBALIZED ECONOMY*

Dagmar Kopencova ¹, Vladimir Sulc ², Roman Rak ³, Magdalena Naplavova ⁴, Frantisek Vlach ⁵

^{1,2,3,4,5} Department of Security and Law, AMBIS University, Lindnerova 1, 180 00 Prague 8, Czech Republic

E-mails: ¹ Dagmar.Kopencova@ambis.cz; ² Vladimir.Sulc@ambis.cz; ³ Roman.Rak@ambis.cz;
⁴ Magdalena.Naplavova@ambis.cz; ⁵ FVlach@avs.justice.cz

Received 10 April 2022; accepted 25 May 2022; published 30 June 2022

Abstract. The paper deals with security issues in a globalized, economically oriented world. The authors present a general, theoretical-practical view of a systemic, object-process approach to analysing security threats of various categories. The paper generally analyses and categorises the sources and characteristics of threats according to various factors, which in practice may pose a threat to objects of interest or processes that have significant value for their owners. Emphasis is placed on threats of an economic, social, societal, or political nature that are typical of societies today, primarily unilaterally oriented towards economic gain. The authors' approach is purposefully general so that it can be applied to all sectors where security analysis is necessary i) to identify threats, weak spots in protected objects, states, or processes, ii) to discover vulnerabilities, iii) to realistically assess risks and propose protective measures.

Keywords: Threat; hazard; threat source; agent of threat; vulnerability; threat impact; economy; security; risk management

Reference to this paper should be made as follows: Kopencova, D., Sulc, R., Naplavova, M., Vlach, F. 2022. Threats and their triggers in the globalized economy. *Entrepreneurship and Sustainability Issues*, 9(4), 139-155. [http://doi.org/10.9770/jesi.2022.9.4\(7\)](http://doi.org/10.9770/jesi.2022.9.4(7))

JEL Classifications: C88, H56, J11, J15, F22, F24, F52

Additional disciplines: security, risk management, sociology, information system, informatics

1. Introduction

A globalized economy is not just a global market for products or services. The global economy is also strongly interconnected with raw materials and energy resources (Androniceanu, Căplescu, Tvaronavičienė, Dobrin, 2021; Borodin, Tvaronavičienė et al., 2021), which can become significant threats to individual states and their economic groupings if the global balance is disturbed (Alanen, Linnsmaa et al., 2022). With the change in the global division of the world, the transport routes for energy, raw materials, and goods have also changed (Hudecova, 2021a; Hudecova, Chriastel, 2021).

* The research has been funded by Department of Security and Law, AMBIS University, Czech Republic

In addition, high levels of industrial specialisation have blinded or rendered politicians and many economists incapable of taking a comprehensive view of the interdisciplinary world. This has been evident during the current military conflict in Ukraine and in the years prior to it as well. When diplomatic means of resolving such conflicts have been exhausted, they are often decided through conventional military mean, but also information warfare (Sopilko, Svintsytskyi et al., 2022; El Kafhali, El Mir, Hanini, 2022), thereby influencing the views of the population and economic blockades. Economic blockades reflect the complex interconnectedness of the world economy (Kharlamova, Stavytskyy, Fedorenko, 2021) and globalized world. They can be very unpredictable even if they seem simple at first glance. One of the major threats in the 21st century is the huge migration of populations (Besenyő, 2016; Alkopher, Blanc, 2017; Alkopher, 2018; Kriviņš, Teivāns-Treinovskis, Tumulavičius, 2021) between continents and individual states, especially with regards to Islam. In recent years, pandemics such as COVID-19 have also become a significant threat (Besenyő, Kármán, 2020; Tušer, Jánský, Petráš, 2021) in particular with regards to their impact on the economic, social (Stefan et al., 2020; Jackulikova, Vrankova et al., 2022), and political environments. The connection between phenomena (threats), events (adverse events), threat to object, object destruction, and security event is presented below in Table 1.

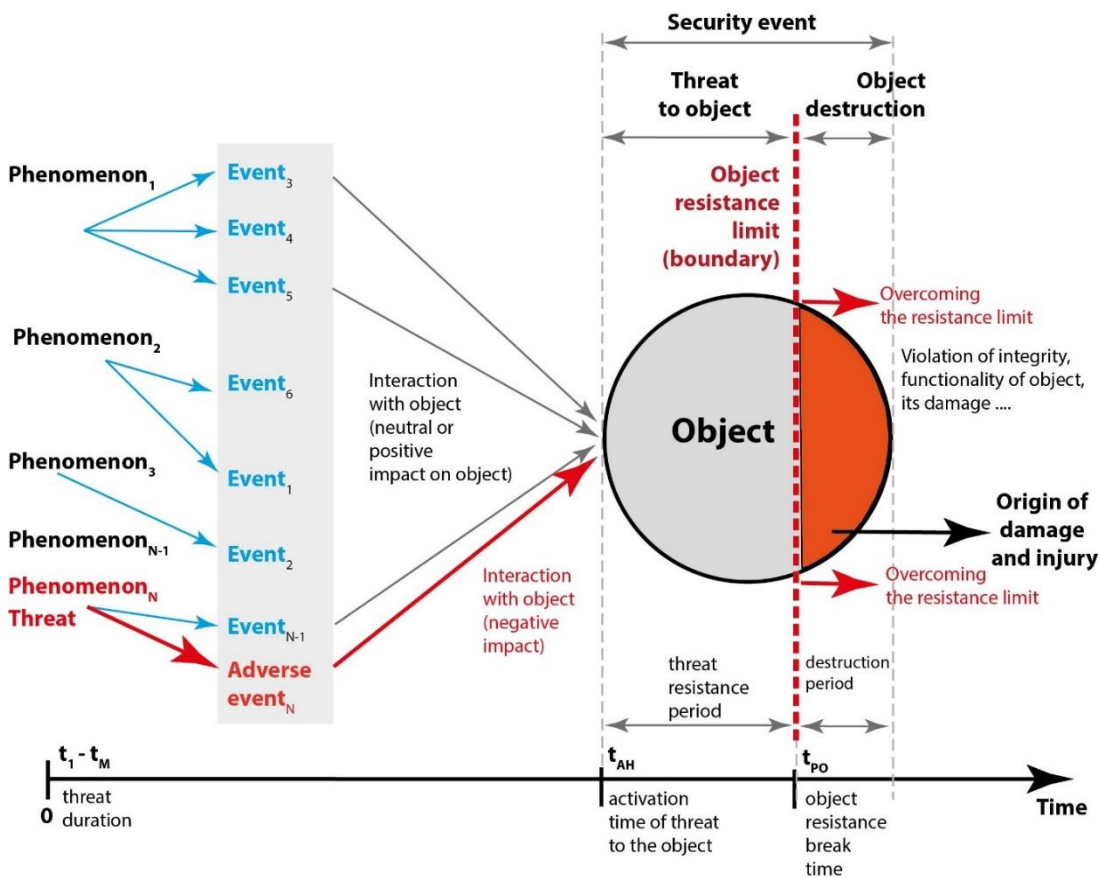


Figure 1. The connection between phenomena (threats), events (adverse events), threat to object, object destruction, and security event.

Source: Roman Rak

Today, security is part of every human activity (Adams, Chisnall et al., 2021). There are countless theoretical definitions of security, one more complex than the other (Hudecova, 2021b). However, from the simplest point of view, security is the preservation of the continuity of a particular state, process, or object. This can be our health, life, employment, the existence of a company, its sustainable development, business continuity, economic prosperity, a prosperous national economy, etc.

In a globalized world, sustainable development can therefore be understood as a security phenomenon in today's highly competitive environment full of diverse threats and the resulting risks (Tušer, Hoskova-Mayerova, 2020a; 2020b).

For effective security analysis, including economic security, it is, therefore, useful to look systematically through the prism of elementary objects, states, processes and the properties that determine their behaviour, including strengths and weaknesses, such as vulnerability in an environment full of real threats. We can understand security both regionally and globally (Chehabeddine, Tvaronavičienė, 2020). At present, threats involve digital technologies and cyberspace (Manulis, Bridges et al., 2021) more than ever before. Hybrid threats are also becoming part of the scene (Atkinson, Chiozza, 2021).

The impact of various events on an object is either neutral, positive, or negative, each object having its own resistance to a specific type of negative event (threat). This resistance is a property an object possesses, one which indicates a certain limit (boundary), with the object usually being resistant to several types of threats (Hammoudeh, Watters et al., 2021).

2. Material and methods

We encounter the term “threat” in all security analyses. Threats exist in all fields of human activity - in industry, energy, economics (Periokaite, Dobrovolskiene, 2021), healthcare (Kharaihvili, Blake et al., 2021), military, critical infrastructure, information technology (Rak, Felcan, Kopencova, 2021), social sphere (Jackulikova, Vrankova et al., 2022; Jüzl, Vlach, 2022), politics, social sciences, etc. Generally speaking, threats can be any theoretical phenomenon that can negatively impact a protected object (protected asset), i.e. it has the potential to cause damage or injury.

At the Academy of the Police Force in Bratislava (Slovak Republic), a scientific research task was initiated to establish the new scientific field of Security Sciences. This new scientific discipline should theoretically address general safety in any field of human activity. One of the first tasks was to compare and unify the basic definitions used in domestic and foreign literature (Botrugno, Malagnino et al., 2022; Ansari, Pandey et al., 2022). In the first phase, an extensive literary search was conducted as part of the solution of the theoretical task (Ajdari, Asgharpour, 2011; Dirnbach, Kubjatko, 2020; Rak, Kopencova, Felcan, 2021). It was found that basic concepts are perceived differently by various security entities - security forces, scientific institutions, companies, and government institutions. The same concept can be perceived or defined identically, similarly, or even oppositely (Ni, Zou and Chen, 2022). The different perceptions of security concepts depended mainly on the field of human activity. For this reason, literary searches were repeated in several subsequent iterations for sources of domestic and foreign literature (Matuszak, Jaskiewicz et al., 2015; 2017). A dictionary of basic security terms and their definitions was then created. In the next phase, the Delphic Fortune Teller method was applied, whereby leading security experts were invited to comment on the results obtained from the search or to define or clarify the basic concepts themselves. Their comments were analysed and subsequently subjected to a complex synthesis. This gave rise to the definitions of threat, hazard, agent of threat, and their further subdivisions. For a better understanding, graphical methods were used to illustrate process relationships and dependencies.

3. Hazard

A **hazard** is understood to be the possibility to activate danger (a threat) in a specific time and space, respectively the source, actor of possible death, injury, or damage to health, causing damage or injury. In literature, a hazard also indicates all factors (threats) that can cause negative phenomenon. A hazard exists independently of the activities and behaviour of the reference object (subject) and the object causing the threat (Buzalka, Blažek, 2011). We can understand a hazard as being a security event.

A **hazard** is a condition affecting humans, objects, systems, processes, or the environment arising from activities (events, processes), whose hazardous properties have not been fully taken into account in ensuring security. Hazard reduction is achieved by minimising the acting agents (causes, sources of threats) implementing organisational and personnel measures, and through the design of a number of active and passive security elements (modified, expanded according to Šimák, 2015).

Within the field of occupational health and safety, various authors have defined a hazard as follows:

1. A **hazard** is a source of possible damage or injury to an object, process, or system from certain exposure and under certain conditions.
2. A **hazard** is a set of conditions created by humans or their interaction with natural influences or technical equipment, which results in the possibility of damage or injury to objects, processes, or systems.
3. A **hazard** is an active property of an object, process, or system (e.g. material, machinery, work activity, technical equipment, technology, or the specific situation) that causes a negative phenomenon that results in damage or injury. A hazard is only present if a person, the environment, property, or other values can potentially be exposed to an activated hazardous property.

A **hazard to an object** can be more narrowly defined as **the process resulting in the threat to an object being activated, whereby the limit (boundary) of the object's resistance has not yet been exceeded, i.e. no damage or injury has (yet) been caused**. When a hazard to an object occurs, object monitoring is usually activated and possible security measures implemented if the resistance limit is exceeded, or to prevent further hazard to the object or to increase its resistance.

Example:

A tree bends strongly in a storm, but the branches and the trunk of the tree do not break. For preventive reasons, objects in the surroundings that could be damaged by falling branches or the trunk are cleared away and the area is closed off to the public. If it concerns a small tree, a stake is hammered into the ground to support it in the storm.

If the limit of the object's resistance to one threat is exceeded, the process of destruction of the object due to damage, violation of its integrity, functionality, etc., begins. In practice, we perceive the threat to the object and the subsequent process of destruction of the object as a **security event involving the object**.

The hazardous state always lasts a certain time. Threats and the activation thereof can have a domino effect. Even if one threat stops, it could trigger another adverse event that further threatens or damages the object.

Endangerment by a threat is defined as the set of maximum impacts of the threat, which can be expected in a given place for a specified time interval with a probability equal to a specified value. According to norms and standards, this is determined by the magnitude of the threat that will occur with a probability or frequency distribution equal to 0.05 for a time interval of 100 years.

We can also understand a hazard to be an **emergency**. In the event of a hazard, no damage or injury will occur until the resistance limit of the object is exceeded. During an emergency, various active, usually known or planned procedures, are therefore implemented to delay the resistance limit being exceeded or to strengthen the resistance of the object so that there is no deformation or damage to the object and its functionalities (Buzan, Wæver, 2003). Unfortunately, such measures are not always effective.

4. Agent of threat

Within the context of security terminology, the term “agent” has synonyms like source, originator, initiator, actor, attacker, or cause.

An **agent of threat** is an entity, object, or process that initiates or triggers a threat. In professional literature, synonyms include **source, originator, initiator, actor of the threat, attacker, or cause of the threat**. A threat can be triggered by several agents at the same time. Examples of threats and their agents are presented in Table 1 below.

Table 1. Examples of threats and their agents.

Agent of threat	Threat
Undersea earthquake.	Tsunami wave.
Igniter.	Bomb, grenade explosion.
Low salaries.	Key employees leaving a company.
Dissatisfaction, frustration, burnout.	Loss of loyalty, betrayal, employee leaving to join a competitor.
Inattention, ignorance, irresponsibility in inspecting technical equipment.	Occurrence of a failure, subsequent aircraft crash, vehicle brake failure, etc.
The extreme-left or extreme-right coming to power.	Violation of democratic principles in a country, threat to constitutional security.
Human inattention.	Traffic accident.
Unsecured money deposits, low morale.	Theft of money.
COVID-19 pandemic.	Diseases, deaths, declining economic productivity, social unrest, political instability.

Source: Authors

In other literature, **agent of threat** is synonymous with **motivation**, as defined by an interest in initiating a threat to an asset (Smejkal, Rais 2013). However, this definition is only applicable to intentional threats. Flow diagram of the dependencies of basic security elements (concepts) within security management is presented below in Figure 2.

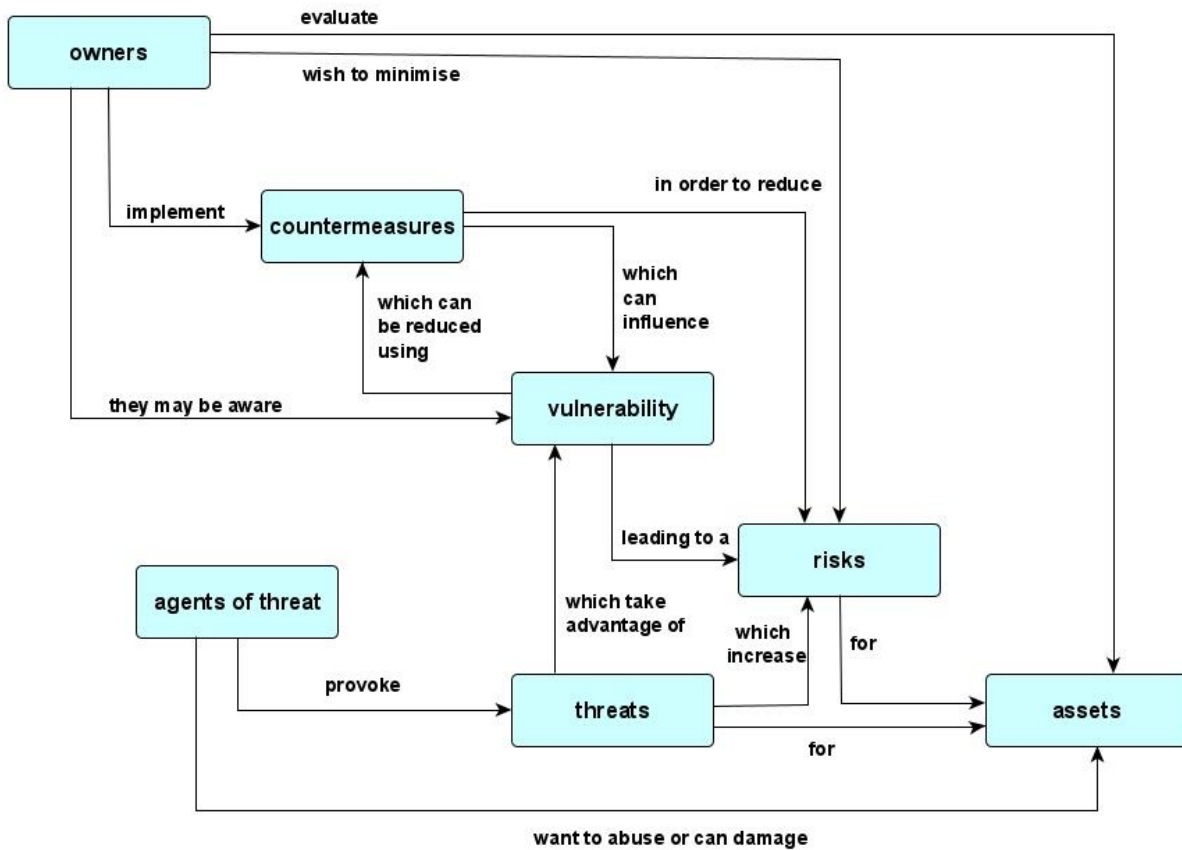


Figure 1. Flow diagram of the dependencies of basic security elements (concepts) within security management. Processed according to ČSN ISO/IEC 15408-1.

Source: Roman Rak

The behaviour of agents of threat can be predictable, completely unpredictable, random, and without any obvious context (Dirnbach et al., 2020).

Agents of threat can be natural processes and technological processes from which unintentional threats arise. However, an agent of threat can also be a person, different groups of people, associations of different organisational forms and institutions. Threats can then be triggered knowingly (intentional threats) or unknowingly (unintentional or unwanted threats).

In the case of intentional threats and events, the motivation is usually conditioned by the value of the object of interest (material goods, information) and the values or motivation of the “attacking” object - a person (revenge, the instinct for self-preservation, etc.).

In practice, for some threats, it is imperative that they are prevented from becoming reality. This can be done by “eliminating” the actor of the threat, which then cannot activate (initialise, trigger) the threat to the object(s), so the threat is not carried out (see Figure 3).

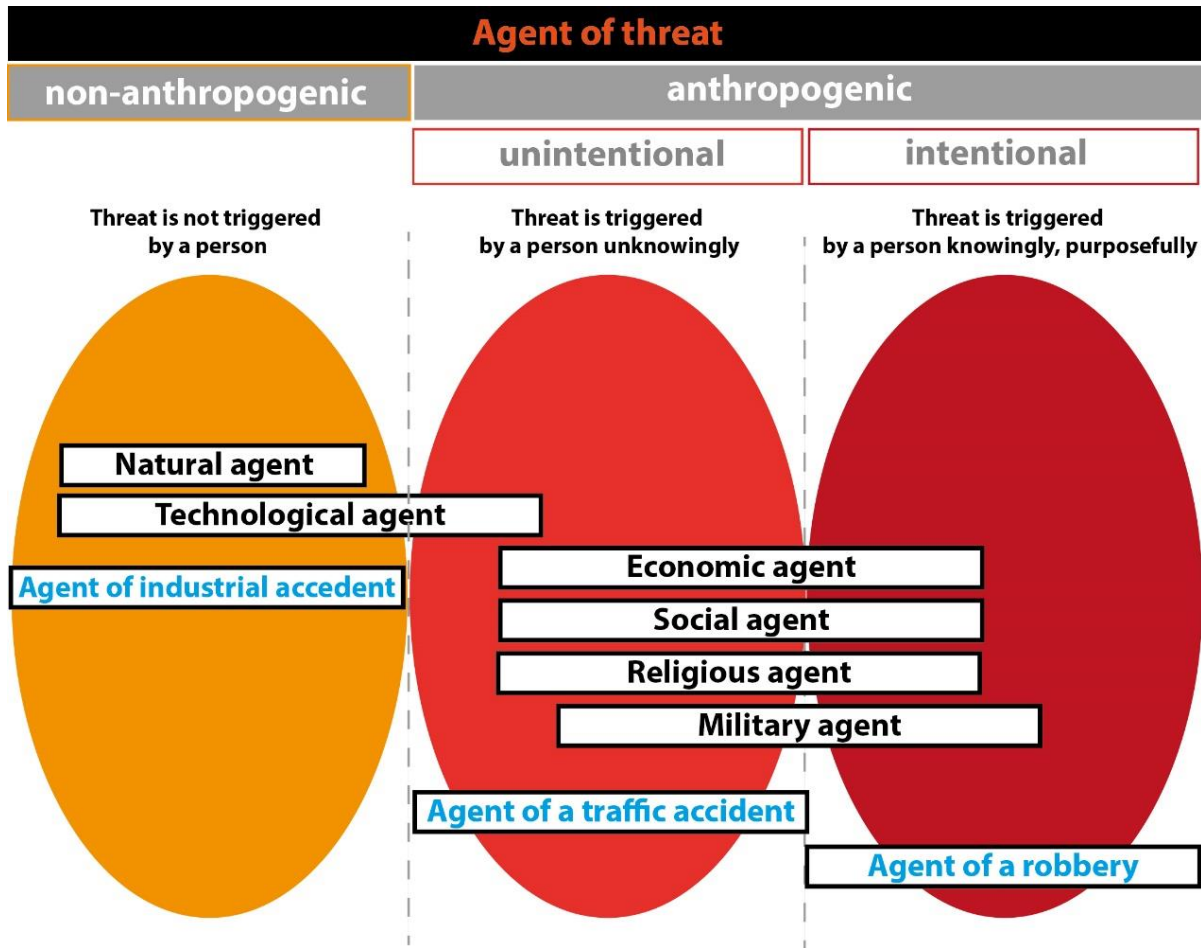


Figure 2. Agents of threat can be divided into non-anthropogenic (not triggered by a person) and anthropogenic (triggered by a person). These are further divided into unintentional (unknowingly triggered) and intentional (knowingly triggered). Agent of industrial accident - in this case, it could concern a situation in which a failure occurs due to material fatigue in hitherto unknown operating conditions. Humans created the technology but could not influence it in extreme conditions. Agent of traffic accident - driver inattention, fatigue (unintentional anthropogenic agent). Agent of robbery - desire for profit, planned robbery.

Source: Roman Rak

5. Basic and specific agents of threat

In practice, agents of threat can be divided into the following **basic types** (although, significantly more exist depending on the point of view and the depth or accuracy of their classification):

- **Natural agent** - the trigger of the threat is nature itself, natural phenomena, events, and processes. It is usually not possible to stop this type of agent, i.e. prevent the threat from being activated at all, so that it does not freeze, the wind does not blow, there is no earthquake or tsunami, measles and smallpox do not spread in developing countries, etc.
- **Economic agent** - this agent triggers threats based on economic characteristics and indicators (*high exchange rate of the domestic currency prevents economic development; non-payment of child support, risks distraint*) (Nálepová, 2020; Kliková, 2017).

- **Societal agent** - the threat is triggered by something that happens in society (Jakulikova et al., 2020) (*for example, “when those who rule can no longer rule in the current way and those who form the mass of the people no longer want such a government”*).
- **Religious agent** - the trigger of the threat can be ideological, religious beliefs, opinions, requirements, which in their essence promote other religious or power interests; they are in conflict with other ideas, religions, etc.
- **Military agent** - the trigger for the threat is the transition from solving problems or conflicts by political means to their solution by weapons and military force.
- **Technological agent** - the threat to the object is activated by a certain technology, created and (not) controlled by man. The moment of launch or activation of the threat can be accidental (fault, defect, etc.) or planned at a certain point in time (Kubjatko et al., 2018; Böhm et al., 2020). For example, a terrorist bomb is detonated by a mobile phone or a time trigger. The threat activating technology agent is therefore the mobile phone or timer. In this case, the technological agent is subordinated (controlled) by an anthropogenic, intentional agent.
- **Anthropogenic agent** - the initiation always involves human factor, i.e. a person or a group of people. The threat can be activated by an individual or a group of people of various sizes (institutions), either knowingly (*intentional threat*) or unknowingly (*unintentional threat*), etc. It is important to realise that the anthropogenic agent does not have to trigger or activate the final threat immediately, but gradually, with time delays and through other agents (anthropogenic and non-anthropogenic) (Stieranka, Busarova, 2017).

In general, activating various threats through agents can be done gradually.

Example:

Poor quality materials in a thermostat prevent the circulation pump from switching on. The temperature of the coolant rises. The warning light comes on, but the driver doesn't notice. Due to the lack of refrigerant, which begins to evaporate, the engine temperature rises and the engine stalls.

In this case, there are de facto two agents responsible for the threat of stalling: poor quality materials and an ignorant or inattentive driver, who should have noticed the temperature indicator light come on and prevented a further temperature increase by taking specific, known measures.

Similar dependencies of the actors of the threat and danger can be observed in intentional and unintentional anthropogenic agents. The human race is characterised by organisation, which can be hierarchical, flat, etc.

Different entities (individuals, organised groups of people in various forms of institutions) can then act in sequence (gradually over time) on other anthropogenic subjects, both intentionally (consciously, knowingly) and unintentionally (unconsciously, unknowingly) and ultimately activate a specific threat. The activation of the final threat can take place in several successive steps. The final threat can be, for example, terrorism, organised crime, the penetration thereof into political and executive structures (Kotlan, 2020), a political coup, social or economic instability, revolution, war, etc.

According to their interests, **anthropogenic agents** can be divided into the following **specific types**:

- **Minority or individual interest agents (executive agents)** - these agents are usually at the lower level of the human process management hierarchy. They carry out, knowingly or unknowingly, certain activities usually ordered by their superiors, or have and assert personal interests or the interests of small groups of people. In some cases, they may not be aware of the threats they cause, e.g. duress within the field of

forensics. From a global perspective, the impacts of these threats on society do not have to cause significant damage or injury to the state (even if these result in substantial financial costs or cause harm to the health and lives of many people). The options for these agents to hide their interests or activate threats vary; their own interests are limited from society's point of view because they have probably already appeared in some form in the past and therefore are more determinable and predictable in terms of risk analysis and agents than the following two types of agents.

- **Agents of political, national, and supranational interests (ideological agents)** - their official interests externally have a strong programmatic character, which is constantly declared to the public (during elections, political negotiations, disputes, etc.). In addition to official interests, there may also be purely intra-party, intra-group interests, which may be pursued in a hidden manner (e.g. the promotion of restitution on the one hand and personal enrichment resulting from it on the other). This type of agent already has great power, strength, and support from allies with regards to promoting programmes and activating various threats, including international ones (the emergence of nationalism in the interwar period in Germany, the uncontrolled and uncontrollable influx of immigrants, the abuse of the institutes responsible for light fuel oils and solar energy for own enrichment, etc.). Agents of this type often have executive power. They can assign tasks, command, transfer responsibility to subordinates, and hide evidence. They can also influence the decisions or investigations of security forces, becoming a dangerous threat to them (for certain independent, loyal entities). In addition to political interests, this category can include economic, political, supranational, and other interests. From the point of view of risk analysis, the activity (including the activation of specific threats) of this type of agent is complicated to predict because, within a large number of positive actions for the benefit of society, less frequent actions with a negative impact on society may be hidden. If the agents of threat are foreign entities (political parties, governments, powers, government executive bodies, etc.), they can initiate other professional entities, their own specialised institutions (intelligence agencies, security services, the army, etc.), to promote their interests. In some cases, the interests and the initiation of threats are professionally hidden (secret) at the very highest levels and it is not a trivial matter to identify them, whereas in other cases, they are quite evident (deterrent threats by force, open declaration of military technology, technological sophistication, etc.).
- **Agents of private, oligarchic, and global interests (hidden, ideological agents)** - this type of agent is usually under-represented in society, but is all the more influential for being so. These are usually very rich, privileged, often educated individuals and small groups of people who have acquired their current wealth and property by both legal and illegal means and are interested in further expanding their wealth, influence, or power. These agents then directly, but far more often in a secret manner, lobby or order various activities to be carried out to achieve their goals. The activities in their final form can also be violent and brutal (in less socially developed countries - murders, kidnappings, extortion, Nazism...). These agents include individuals, small groups of people, controlling international economic groups, multinational companies, but also organised crime, mafias, etc. They can also include the heads of churches, religious sects, and secret societies (e.g. Masonic lodges, "Brotherhoods"), which then exercise influence over politicians, the performance of state authorities, etc. This type of agent is very well aware of the need to keep its activities highly confidential and hidden from the public. It is therefore probably not possible to work with them in terms of risk analysis, their activating agents, and subsequent threats. On the whole, evidence of such activity is lacking.

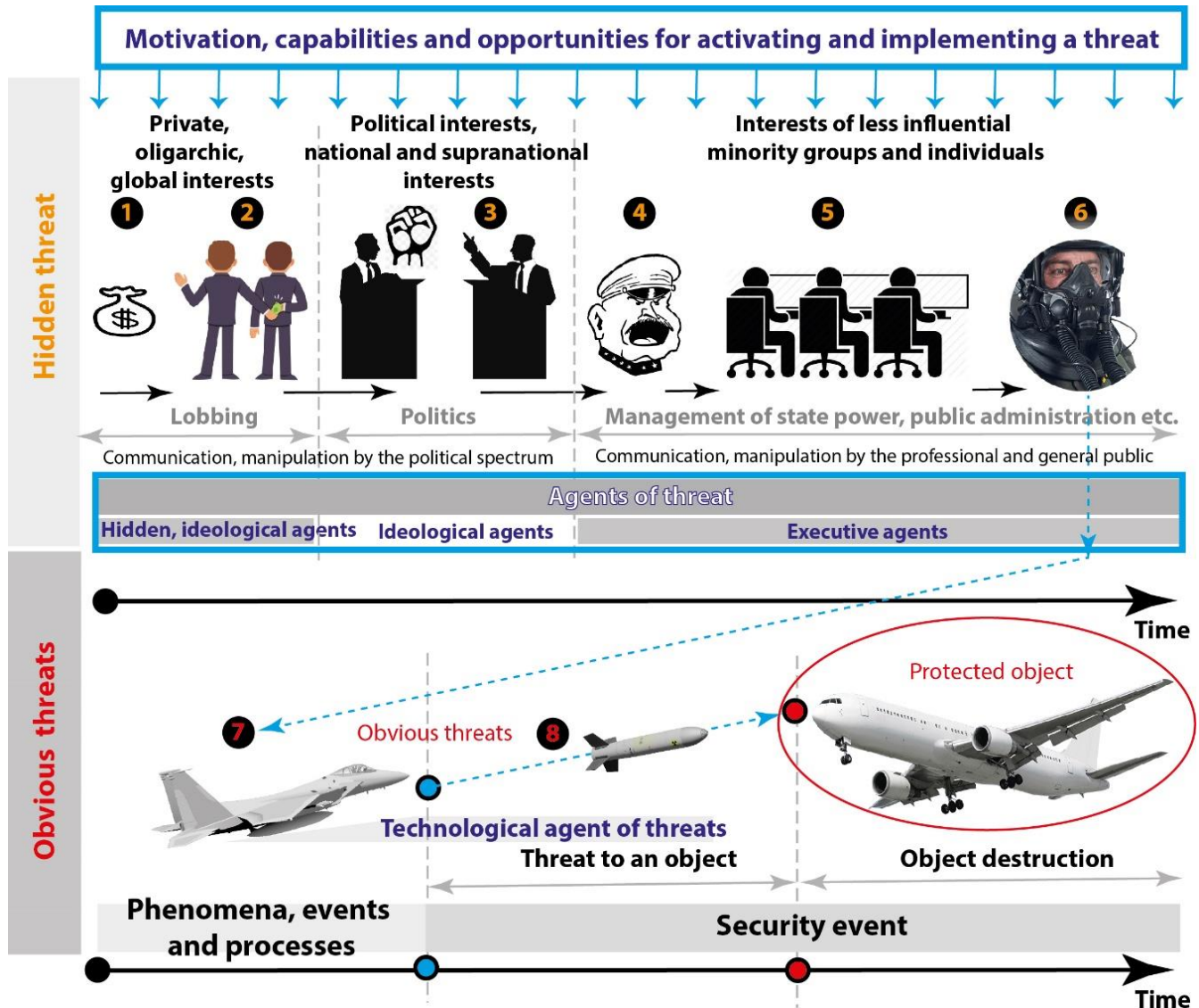


Figure 3. Explanation of the term agent of threat (originator, initiator)

Source: Roman Rak

The above division of anthropogenic agents into specific types helps to improve understanding of the dangers and threats that these agents potentially trigger. Many dangers and threats can be hidden during a security risk analysis. After all, we may not be aware of them because of a lack of knowledge of all the anthropogenic agents, let alone their interests, goals, and motivations. This is especially true when these anthropogenic agents professionally hide and even consciously conceal their interests (only a small group of people with strong influence, status, wealth, etc. know about their real interests, goals) and manipulate the lay and professional public with the help of substitute, insignificant interests, and the use of a variety of manipulative techniques to work with individuals, groups, and large swathes of the population. Hidden, classified threats or their anthropogenic agents can be detected, for example, by a group of professionals (intelligence agencies and security services, etc.) who are trained in such activities on a long-term and professional basis. In practice, a problem may arise and usually does when institutions (e.g. government, politicians) and individuals (representatives of government, politicians, etc.) who, based on information from security services and intelligence agencies, have to make executive decisions, but do not trust or do not want to trust security professionals, questioning them accordingly.

Categories of agents of threat can interact in all directions: the individualists (executive agents) may try to get into politics (ideological agents) and trigger various events (which can pose a threat to other entities) or, after obtaining significant resources, gradually work their way into oligarchic groups, where they then secretly influence politicians (hidden, ideological agent). Conversely, a politician (or even an individual from a lower category of agents of threat) can use (abuse) another person to activate a threat (e.g. the transfer of money obtained through organised crime as part of a laundering process).

For some agents (see Figure 2) it is not always easy to decide which category (intentional, unintentional) the anthropogenic agent of threat belongs to. This depends on the point of view or the specific threat. This division is profound if a large number of people in a historically and geographically large area participate in certain processes and the resulting threats. This applies in particular to, for example, economic, social, religious agents, etc.

Example:

How do we identify the agents of a religious threat such as the Hussite Revolution? On the one hand, the agent or cause can be considered to be the general religious conflict between the Czech- and German-speaking populations. On the other hand, the agent can be considered to be Jan Hus, who managed to show the contradictions in such a way that he won masses of Czech believers over to his ideas. Were it not for Jan Hus, another person would probably have appeared on the scene. In terms of risk analysis and the search for causes, triggers - agents of threat, the intentional and unintentional components of the anthropogenic threat must be identified. The unintentional component, in this case, is the objective religious conflict that was not caused by the general population; the intentional component is the teachings of Jan Hus, which consciously aimed to change and remedy the situation. In making an analysis, it is important to always be aware of dependencies, the primary nature of threats and their agents, and to subsequently decide which agent of threat or threat to eliminate first, insofar as this is possible and intentional (the church could not accept the objective truth of Jan Hus and therefore burned him at stake).

It is important in life (practice) to be able to correctly distinguish the nature of agents of threat, the threats themselves, and their impacts (caused damage and injury) on the security of the (protected) object of interest. If we want to eliminate a threat, it is often necessary to “eliminate” the launch or activation of the threat, thereby eliminating the agent of threat. From the point of view of investigations and court proceedings in relation to negative events that have already occurred, it is also important during the process of clarification and investigation to prove the intentionality of the launch of the threat, i.e. the conscious or unconscious involvement of the person in the crime.

In our opinion, this strongly depends on what threats exist, which agents these involve, and how they are perceived, evaluated, and managed in real time. In practice, we may respond to partial, acute threats and, at the same time, far greater threats we cannot identify that may have more far-reaching consequences. An example of a possible basic view is given in the following Table 2.

Table 2. Examples of threats, agent of threat, and elimination of threats.

Threat	Agent of threat	Elimination of threat
Missile fired from an aircraft.	Fighter jet and its pilot.	Shoot down the missile. Guide the missile to a decoy target. Maneuver the passenger aircraft to avoid the missile.
Aircraft with attack capabilities.	Military order, air traffic control centre, communication between air traffic control and the pilot.	Force the aircraft to leave the airspace, disrupt communication with the aircraft, radio-electronic warfare, shoot down the fighter jet.
A political situation that can result in a military conflict.	Government decisions, orders from army command, lack of discipline, initiative of subordinates.	Political negotiations, international peace activities, international treaties, pacts, strengthening one's own army, security forces.
Penetration of organised crime, oligarchies into the public administration, executive bodies of a democratic system.	Secret, non-public, private, oligarchic, global interests of groups of influential, criminal and lobby groups; their motivation to gain power, control over processes, benefits, resources, raw materials, etc.	Transparency of the political, governmental and social systems, the fight against organised crime, the independence of the security forces, the judiciary, independent controls and audits.

Source: Authors

Example:

- a) For a passenger aircraft, the threat is a missile aimed and fired at it from a military aircraft. The agent of threat is a fighter jet and its pilot. The pilot of the passenger aircraft has few options to deal with the threat, which must be solved immediately.
- b) Another threat is the same military aircraft in the airspace of another state. This military aircraft can shoot down more passenger aircraft and attack other objects. The agent of threat is the pilot's superior commander, the air traffic control centre.
- c) Military orders, air traffic control centres, and other combat control centres are agents for military threats to the invaded country and can activate other threats.
- d) A military solution for a specific situation, military threats activated by political situations, the decisions of politicians (governments, etc.). These are agents of military threats.
- e) A country's politics may also be dominated by hidden oligarchic groups that have secret, private, global interests. These groups are agents of threat to politicians. Oligarchs are interested in a country's mineral wealth and may provoke the downing of the passenger aircraft in order to instigate a political crisis and to be able to seize raw material reserves for their multinational companies through subsequent planned activities.

In practice, the primary motive for the shooting down of a civilian aircraft may be seen (by the public and investigators) as a terrorist act. However, in reality, the attack can be put down to a group of supranational oligarchs trying to obtain minerals in a particular country for their manufacturing plants, whereby the shooting down of the civilian aircraft is purely considered a means to an end.

The human factor is very complex. Its effect does not always have to be direct, but it can have a subsidiary character, i.e. the character of subordinate articles (Velas et al., 2019). To properly manage security and understand the variety of threats that exist, it is necessary to think systematically, to clarify the links between anthropogenic agents that can trigger different types of threats on objects of interest. The basis of this principle is that it can be applied in general.

Threat impact

The **threat impact** is the negative result of a realised threat on a protected asset (object, process, interest) that causes damage or injury. In professional literature, the word “consequences” is also synonymous with “impact”.

The **threat impact** is the adverse effect of an undesirable event at a given place and time on a protected asset or against an interest (Božek, 2015).

The purpose of risk management is to minimise the impact (consequences) of threats (undesirable situations) to zero or at least an acceptable value. If the impacts can be quantified in units (e.g. money), we speak of damages. If the impact is not quantifiable, we speak of injuries (e.g. harm to health, reputation, brand damage, etc.).

In the first case, this concerns a **quantitative impact assessment** (damage assessment), in the second case, this concerns a **qualitative impact assessment** based on, among other things, verbal expressions or a description of the characteristics of the injury caused.

6. Discussion

Threats precede adverse events. Threats are phenomena that can occur and can have adverse effects, thereby causing damage and injury. Adverse events can escalate into crises and disasters. If such events are to be prevented, it is necessary to be able to correctly identify threats, including the impacts and risks thereof, in a timely and appropriate manner, so that appropriate measures can be put in place. Unfortunately, these may not be adequate.

Many anthropogenic disasters arise for the convenience of going mainstream. There is often a lack of perspective on different sides, which is fueled by the absence of discussion, the search for the truth and the real causes of problematic situations. To accomplish this, the scientific and professional discussions must be apolitical to objectively recognise the world as it is, regardless of the desire for it to be as we want it to be at all costs.

The end of the 20th and the beginning of the 21st centuries created a whole new digital world thanks to the invention of the Internet. However, its virtuality is often outside the real world and, combined with the existence of a physical, global world, brings entirely new threats that can fundamentally change our world and lead to devastating global conflicts.

Today, however, politics is not created a priori by politicians, but by the mass media or those who control them (own or paid). As a result, politics lacks real personalities that are able to see the world in a broader context with a view to the more distant future. Mass media spread a huge amount of misinformation, which in turn, adversely and unilaterally affects weak secondary politicians who do not solve problems and who, with their narrowly focused orientation or lack of insight, deepen or create new problems.

Globalized conflicts are often accompanied by information and economic wars. An economic or financial war is waged through the implementation of various restrictions. Unfortunately, these restrictions can prove very problematic because they tend to be created and decided politically at a time when emotions are running high. The impact of such restrictive measures is also often exacerbated by the fact that they are not consulted with experts. Their hasty adoption then poses considerable threats, which over time can turn against the instigators of the restrictions themselves.

7. Conclusion

To manage the security of objects, states, and processes, it is necessary to be able to identify potential and real threats correctly, whilst taking into account the vulnerabilities of the entities that need to be protected. To do this, it must be possible to realistically estimate all potential phenomena that may escalate into events with adverse effects. Phenomena with adverse effects on protected entities are threats. Being able to categorise threats correctly is an essential precondition for determining how to face them in practice and prevent their further development.

Threats have their initiators, triggers. Unfortunately, in a profit-oriented economy, private interests and the interests of oligarchs and elites, which may be behind political, national, or international interests, are frequently motivational factors. In practice, this motivation for triggering threats can turn into real threats to national interests, the economy, etc.

References:

- Adams, N., Chisnall, R., Pickering, C., Schauer, S., Peris, R.C., Papagiannopoulos, I. (2021). Guidance for ports: security and safety against physical, cyber and hybrid threats. *Journal of Transportation Security*, 14 (3-4), 197-225. <https://doi.org/10.1007/s12198-021-00234-6>
- Ajdari, B., Asgharpour, S., E. (2011). Human security and development, emphasizing on sustainable development. *Procedia Social and Behavioral Sciences*, 19, 41-46. <https://doi.org/10.1016/j.sbspro.2011.05.105>
- Alanen, J., Linnosmaa, J., Malm, T., Papakonstantinou, N., Ahonen, T., Heikkilä, E., Tiusanen, R. (2022). Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. *Reliability Engineering and System Safety*, 220, art. no. 108270 <https://doi.org/10.1016/j.ress.2021.108270>
- Alkopher, T.D., Blanc, E. (2017). Schengen area shaken: the impact of immigration-related threat perceptions on the European security community. *Journal of International Relations and Development*, 20(3), 511-542. <http://doi.org/10.1057/s41268-016-0005-9>
- Alkopher, T.D. (2018). Socio-psychological reactions in the EU to immigration: from regaining ontological security to desecuritisation. *European Security*, 27(3), 314-335. <http://doi.org/10.1080/09662839.2018.1497981>
- Ansari, M.T.J., Pandey, D., Alenezi, M. (2022). STORE: Security Threat Oriented Requirements Engineering Methodology, *Journal of King Saud University - Computer and Information Sciences*, 34 (2), 191-203. <https://doi.org/10.1016/j.jksuci.2018.12.005>
- Androniceanu, A.-M., Căplescu, R.D., Tvaronavičienė, M., Dobrin, C. (2021). The Interdependencies between Economic Growth, Energy Consumption and Pollution in Europe. *Energies*, 14, 2577. <https://doi.org/10.3390/en14092577>
- Atkinson, C., Chiozza, G., (2021). Hybrid Threats and the Erosion of Democracy from Within: US Surveillance and European Security, *Chinese Political Science Review*, 6(1), 119-142. <https://doi.org/10.1007/s41111-020-00161-2>
- Besenyő, J. (2016). Security preconditions: Understanding migratory routes. *Journal of Security and Sustainability Issues*, 6(15–26), [http://dx.doi.org/10.9770/jssi.2016.6.1\(1\)](http://dx.doi.org/10.9770/jssi.2016.6.1(1))
- Besenyő, J., Kármán, M. (2020). Effects of COVID-19 pandemy on African health, political and economic strategy. *Insights into Regional Development*, 2(3), 630-644. [https://doi.org/10.9770/IRD.2020.2.3\(2\)](https://doi.org/10.9770/IRD.2020.2.3(2))
- Borodin, A., Tvaronavičienė, M., Vygodchikova, I., Kulikov, A. Skuratova, M., Shchegolevatykh, N. (2021). Improving the Development Technology of an Oil and Gas Company Using the Minimax Optimality Criterion" *Energies* 14(11), 3177. <https://doi.org/10.3390/en14113177>
- Božek, F. (2015). *Řízení rizik. (Risk management) Univerzita obrany, Fakulta vojenského leadershipu, Brno*, 127 pp.
- Böhm, K., Kubjatko, T., Paula, D., Schweiger, H.-G. (2020). New developments on EDR (Event Data Recorder) for automated vehicles. *Open Engineering*, 10(1), 140–146 ISSN 23915439 <https://doi.org/10.1515/eng-2020-0007>

Botrugno, M., Malagnino, A., Lazoi, M., Mangia, M., (2022). Building Information Modelling Supporting Safety and Security Threats Management: A Literature Review. *IFIP Advances in Information and Communication Technology*, 640 IFIP, 171-184. https://doi.org/10.1007/978-3-030-94399-8_13

Buzan, B., Wæver, O. (2003). Regions and Powers– The Structure of International Security. *Cambridge Studies in International Relations* Volume 9. Cambridge: Cambridge University Press <https://doi.org/10.1017/CBO9780511491252>

Buzalka, J., Blažek, V. (2011). Metodologie a metodika vypracování analýzy vnitřního ohrožení bezpečnosti SR, a z něj vyplývajících ohrožení a rizik (Methodology and methods of elaboration of the analysis of the internal security threat of the Slovak Republic, and the resulting threats and risks), *Zborník metodológia a metodika analýzy zdrojov ohrozenia vnútornej bezpečnosti SR*, Katedra krízového manažementu vo verejnej správe, Akadémia Policajného zboru v Bratislave, str. 16-39, Slovensko, ISBN 978-80-8054-517-8

Chehabeddine, M., & Tvaronavičienė, M. (2020). Securing regional development. *Insights into Regional Development*, 2(1), 430-442. [http://doi.org/10.9770/IRD.2020.2.1\(3\)](http://doi.org/10.9770/IRD.2020.2.1(3))

Dimbach, I., Kubjatko, T., Kolla, E., Ondruš, J., Šarić, Z. (2020). Methodology designed to evaluate accidents at intersection crossings with respect to forensic purposes and transport sustainability. *Sustainability (Switzerland)*, 12(5), 1972 ISSN: 20711050, <http://doi.org/10.3390/su12051972>

El Kafhali, S., El Mir, I., Hanini, M. (2022). Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing. *Archives of Computational Methods in Engineering*, 29(1), 223-246. <http://doi.org/10.1007/s11831-021-09573-y>

Hammoudeh, M., Watters, P., Epiphaniou, G., Kayes, A.S.M., Pinto, P. (2021). Special issue “security threats and countermeasures in cyber-physical systems. *Journal of Sensor and Actuator Networks*, 10(3), art. no. 54. <http://doi.org/10.3390/jsan10030054>

Hudecova, V. (2021a), Road Safety from the Perspective of European Union. In Kavan, Š. (eds.) International Conference Safe and Secure Society 2021. Conference proceeding. Ceske Budějovice: College of European and Regional Studies, Czech Republic, 2021. pp. 15 – 23. http://doi.org/10.36682/SSS_2021 ISBN je 978-80-7556-097-1, ISSN 2533-6223.

Hudecova V. (2021b). National Firearms and ammunition information systems. In: Koshovyi, B. Development and Security of the State, Citizens and Business Entities in the Modern World: Challenges and Perspectives, pp. 78-93, Oktan Print, Prague, Czech Republic <https://doi.org/10.46489/DaS.5>

Hudecova, V., Christel, P. (2021). The Directive Facilitating Cross-Border Exchange of Information. *The Archives of Automotive Engineering – Archiwum Motoryzacji*, 92(2), 17-31. <https://doi.org/10.14669/AM.VOL92.ART2>

Jackulikova, M, Vrankova, J, Bartkovjak, M, Mikolasova, G, Kozon, V, Olah, M, Mikloskova, M. (2020). Quality of Lives & Origin of Unaccompanied Minors & Migration to Europe, *So Clinical work and health intervention*, 11(1), 28-31, Austria, ISSN 2222-386X, eISSN 2076-9741 http://doi.org/10.22359/cswhi_11_1_04

Jůzl, M., Vlach, F. (2022). Modern Approaches in Czech Prison Staff Education and Training Against a Background of Comenius’ Thoughts. In: Tušer I., Hošková-Mayerová Š. (eds) Trends and Future Directions in Security and Emergency Management. *Lecture Notes in Networks and Systems*, vol 257. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-88907-4_24

Kharraishvili, N., Blake, J.W., Gorsline, D.H., Brooks, L.R. (2021). Global Health Security Capacity and Capability Measurement Framework within the Biological Threat Reduction Program. *Health Security*, 19(2), 163-172. <http://doi.org/10.1089/hs.2020.0023>

Kharlamova, G., Stavitskiy, A., Fedorenko, I. (2021). Solving Economic Security Issues in the Coordinate System of Modern Risks and Threats. *Studies in Business and Economics*, 16(3), 87-108. <http://doi.org/10.2478/sbe-2021-0047>

Klikova, Ch., Kotlan, I., Machova, Z. (2017). The role of social policy within economic policy: theoretical categorization, *Proceedings of the International scientific conference economic and social policy: Economic policy in global environment*, Ostravice, Czech Republic, pp. 143-151, ISBN 978-80-87291-20-7

Kotlan, P. (2020). Relationship of Criminal Proceedings to Civil Litigation, Insolvency and Tax Proceedings, *DANUBE: Law, Economics and Social Issues Review*, 11(2), 141-155, eISSN 1804 – 828 <https://doi.org/10.2478/danb-2020-0008>

Kriviņš, A., Teivāns-Treinovskis, J., Tumulavičius, V. 2021. Issues of state and national security: Religiously inspired terrorism in the Baltic States: internal and external factors. *Insights Into Regional Development*, 3(1), 65-79. [http://doi.org/10.9770/IRD.2021.3.1\(4\)](http://doi.org/10.9770/IRD.2021.3.1(4))

Kubjatko, T., Görtz, M., Macurova, L., Ballay, M. (2018). Synergy of forensic and security engineering in relation to the model of deformation energies on vehicles after traffic accidents (Conference Paper) *Transport Means - Proceedings of the International Conference Volume 2018-October, 2018*, pp, 1342-1348, *22nd International Scientific on Conference Transport Means 2018*; Trsalis - Trakai Resort and SPAGedimino str. 26, Trakai; Lithuania; 3 October 2018 through 5 October 2018; Code 140271. ISSN 1822296X

Manulis, M., Bridges, C.P., Harrison, R., Sekar V., Davis, A. (2021). Cyber security in New Space: Analysis of threats, key enabling technologies and challenges. *International Journal of Information Security*, 20(3), 287- 311. <http://doi.org/10.1007/s10207-020-00503-w>

- Matuszak, Z., Jaskiewicz, M., Ludwinek, K. et al. (2015). Special characteristics of reliability for serial mechatronic systems. *Selected problems of electrical engineering and electronics (WZEE)*. <http://doi.org/10.1109/WZEE.2015.7394039>
- Matuszak, Z., Jaskiewicz, M., Wieckowski, D. et al. (2017). Remarks to the Reliability Assessment and to Human Actions. Especially Car Driver. *18th International Scientific Conference on LOGI Location: Book Series: MATEC Web of Conferences*. 2017; 134, Article Number: 00036. [10.1051/mateconf/201713400036](http://doi.org/10.1051/mateconf/201713400036)
- Nálepová, V. (2020). The position Of the Czech Republic in European Corporate Taxation, In: Nálepová, V., Uhrova, N. (eds.) *Proceedings of the International Scientific Conference Economic and Social Policy*. Ostrava, University Prigo, pp. 293-301, ISSN 2571-1776, ISBN 978-80-87291-27-6
- Ni, S., Zou, S., Chen, J. (2022). Evolutionary Game Model of Internal Threats to Nuclear Security in Spent Fuel Reprocessing Plants Based on RDEU Theory, *Sustainability (Switzerland)*, 14(4), art. no. 2163 <http://doi.org/10.3390/su14042163>
- Periokaite, P., Dobrovolskiene, N. (2021). The impact of COVID-19 on the financial performance: a case study of the Lithuanian transport sector. *Insights into Regional Development*, 3(4), 34-50. [http://doi.org/10.9770/IRD.2021.3.4\(3\)](http://doi.org/10.9770/IRD.2021.3.4(3))
- Rak, R., Kopencova D. and M. Felcan, (2021). Digital vehicle identity – Digital VIN in forensic and technical practice, *Forensic Science International: Digital Investigation*, Elsevier, 39, 301307, ISSN 2666-2817 <https://doi.org/10.1016/j.fsidi.2021.301307>
- Rak, R., Felcan, M., Kopencova, D. (2021). Digital identification of vehicles not only for investigative and forensic purpose, *2021 5th International Conference on Vision, Image and Signal Processing (ICVISP)*, 2021, pp. 18-26. <https://doi.org/10.1109/ICVISP54630.2021.00013>
- Smejkal, V., Rais, K. (2013). *Řízení rizik ve firmách a jiných organizacích*, 4. aktualizované a rozšířené vydání, Praha, Grada, 466 p. ISBN 978-80-247-4644-9
- Šimák, L. (2015). *Krizový manažment vo verejnej správe*, Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, 259 p. ISBN 978-80-554-1165-1
- Sopilko, I., Svintsytskiy, A., Krasovska, Y., Padalka, A., Lyseiuk, A. (2022). Information wars as a threat to the information security of Ukraine, *Conflict Resolution Quarterly*, 39(3), 33-347. <https://doi.org/10.1002/crq.21331>
- Stefan, G., Coca, O., Creanga, D.E., Mursa, G.C., Mihai, C. (2020). The Impact of the Crisis Generated by Covid-19 on the Population Concerns. A Comparative Study at the Level of the European Union. *Transformations in Business & Economics*, Vol. 19, No 2B (50B), pp.703-719.
- Stieranka, J., Busarova, O. (2017). Characteristics of Evidencing and Investigating Money-Laundering in Slovak, Republic, *Pravo-Zhurnal vysshei shkoly ekonomiky*, Moscow, Russia, ISSN 2072-8166, 144-165, <https://doi.org/10.17323/2072-8166.2017.1.144.165>
- Tušer, I., Jánský, J., & Petráš, A. (2021). Assessment of military preparedness for naturogenic threat: the COVID-19 pandemic in the Czech Republic. *Heliyon*, 7(4), e06817. <https://doi.org/10.1016/j.heliyon.2021.e06817>
- Tušer, I., Hoskova-Mayerova, S. (2020a). Emergency Management in Resolving an Emergency Situation. *Journal of Risk and Financial Management*. 13(11), 262. <https://doi.org/10.3390/jrfm13110262>
- Tušer, I., Hošková-Mayerová, S. (2020b). Traffic safety sustainability and population protection in road tunnels. *Qual Quant* <https://doi.org/10.1007/s11135-020-01003-8>
- Vel'as, A, Lenko, F, Lenkova, R, Felcan, M. (2019). Creation and teaching life and health protection courses for high schools, 12th International (ICERI2019), ICERI Proceedings, *12th Annual International Conference of Education, Research and Innovation (ICERI)*, Seville, Spain, ISSN 2340-1095

Acknowledgements

Our special thanks go to AMBIS University, especially its Department of Science and Research and the university's management, without whose financial support it would not be possible to publish the research results. Additional thanks go to those providing general support to other research in the field of Security and Law.

Author Contributions: conceptualisation: Kopencova, Rak; methodology: Sulc, Naplavova; data analysis: Kopencova, Vlach, Naplavova; writing - original draft preparation: Rak, Sulc; Writing - Kopencova, Vlach; review and editing: Vlach; Visualisation: Rak

Dagmar KOPENCOVA, JUDr., Ph.D. teaches forensic science and criminal law. She conducts practical exercises at Ambis University. For many years she worked in the elite units of the Police of the Czech Republic. She has successfully dealt with drug-related crime and organized crime. She deals with breeding and training of rescue dogs. ORCID ID: <https://orcid.org/0000-0003-4934-160X>

Vladimir SULC, Dipl. Eng., Ph.D. he works not only as a security consultant, but above all as an academic personnel at the Department of Security and Law of the AMBIS University. Brno, Czech Republic. He deals professionally with issues of management, information and cyber security. He has been publishing in this area for a long time, participating in and lecturing at international conferences and cooperating with other experts in the field of various research projects. ORCID ID: <https://orcid.org/0000-0003-2061-888X>

Roman RAK, Prof. Dipl. Eng., Ph.D. is a professor at the Department of Security and Law of the AMBIS University. Prague, Czech Republic. He deals professionally with the issues of technical aspects of forensic sciences. His professional activity is focused on the forensic identification of objects (persons, vehicles), vehicle crime, concepts and implementation of critical infrastructure information systems. Author of several dozen professional books, over 300 articles. ORCID ID: <https://orcid.org/0000-0002-9792-1572>

Magdalena NAPLAVOVA, Dipl. Eng., Ph.D. is a graduate of the Faculty of Military Leadership at the University of Defence in Brno, where she received her PhD from the Department of Crisis Management in the field of Protection of Troops and Population in 2017. As part of her doctoral studies, she dealt with the issue of risk management and health risk assessment. She currently works at the Department of Security and Law as a member of the academic staff and secretary of the department, where she is the guarantor of the subject Protection of the Population and also participates in teaching subjects related to risk management. She regularly publishes her results in domestic and foreign journals and at relevant conferences. <https://orcid.org/0000-0002-3590-2245>

Frantisek VLACH, Ph.D. MBA, LL.M., colonel is the Director of the Academy of the Prison Service of the Czech Republic. Research interests: prison staff training and education, employees, professional development, prison service. He also deals professionally with process optimization and human resource management. He cooperates externally with the Ambis University. Dr. Vlach is the author of a professional book and dozens of professional articles. ORCID ID: <https://orcid.org/0000-0002-7598-8370>

Make your research more visible, join the Twitter account of ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES: @Entrepr69728810

Copyright © 2022 by author(s) and VsI Entrepreneurship and Sustainability Center
This work is licensed under the Creative Commons Attribution International License (CC BY).
<http://creativecommons.org/licenses/by/4.0/>

