Human Factor Failure in Hybrid Warfare and its Impact on Airport Security

Zbyšek KORECKI[1], Blanka ADÁMKOVÁ[2]

[1]*University of Defence in Brno, Department of Air Forces, Kounicova 156/65, 662 10 Brno, Czech Republic*
[2]*Ministry of Defence, Tychonova 221/1, 160 00 Praha 6, Czech Republic*

E-mails:[1]zbysek.korecki@unob.cz, [2]blanka.adamkova@email.cz

Abstract

The human factor is a source of errors that arises not only in airports activities but also in the process of internal and external communication. The hybrid campaign consists of a spectrum of classic tools, called DIMEFIL, which affect the dimensions of power in seven areas (diplomacy / politics, information, armed forces, economics, finance, intelligence, public order and the rule of law) [1].

Hybrid threats are a complex and multidimensional threat caused by the convergence and interconnection of various elements of social life [2]. The hybrid threat aim is to weaken mutual ties and conduct different types of espionage. Espionage can be part of the attack preparation, mostly in a latent form, or to get information security technological progress. Determining the level of cyber security requires investigating phenomena and activities that could pose real or potential threats to the internal and external communications of critical infrastructure [3, 4].

Security of critical infrastructure is important not only in aviation but also in other industries such as metallurgy. This is mainly due to environmental protection and the possibility of an ecological disaster [5]. Modern society is not only connected by computer networks, but we are increasingly dependent on technical infrastructure.

The interconnectedness of the infrastructure systems creates a dependency where the failure of one infrastructure subject affects the functionality of other infrastructure elements [6]. Mutual multilevel infrastructure systems inter-connection is a modern society development basic prerequisite. Assessing the level of infrastructure vulnerability is directed in two ways, technical and human failure.

The authors analyzed aerospace technical infrastructure inter-connectivity and an internal communication vulnerability. The authors analyzed the elements of an inter-connectivity level protection of aerospace technical infrastructure and internal communication vulnerability.

The authors concluded that by reducing the disconnection point's number and splitting internal ways, they are a possible solution to cut the penetration possibility into the internal network of air transport entities.

The results of the research show that interdependent systems should have internal systems divided into open systems for outdoor and indoor access, with no external access. Protection against intrusion is the first phase and requires the firewalls and antivirus programs implementation in the critical infrastructure network.

The monitoring systems implementation is the most suitable solution to protect against data leaks, which is the most risky area, by employees and visitors. An aircraft monitoring system gains, monitors, process, and records aircraft system condition (characteristics) and failures [7].

The authors believe that the ongoing use of penetration tests [8] based on a simulated hacker attack is a proper method of verifying the level of cyber security.

KEY WORDS: *critical infrastructure protection, cyber security, human error, human Reliability Analysis, TESEO*

1. Introduction

A hybrid campaign defined as: „broad, complex, adaptive and often highly integrated combination of conventional and unconventional means, overt and covert activities, by military, paramilitary, irregular and civilian actors targeted to make (geo) political and strategic goals [9], [10], [11].

[1] Corresponding author.
E-mail address: zbysek.korecki@unob.cz.

Table 1.

Hybrid campaign areas

Designation	Area	Sphere of influence
D	diplomacy / politics	exerting influence and exerting pressure through the mouth and actions of the official political representation
I	information	media, social network and other means of disseminating information, its manipulative use, disinformation campaign and propaganda
M	Military forces	open use as a threat (demonstration of military presence and readiness) or directly combat use or for various forms of covert deployment of people, small groups and infiltration of the attacked state using them
E	economy	different forms of economic pressure (imposing customs duties, embargoes, refusing to supply raw materials or energy, banning the use of transport routes, destabilizing key sectors, businesses, etc.)
F	finance	currency destabilization, stock and bond market, banking sector, influencing key financial institutions;
I	coverage	intelligence activities, espionage, recruiting associates (especially state or political officials) to engage in anti-state activities;
L	public order and the rule of law	exploiting various disruptive activities attacking the value, legal and other aspects of social ordering, such as inciting riots in the attacked country using ethnic, religious or social divisions in society or using a range of terrorist attacks and other typically criminal methods.

Air traffic security is interrelated by a human factor and engineering system. *Although pilots are responsible in many human factor failures, experience has shown that maintenance factors account for 18% of accidents.*

"*The **SHELL model** is a conceptual **model** of human factors that clarifies the scope of aviation human factors and assists in understanding the human factor relationships between aviation system resources/environment (the flying subsystem) and the human component in the aviation system (the human subsystem)*" [12].

2. Method of Investigation

The concept of Human Reliability Analysis (HRA) expressed the fact that people and systems are not fault tolerant and that increased reliability requires an understanding of error problems, leading to the innovative strategies implementation and overall mitigation of human error [13].

The goal of HRA is to quantify the probability of human error for a given task. The HRA can help find vulnerabilities within a defined task and provide information on how to increase reliability in performing that task. Evaluation of human reliability involves the use of qualitative and quantitative methods to assess the degree of human responsibility to risk [14]. In general, HRAs calculate the error chance for a particular task type, taking into account the impact of performance factors [15].

Quantitative techniques use a database of human-performed tasks and work with error rates to calculate the average chance of error for a particular task. The aim of the method is to make an estimate of the failure chance when using data in the long-term [16].

Hierarchical task analysis performed for critical activities, (i.e. activities with the potential to cause a dangerous event) and begins by identifying each task and steps within the activity.

A typical quantitative approach first identifies the nominal error rate for a task type [13]. The types of tasks vary between tools and are very specific or general. Further, the performance factors calculate for the task. Performance factors can increase or decrease errors chance for a given task.

The human factor interaction and technical means in the security process at the airport then uses the graphical presentation of relationships by the SHELL model [17]. The authors use five quantitative factors in possible the human error assumption (HE) in *Tecnica empirica stima errori operatori method*.

Factors take advantage of lean logistics knowledge and represent the human factor intersection with work environment requirements where: K1 - The action taken type, K2 - Planned working time, K3 - Preparatory phase (time), K 4 - The worker emotional state and K5 - Ergonomic environment.

The authors analyzed the necessary internal communication for selected areas of air traffic security. The use of coefficients, especially planned working time, can be used by the TESEO method to decide the worker reliability for a selected task type, which he / she performs in a defined time interval by default.

The HE probability in the TESEO method using the formula: P = K1 K2 K3 K4 K5, where there are time-related coefficients. The Human Error Assessment and Reduction Technique method (HEART) takes into account the tasks of the operator and the environment (ergonomic and environmental factors). The method also works with conditions that have a negative impact on human actions. In this way, the safety management process may include a worker's level of experience.

3. Human Factor Evaluation in Aircraft Repairs

The human factor, in aeronautical maintenance and pre-flight preparation, is a significant factor, which can produce error, or alternatively reliability. Two aspects of human labour, speed, and well-being cannot be separated. If a person is part of the system, it is necessary to create conditions to reduce the level of latent failure.

Human well-being is associated with health and the working environment, where the proper condition creation is the employer's task. Reducing the level of human error is based on measures to reduce errors or its equal, so we are talking about reliability improvement. The most accepted model for reducing error levels is reliability analysis [18], but the errors produced by humans are more accepted by the cognitive model that was originally developed for pilot training, industrial process control, and air traffic control [19].

Active failure can be classified as latent errors that differ from the originator, experience, and education. By taking measures to cut latency errors and create barriers, we cut failures and further propagation of errors in the system. The aim of aviation measures is to prevent the spread of a systemic error when the solution is to create non-porous barriers, such as by changing packaging.

Two methods can be used to detect resident behavioral personnel.

1. Incident - based: The incident has already occurred, and a detailed analysis of resident pathogens and active failure is underway.

2. Task-analysis- based: Manager actively looking for possible human errors in meeting the requirements. An effort is heading to cut resident pathogens.

Operators have divided maintenance-related failures into four groups and designed incident analysis schemes. Error types:

- improper installation,
- servicing, improper/incomplete repair, improper fault,
- isolation/inspection/testing, actions causing foreign,
- object damage, actions causing surrounding equipment,
- damage and actions will cause personal injury [20], [21].

Another criterion is the contributing factor (PSFs), which says the process of sharing information, the working environment and equipment, the knowledge and the personnel experience, and how the company is managed and managed. Pre-flight helicopter preparation includes:

- helicopter pre-flight inspection;
- checking the amount of fuel, oil, hydraulic fluids and gases and, if necessary, replenishing them;
- placing removable equipment on the helicopter;
- check helicopter readiness according to task;
- preparation of ammunition;
- helicopter armament (as planned);
- troubleshooting.

The SHELL model places special emphasis on the human activity interface with other subjects of the analysed system. People's responsibility for performing aeronautical maintenance operations is expressed by L (Liveware). People's collaboration with establishments is expressed by H (hardware), and their relationships with various environmental factors are expressed by E (environment). Uneven contact edges are influenced by various factors, which are expressed by physical, psychological, and psychosocial conditions.

The Liveware - Software (L-S) factor expresses different forms of relationship between instructions, software used, checklist, and procedures. The factors on the L-L line are the relationships between the operator and the other in the workplace. The system operating errors are reflected on the contact edges.

Operating errors along the edge of the aeronautical maintenance operator and any element of the system may result in a decrease in the level of safety of air operations. The methods described in the first chapter were the basis for analysing the activities of maintenance personnel. The aircraft maintenance staff was experienced in all cases.

Table 2.

Operator error probability parameters used in TESEO (Bello and Colombari, 1980)
(Courtesy of Elsevier Applied Science Publisher Ltd)

Type of activity	
	K_1
Simple, routine	0,001
Requiring attention, routine	0,01
Not routine	0,1
Temporary stress factor for routine activities	
Time available (s)	K_2
2	10
10	1
20	0,5
Temporary stress factor for non-routine activities	
Time available (s)	K_2
3	10
30	1
45	0,3
60	0,1
Operator qualities	
	K_3
Carefully selected, expert, well trained	0,5
Average knowledge and training	1
Little knowledge, poorly trained	3
Activity anxiety factor	
	K_4
Situation of grave emergency	3
Situation of potential emergency	2
Normal situation	1
Activity ergonomic factor	
	K_5
Excellent microclima, excellent interface	0,7
Good microclima, discrete with plant	1
Discrete microclima, discrete interface with plant	3
Discrete microclima, poor interface with plant	7
Worst microclima, poor interface with plant	10

Based on the TESEO table 2, the following assumptions that best describe the system analysed were adopted:
K 1 = 0,01 - operation requires concentration
K 2 = 0,1 the available time is longer than 60 seconds
K3 = 0,5 - the operator is an expert
K4 = 1 - there may be a potential threat
K 5 =0,7 - ergonomic factors are at a good level

The human error probability was obtained by assuming the above assumption:
$P = K_1K_2K_3K_4K_5 = 0{,}01x0{,}1x0{,}5x1x0{,}7 = 0{,}\ 00035$

The reliability analysis of the work of an aeronautical maintenance worker using the HEART method was based on Generic Task Unreliability.

Table 3.

Generic Task Unreliability

Generic task	**Proposed nominal unreliability (5th – 95th percentile boundaries)**	
A	Totally unfamiliar, performed at speed with no real idea of likely consequences	0,55 (0,35 – 0,97)
B	Shift or restore system to a new or original state on a single attempt without supervision or procedures	0,26 (0,14 – 0,42)

C	Complex tasks requiring high level of comprehension and skill	0,16 (0,12 – 0,28)
D	Fairly simple task performed rapidly or given scant attention	0,09 (0,06 – 0,13)
E	Routine, highly practised, rapid task involving relatively low level of skill	0,02 (0,007 – 0,045)
F	Restore or shift a system to original or new state following procedures, with some checking	0,003 (0,0008 – 0,007)
G	Completely familiar, well-designed, highly practised, routine task occurring several times per hour, performed to highest possible standards by highly motivated, highly trained and experienced person, totally aware of implications of failure, with time to correct potential error, but without the benefit of significant job aids	0,0004 (0,00008 – 0,009)
H	Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system stage	0,00002 (0,000006 – 0,00009)
M	Miscellaneous task for which no description can be found.	0,003 (0,008 – 0,11)

Then it was used Error-Producing Conditions (EPCs):
H class task G = 0.00002 - Respond correctly to system command even Error-Producing Conditions in area a need for absolute judgements which are beyond the capabilities or experiences of an operator has a level 1,6.
The value of coefficients of influence was calculated by following a formula.

$$AE = ((E-1)\ .P) + 1 = ((1{,}6 - 1)\ .1) + 1 = 1{,}6 \qquad (1)$$

where the weight P was taken as 1, due to the fact, that it much limits the detection time of the deviation.
The probability of the error occurring was estimated at the following level:

$$P = 0,\ 0002x1,\ 6 = 0,\ 00032$$

In the long-term, we can see that the aircraft repair process is at a very good level, as shown by the ratio of flight hours, air accidents, and incidents. The existing processes for the current maintenance of technology are systematically developed and carried out by educated and qualified technicians.

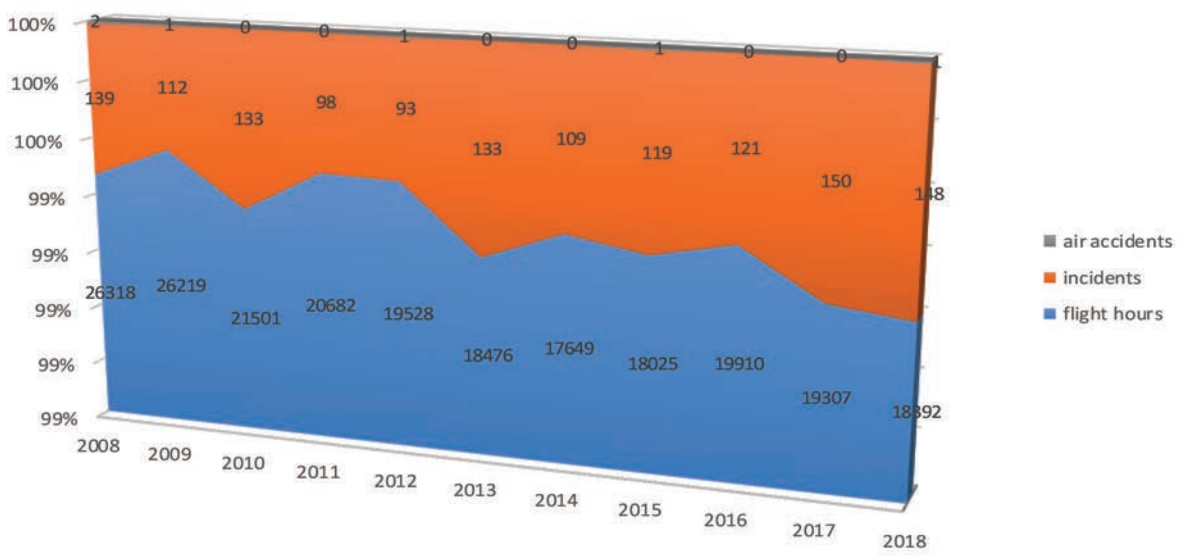

Fig. 1. The correlation between flight hours, air traffic events and air traffic accidents.[2]

[2] Custom processing based on the Annual Summary of Air Traffic Events 2018.

The airstrike trend for one event in air traffic has a decreasing tendency.

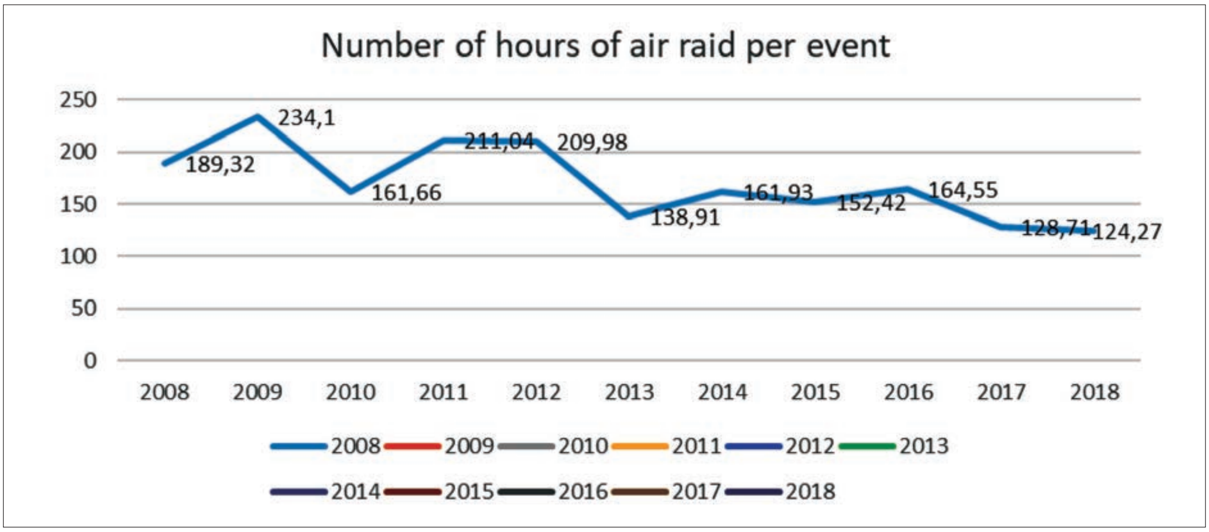

Fig. 2. Number of hours of air raid per event[3].

The above methods make it possible to determine the reliability of an aeronautical maintenance worker without taking account of the error that has occurred.

The reliability definition of effective aeronautical maintenance control can be described as the probability that the aeronautical maintenance worker will not make any errors.

In the case of an aeronautical maintenance system, two types of errors can be defined for an aeronautical maintenance worker:

- process errors are identified (manual) the worker does not take any steps to eliminate it - type I error,
- errors are identified in the process (manual) worker takes steps to cut it - type II error.

4. Partial Conclusion

Processing of air incident analyses for the years 2016 - 2019 showed that the maintenance system, timing of personal inspection activities and work carried out on specified types of helicopter preparation for flight and overview of prescribed work depending on the several hours flown, number of landings and standing time for helicopter Mi -17 of all versions maintenance is sufficient.

5. Hybrid Threats of the 21st Century

State and non-state actors seek to do political, economic and security goals by using a range of dimensions of power - diplomacy, information, armed forces, economics, finance, intelligence, public order and the rule of law.

Hybrid threats represent coordinated efforts, especially in the foreign power, cyberspace threats, energy, raw materials, industrial security, and terrorism areas.

Hybrid threats can also manifest themselves in the security aspects of migration and extremism.

Hybrid threats are mostly used as part of a coordinated campaign where may be overlapping threats, which represent confrontation, or conflict, in a latent form.

Hybrid warfare uses a combination of conventional and unconventional means by military, paramilitary and civilian actors. Actors using hybrid threats prepare conditions to prevent the event interpretation exploiting the weaknesses of the adversary, which disguised as legitimate targets in the area of interest.

The decision-making process destabilization of the State of interest makes it impossible to respond in a timely and effective way to the situation. Actors using hybrid threats against a territory of interest where they harm vital, strategic or security interests by creating a concept of credible deny (plausible deniability). Plausible deniability is the entity's ability to deny responsibility due to lack acts evidence committed by other organizational structures. Personal participation cannot be unequivocally confirmed. Identifying the originator of illicit activities is a complex legal process, although all available evidence suggests responsibility. At the same time, the originator has evidence to deny participation.

[3] Custom processing based on the Annual Summary of Air Traffic Events 2018.

The evidence submitted must be credible to be able to convict the author, even though he refuses to take part. During the originator identification, logical explanations and the context of the obvious benefits of supporting or organizing hostile activities are examined. The hybrid campaign also uses some form of military means, avoiding armed aggression so that the originator cannot be condemned by the international community.

Cyberspace is a specific area of hybrid warfare where cyber-attacks allow to intervene and threaten the functioning of public administration, critical infrastructure, or the financial sector. The exponentially increasing connectivity of cybernetic users increases the risk of cyber-attacks. The current period is characterized by the fact that the entity using the cyber-attack is the state. State-controlled cyber-attacks are directed against government institutions and businesses in critical infrastructure segments.

If the target country identifies the attack method pattern, the security level against cyber-attack is higher.

The discovery of scenarios makes it possible to take measures to protect sensitive systems and critical infrastructure information and cut potential damage. The originator of the cyber-attack prepares its interest for the medium to long-term horizon. The advanced technology and human factor use the originator to infiltrate the internal communication system.

5.1. Energy Sector as Part of Critical Infrastructure

The energy sector is an important part of the state's economy, and all forms of assault threaten the state's economy.

Analysis of the power outage in Ukraine in 2015 will identify the mode of cyber-attack operandi.

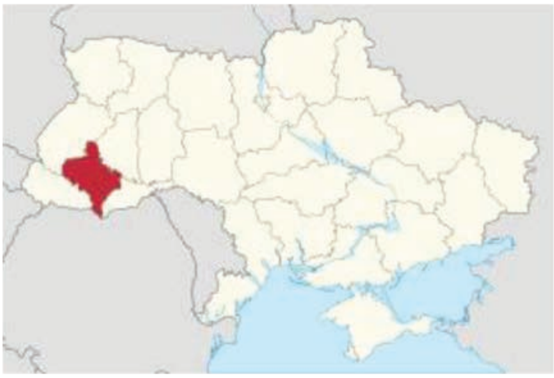

Fig.3. https://en.wikipedia.org/wiki/Ivano-Frankivsk_Oblast.

A power outage by attacking energy sources is one of the possible scenarios of cyber-attacks that could lead to paralyzing public systems. Cyber-attack scenarios include outages in the supply of energy and water services, transport systems [22], and communications networks. The cyber-attacker aim is to influence many of the population by restricting access to electronic devices. The percentage of reported attempts to penetrate energy networks is low due to active cyber-security measures taken.

On 23 December 2015, a cyber-attack was carried out against the residents of the Ivano-Frankivsk area, where the supply disruption occurred. One of the identified programs is BlackEnergy Trojan Horse.

The BlackEnergy malware package was developed in 2000 [23] and has been upgraded since its first use.

BlackEnergy's development phases have milestones between 2010 and 2014. In 2010, BlackEnergy 2 appeared, rewriting the code and implementing a simple installer to simplify the use of BlackEnergy.

In 2011, a UAC bypass was added to allow increased code execution privileges using a framework provided by Microsoft. Subsequently, the system was supplemented with a 64-bit driver. BlackEnergy 3 replaced the earlier version in 2014 and introduced a brand new program that did not use parts of the earlier version and implemented ID format as a timestamp, while using many advanced protection mechanisms. The new version includes plug-ins that enhance the BlackEnergy 3 performance features while allowing use by the originator. A prerequisite for powerful malware is the ability to cover the originator that uses fake Microsoft digital certificates and can disrupt and change the code signing process to authenticate the author. The originator can hide among the crimeware groups by sharing Tradecraft, which provides him with relationship and sponsorship coverage.

BlackEnergy 3 plug-ins are:

fs.dll — File system operations
si.dll — System information, “BlackEnergy Lite”
jn.dll — Parasitic infector
ki.dll — Keylogger
ps.dll — Password stealer
ss.dll — Screenshots
vs.dll — Network discovery, remote execution
tv.dll — Team viewer
rd.dll — Simple pseudo “remote desktop”
up.dll — Update malware
dc.dll — List Windows accounts
bs.dll — Query system hardware, BIOS, and Windows info
dstr.dll — Destroy system
scan.dll — Network scan [24]

The originator of a cyber-attack uses malicious code to carry out temporary takedown of power substations.

In 2014, Dragonfly’s ability to carry out sabotage operations against selected targets was identified - oil pipeline operators, electricity generators, and Industrial Control Systems (ICS) equipment providers for the energy sector.

Like other hacking groups, the main goal of Dragonfly 2.0 is to gather information and access the target organization’s networks. Along with the input data collection, it organizes a group capable of carrying out sabotage operations. Dragonfly 2.0 focuses on the critical energy sector infrastructure in the interest countries, especially in the USA, Turkey, and Switzerland. Like earlier Dragonfly campaigns, hackers send malicious e-mails with specific content to the energy sector with the clear goal of gaining access to a potential victim’s network.

The group uses a toolkit called Phishery (available in GitHub) that uses malicious email to do an attack. E-mail carries an encrypted message to a potential victim. Because the hacking group uses publicly available management tools such as PowerShell, PsExec, and Bitsadmin, it is very difficult to prove a negative impact on the critical infrastructure of the country of interest. Dragonfly 2.0 divides campaigns into phases that are part of the strategy. The most significant and time-consuming is the phase of gaining access to operating systems, which group exploits for a disruptive campaign in the future.

Cyber-attacks on energy networks are not a new thing. Energy companies in Ukraine, which hackers focused on two different occasions in late 2015 and late 2016, indeed caused a power outage in several regions in Ukraine, causing tens of thousands of citizens to go out around midnight [25].

Hacker groups use a human factor to give them access to a network of critical infrastructure of interest. The network penetration strategy based on:

1. sending malicious emails,
2. „watering hole” attacks”[4],
3. infecting software with a Trojan horse,
4. malware programs.

Hacker groups collect the information and credentials that underlie the potential launch of an attack by:

1. detection of internal communication,
2. breaking the e-mail system,
3. theft of company data,
4. threatening physical violence,
5. targeted spear phishing emails[5].

If the activity of the hacking group focuses on a private company or private entity and internal communication is detected, the interest society is forced to disconnect the systems from the network. The threat of a cyber-war led by states was identified in 2016, when the originator of the cyber-attack was first identified. The cyber-war threat led by states was first revealed in 2016 when the attacked state authorities identified the originator of the cyber-attack.

5.2. Spyware in Ukrainian Artillery (2014-2016) [26]

Ukrainian artillery officers receive an infected version of the mobile application for fire control 122 mm howitzer D-30. According to CrowdStrike, Fancy Bear used Android malware against the missile forces and artillery of the Ukrainian Army from 2014 to 2016. The group distributed an infected version of the Android application, whose original purpose was to check the targeting data for the 122mm howitzer D-30. The application used by Ukrainian officers was infected with X-Agent spyware and was available on military online forums.

CrowdStrike, in a corrected version, confirmed that the malicious software caused about 15-20% [27] of the losses of the Ukrainian D-30 howitzers, and these losses “have nothing to do with the cause” [28].

[4] Frequently visited websites are infected with malware

[5] Emails that look like from trusted sources but actually contain malware or other malicious content.

5.3. Active Cyber Security Strategy

Cyber-attacks originate their attacks usually in cooperation with the security strategy of the contracting state so that, the attack is phased, and uses the full spectrum of DIMEFIL strategy.

The identified fact requires a potentially attacked state to develop a strategy for securing government systems across a range of potential violations.

Cyber-attacks are performed, in several stages, as follows:

1. gathering information,
2. a regular presence in the system using Advanced Persistent Threats (APTs) and Remote Access Tools (RATs),
3. data acquisition,
4. Implementation of Attacks.

The methods used in the process of breaching the system security integrity are the same, both for self-acting hacking groups and for state-sponsored activities. The direct effort of the originator in the preparatory phase is to do knowledge that will limit the latter disruption of the internal communication network. In preparation, the attacker focuses on collecting and analysing data, which is then used to prepare and execute an attack on critical systems.

The modern technologies implementation by organizations to cut cyber threats to the communication system must be supported by a strategic plan that will represent a comprehensive set of activities to do a synergy outcome. A hybrid strategy is an offensive strategy based on the party's willingness to take measures to protect values, the willingness to oppose the originator, and the level of risk acceptance by the originator. Many experts have also identified the need to support the international community in defending the contested party.

It can be stated that lowering the level of strategic communication of critical infrastructure is the key to mastering the critical infrastructure system.

The originator may use non-hybrid actions that cut the willingness and threshold of the attacked party to take action in a hybrid environment. The attacked party is taking measures to increase the willingness and lower the threshold of the hybrid attack possibility, and at the same time must clarify, and prove the level of attack reality using all components of DIMEFIL. The aim of the attacked party is to cut the risk of hybrid attacks, to the lowest possible extent while maintaining the support of their own population by clearly defining the originator and its target.

An active approach to dealing with hybrid threats implies a reduction in the acceptable level of threats while increasing the willingness to take and carry out measures against the agent. The mathematical model is defined by the capacity χ of the attacked party, the level of the threat level τ, and the willingness ω .

The relationship of factors can be expressed by the formula:

$$\chi = \tau - \omega \tag{2}$$

If $\chi \leq 0$ it can be assumed that the originator supports or initiates an armed conflict. The originator seeks to keep the capacity χ above zero (ie $\chi > 0$), until it completely destabilizes the attacked party and creates an environment that will enable it to make its geographical and strategic goals. The threat level threshold is dependent on four parameters as follows:

1. normalization of the current level of instability,
2. STRATCOM originator,
3. STRATCOM of the contested state,
4. Area level achieved in all DIMEFIL areas.

The cyber-attacks different phases in the long and medium term use a historically comparative method to assess the originator activities. Analysis of the originator's activities shall analyze verbal or written manifestations, including any identifiable previous actions and the frequency of their implementation.

The frequency of events in the area of interest is part of the draft hybrid strategy, which analyses the impact on regions of the state of interest, national groups, and the level of uncertainty of state development, including confidence in improving the economic and social level. Normalization parameters are an important indicator for the normalization factor calculation and include ethnic and religious divisions, levels of discrimination or tolerance, and possibly levels of rivalry.

5.4. Vulnerability

ICT Security Checking is aimed at examining the existing vulnerabilities occurrence within the operating systems, Middleware, and applications themselves. Penetration tests are one of the options, and in their early stages they use methods of scanning and identifying existing vulnerabilities, which are then often manually verified (if false-positive detection). However, their primary aim is to verify the (no) compromise of the systems and solutions as a whole and not to compile a full list of all existing vulnerabilities within the tested infrastructure.

The penetration tests frequency even in large organizations, which care about the system's security, is rather in the order of units of test per year, which is not sufficient given the speed at which new vulnerabilities arise today. Penetration tests can help us with vulnerability management in some way, but they cannot be fully replaced.

Vulnerability management is an important topic in today's IT world. The number of vulnerabilities is increasing every year, and 31,000 new unique vulnerabilities have been identified this year, which are described and recorded in the National Vulnerability Database (NVD) [29].

The Common Vulnerability Scoring System (CVSS) [30] the severity of each vulnerability is determined in four severity levels - low, medium, high, and critical. Of course, the most critical are vulnerabilities rated critical, often having a significant impact on the triad of systems (confidentiality, integrity, availability), and their exploitation tends to be simpler than for less serious vulnerabilities [31]. Vulnerability Management [32], [33] is a tool that enables the detection, analysis, and removal of vulnerabilities in an organization's network, increasing security and reducing the risk of attacking a communications network.

The vulnerability management process begins with identifying and analyzing vulnerabilities and prioritizing them, using the Vulnerability Management Systems (VMS) vulnerability management tool. VMS tools enable vulnerability detection, analysis, prioritization, and reporting through the "Open Web Application Security Project" (OWASP) method [34]. The vulnerability management process can be divided into three basic phases - the detection, reporting, and removal phases. The process in the preparatory phase requires the scope of vulnerability management to be determined. The preparatory phase defines the scanned systems, the responsibility for managing vulnerabilities, the form, and method of removing vulnerabilities, or accepting risk.

The first step of the detection phase is to determine which systems will be scanned to determine the level of vulnerability, how they will be scanned, and at what intervals and time windows. The scanning type is different for systems inside and outside the network perimeter. The authenticated scan is used for systems under the control of corporate administrators in the LAN, using privileged accounts with higher than normal permissions. Classic network scanner is used for systems located outside the company's perimeter. Privileged scanning creates less network and system load by scanning directly on the target device, and can also detect vulnerabilities in software that does not communicate on any network port. However, the disadvantage of privileged scanning is the need to create an account on all scanned systems, which can be a problem for an organization with a large number of devices.

Another important factor is the scanning schedule, where the use of the system by users or other systems on the network must be evaluated. For this reason, scans are performed especially, during the night hours or outside working hours. Critical production servers are scanned every day, less critical systems are scanned once a week. Also important is the awareness of all parties involved, asset owners, firewall managers, IDS or IPS systems, and other monitoring systems. The subsequent analysis is performed according to the OWASP methodology, and the whole process of this phase is shown in Fig. 4.

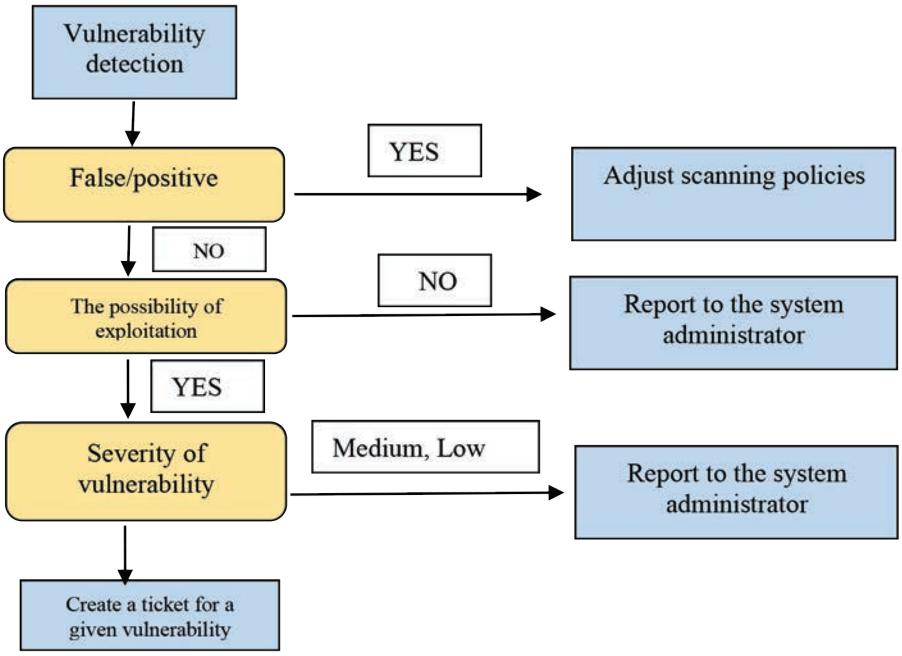
Vulnerability detection
False/positive
YES
Adjust scanning policies
NO
The possibility of exploitation
NO
Report to the system administrator
YES
Severity of vulnerability
Medium, Low
Report to the system administrator
Create a ticket for a given vulnerability

Fig. 4. Vulnerability analysis and reporting process.

In the second phase, according to OWASP methodology, vulnerability analysis and reporting are performed. Assets or scanned devices can be categorized according to various criteria such as function group, geographical location, type of environment, type of operating system, etc.

Other groups of devices may arise from information about vulnerabilities present on these devices. As part of the analysis, it is necessary to select from all the vulnerabilities identified the ones that pose the greatest risk. The right vulnerability management tool is able to prioritize assistance, and in addition to the CVSS assessment, it often provides its own vulnerability severity assessment, taking into account other vulnerability information (such as information on current vulnerability abuse from Threat Intelligence). Once vulnerabilities are prioritized, the most serious is to create tickets to monitor vulnerability remediation and quickly pass it on to asset owners. The final step in this phase is to create reports and distribute them to all stakeholders. The last phase of the OWASP methodology addresses the vulnerability removal process (shown in Fig. 5.).

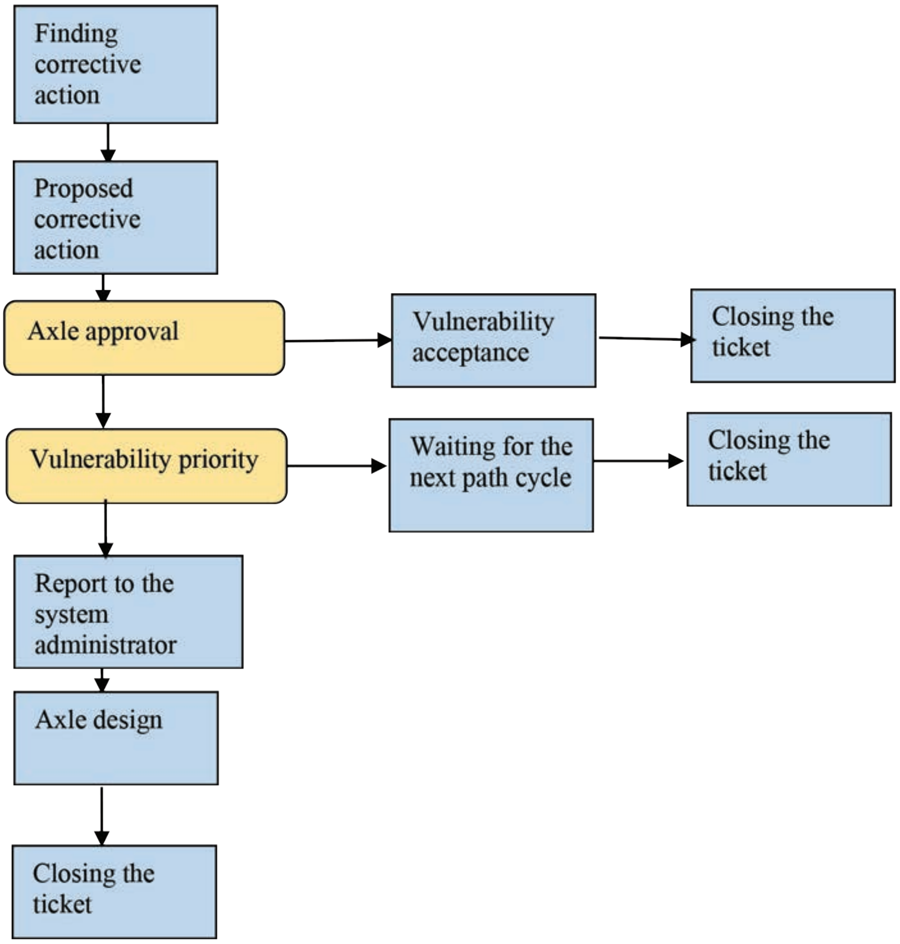

Fig. 5. Vulnerability removal process.

Eliminating each vulnerability is based on creating corrective action. The risk acceptance is based on an estimate of the impact on the system. Once the vulnerability has been removed, it is advisable to run a scan with the Vulnerability Management tool, which confirms the absence of the vulnerability and also marks it as deleted in its database. This type of scan is referred to as a remediation scan and is specific to the same settings as the original scan that was used to detect vulnerabilities.

A suitable solution to the described pitfalls is the implementation of processes adequate to the organization and their interconnection with the processes of IT operations, IT security, and risk management. The ideal way is to cover these processes within the GRC support tool because VMS / VRM tools cannot solve everything. A detailed description of the vulnerability is in the “Vulnerability Library”, which is synchronized with online vulnerability information sources available, such as the National Vulnerability Database operated by the US National Institute of Standards and Technology.

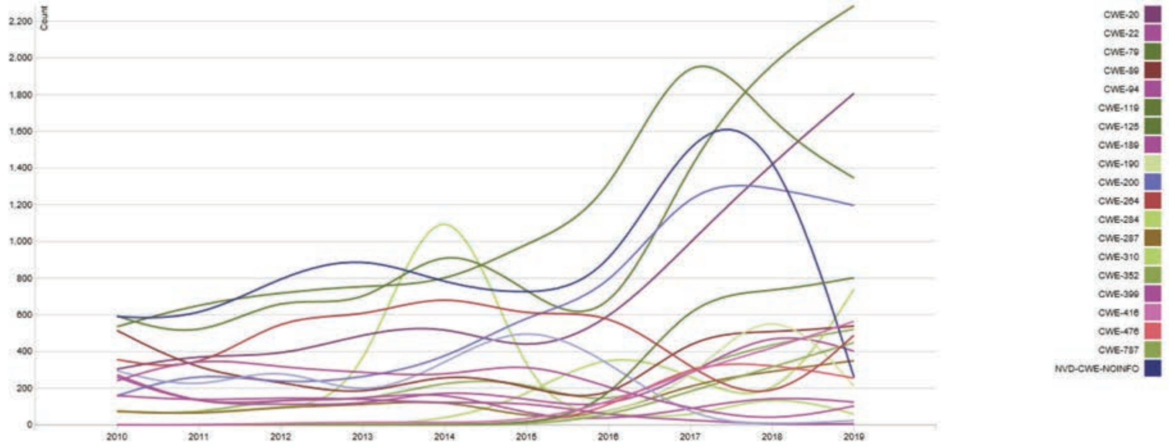

Fig. 6. Vulnerability Type Change By Year[6].

Common weaknesses Enumeration is divided into the "Portion of CWE Structure" tree, where they are visually depicted. Given the growing number of CWEs, it is necessary to respond to vulnerability development and to take action not only by network administrators but also on users.

Table 4.

Vulnerability percentage

CWE	%	
20	10,31	Improper Input Validation
22	2,32	Improper Limitation of a Pathname to a restricted directory
79	13,16	Improper neutralisation of input during web page generation
89	3,1	Improper neutralisation of special elements used in SQL command
94	0,72	Improper control of generation of Code
119	7,72	Improper restriction of operations within the bounds of a memory buffer
125	4.59	Out of bounds read
190	1,13	Integer overflow or wraparound
200	6,85	Information exposure
264	2,82	Permissions, Privileges, and Access Controls
284	4,27	Improper Access Control
287	1,96	Improper Authentication
352	3	Cross-Site Request Forgery (CSRF)
399	0,29	Resource Management Errors
416	3,25	Use After Free
476	1,47	NULL Pointer Dereference
787	2,46	Out-of- bounds write
NVD	1,5	

6. Importance of the Human Aspect in Cyberwar

Increasing the security level of critical infrastructure systems depends on the ability to improve the human aspect of the enterprise (internal) communication system. Cyber-attackers exploit a low-level of knowledge of the human cyber-protection agent, in particular by opening and spreading infected e-mails and links.

The human information security factor has begun to receive increased attention, especially when security technologies fail to protect the network from cyber-attacks [35], [36].

As a first step, users' access to critical systems can be limited (as needed) to decrease the likelihood of damage. Ongoing and regularly updated staff training is a key element in reducing cyber threats and developing a cyber-security strategy.

[6] https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cwe-over-time

6.1. Cyber Security Tools

Tools and technologies remain important, but as state-supported hacking groups have access to the latest technologies, it is clear that users and organizations need to be one step ahead, especially if they are equipped with older software and systems.

An effective cyber security strategy must involve more than just technology. Training workers to understand the risks of cyber-attacks and to discover the usual ways in which these attacks are conducted. Targeted spear fishing is a way to report and ease potential problems before harmful activities can take place. Even the most effective security system can be frustrated by human error. The critical infrastructure communication network security is based on software security. It is important to find, check, and correct vulnerabilities in software applications before integrating software into the system, even during its use.

Cyber security programs lower the risk of ensuring that all software is safe and secure. By applying consistent testing criteria, critical infrastructure entities can begin to cut abuse, effect known malware, strengthen security controls, and increase security awareness. Critical infrastructure protection is increasing in many areas, including cyber-security. Both the civilian and military segments are taking steps to respond to threats and risks.

The Czech Republic is gradually implementing two ways to increase the cyber security level. The first area is the continuous education of people in internal and external communication, and the second area is the efficient setting of processes in all areas of air traffic. The aim is to eliminate communication and automate activities.

The Civil Aviation Authority and the Army of the Czech Republic respond continuously to the recommendations of the National Cyber and Information Security Agency by establishing processes or structures for fighting in a cyber-environment. Army of the Czech Republic creates Cyber Forces (CF) to monitor, plan, and conduct operations in cyberspace and information environment at the tactical level and support planning and management of strategic communication.

The aim of CF will be to increase resistance to cyber-attacks (including prediction, detection and response) in communication and information systems and especially in weapon systems used in the Army of the Czech Republic. CF will be able to support other types of forces in comprehensive management of information operations using the full range of legal tools. Information operations are fully integrated into ACR joint operations. Strengthening cyber security requires an increase in the level of coordination of the level of public authorities. Increasing the level of cyber security requires support for research, implementation of technological innovation, and user education.

The human error elimination should be supported by the establishment of several areas of internal communication, which will limit the possibility of external entities entering the internal communication network.

Reducing the level of exposure to cyber-attack can be achieved by implementing best practices based on increasing the level of employee knowledge in the areas of:

- computer threats
- control system vulnerabilities and attack paths,
- secure architecture design
- implementation of internal documents.

Knowledge of cyber threats of the control system is realized by persons who try to gain unauthorized access to the device or by using the control system networks via data communication path. Potential carriers within the organization can be trusted users, while at the same time connecting from a remote location by an unknown person using the Internet.

Hostile governments, terrorist groups, disgruntled employees and people, or groups deliberately acting as sources of potential deliberate threats to control systems can be the source. Intentional threats can be categorized by the originator as follows (Lawrence K. Gershwin) [37]

- National governments
- Terrorists
- Groups of industrial spies and organized crime
- Hacktivists
- Hackers

National governments are the main initiators of deliberate threats in the area of cyber-attack on critical infrastructure of the target state. To this end, national cyberwar programs are being developed. Damage to the national interests of the target country can be realized across the entire spectrum of DIMEFIL, ranging from low levels of action (propaganda, disruption of the website) to a high level that spans the full spectrum of activities ranging from espionage to widespread disruption of infrastructure. Obviously, large-scale cyber-attacks can only be undertaken in the next 5-10 years by national states that have the technologies and tools needed to carry out cyber-attacks on critical infrastructure elements.

6.2.Terrorists

Traditional terrorist adversaries are less developed than other types of adversaries in their ability to disrupt the computer network and susceptibility to using cyber means. They are, therefore, likely to pose only a limited cyber threat. We expect that cyber threats will be more significant in the future as more technically capable generations will join the ranks.

6.2.1. Industrial Espionage and Organized Crime

Industrial espionage and organized crime groups pose a medium threat to the Czech Republic / the European Union, particularly in their ability to exploit the potential of a young generation that has a positive attitude towards modern technology. We assume that their main goal is profit, but it is clear that gaining access to internal networks can increase the number of attacks on critical infrastructure entities.

6.2.2. Hackers

Hackers, represent a relatively significant threat, there may be a short-term disruption to the necessary operations, and may affect ground crews, with immediate impact on human lives and property.

As the hacker population grows, the likelihood that a qualified hacker will succeed in attacking critical infrastructure SW is increasing. The huge global volume of relatively less qualified hacking activities increases the inadvertently disrupting critical infrastructure possibility. Hackers can be subdivided for further investigation as follows:

- the sub-community of hackers,
- worm and virus makers (attackers who write promotional code used for worms and viruses to disrupt networks and connected computer systems).
- security researcher divided into two subcategories: bug hunters and decoders. Their goal is profit.
- a professional hacker who is rewarded for genuine intrusion into networks. Their goal is profit.

The Army of the Czech Republic creates Cyber Forces (CF) to check, plan, and conduct operations in cyberspace and information environment at the tactical level and to support planning and management of strategic communication. They will protect their own part of cyberspace, acquire information in cyberspace, and work in it.

Cyber Forces are able to provide information and analysis about the information environment, cyberspace, its individual elements, and actors in a common operating space. Cyber Force's aim is to support other force types in comprehensive information operations management using full range of legal instruments. Information operations will be fully integrated into ACR joint operations. CS elements will be capable of independent and joint interaction with other types of forces and VZ, both for the benefit of the ACR and allied operations. Increasing the security level of critical infrastructure communication networks is installing DMZ data between the corporate LAN and the LAN control system (see Figure 2). The added layer of protection will eliminate communication with the LAN control system to the internal LAN communication network.

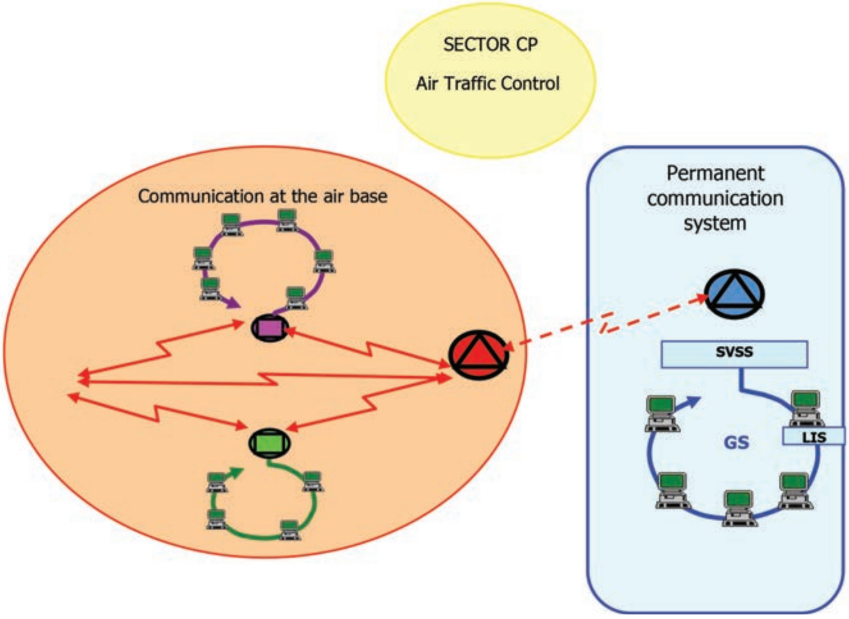

Fig. 2: Internal and external base and air traffic control communication network.

It can be confirmed that reducing the level of risk in the maintenance process is more to use intervention strategies than, such as, to improve individual motivation and training. It can therefore be stated that within the existing network and solution there is a restriction of access to the Internet and the use of portable flash discs.

7. Conclusions

The recommendations are directed to several areas, which together form a system to increase the level of safety. Recommendations will be directed to software security, physical security and vulnerability management.
1. In the area of software security, four key areas were identified as follows:
2. Insufficient updates - Manufacturers provide over-the-air (OTA) updates for a limited time.
Insufficient authentication - Requirements for a strong authentication mechanism with a complex password, or two-factor authentication and authentication mechanisms (Telnet or Basic http) are not sufficiently protected.
3. Change the default login and password.
4. Remote Access. The threat of remote access has two risk factors. The first is the presence of security vulnerabilities in the network services of the device and the second is exposure to the external environment of the Internet.
5. Poor physical security. Physical weakness poses a risk of access to the device storage after it has been removed. A potential attacker is able to access the system and connect to a USB port or other console port.
6. Unsecured communication. Most devices do not encrypt network communication, and both the administration interface and the cloud are communicated over unencrypted HTTP. The solution is encryption at the device interface and cloud services, such as the use of encrypted transmission and standards (TLS 1.2 and higher). Certainly achieve the level of autonomy of transferring internal communication through various networks (internally Bluetooth and Wi-Fi to the Internet).
7. Eavesdropping and Man in The Middle Attacks. Like unsecured communication, tapping inside and outside the network is a way to compromise sensitive information inside the communication.
The eavesdropping risks concern Ethernet and Wi-Fi networks as well as Bluetooth or Zigbee wireless technologies.
8. Personal data leakage. The transmission of diagnostic or statistical information by telemetry may present a risk if appropriate methods of protection are not used. The risk increases with the use of mobile smartphone applications on both iOS and Android platforms).
9. Lack of knowledge. The threat is primarily associated with a human factor. The solution is knowledgeable of good and best practices and security setting options. Deploying sophisticated firewalls and security features is one solution.

Acknowledgements

This work was conducted within air critical infrastructure security area dealing with internal and external communication. The authors are thankful for the close cooperation with Tuřany and Pardubice airport management.

References

1. **Johnson, R.** “Hybrid war and its countermeasures: a critique of the literature.” Small wars & insurgencies 29.1 (2018): 141-163.
2. **Treverton Gregory F., Thvedt A., Chen, R.A., Lee, K., McCue M.** Addressing Hybrid
3. Threats. https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf
4. Výroční zpráva Bezpečnostní informační služby za rok 2018, https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2018-vz-cz.pdf.pdf
5. Kybernetická bezpečnost, https://www.bis.cz/kyberneticka-bezpecnost/
6. **R. Wieszała, R., Gajdzik, B.** The effectiveness of environmental management in a metallurgical company’s sustainable development. Metalurgija 49 (4) (2010) pp. 353-356
7. **Rehak, D., Hromada, M.,** Failures in a Critical Infrastructure System. http://dx.doi.org/10.5772/intechopen.70446
8. **Čičmanec, L., Holeček, J., Kalvoda, P.** Use of an aircraft monitoring system for Condition Assessment of a maneuvering area. In: 2018 IEEE AIAA 37th Digital Avionics Systems Conference (DASC) Proceedings. Piscataway, NJ 08855-1331 USA: IEEE Service Center, 2018, p. 1573-1578. ISBN 978-1-5386-4112-5.
9. **Knowles, W., Alistair, B., McGarr, T.** The simulated security assessment ecosystem: Does penetration testing need standardisation? Computers & Security, Volume 62, September 2016, Pages 296-316
10. **Cherdantseva, Yulia, et al.** “A review of cyber security risk assessment methods for SCADA systems.”
11. Computers & security 56 (2016): 1-27.
12. National Offshore Petroleum Safety and Environmental Management Authority, Human reliability analysis.
13. https://www.nopsema.gov.au/resources/human-factors/human-reliability-analysis/
14. **Davis, J.R.** 2014. The Hybrid Mindset and Operationalizing Innovation: Toward a Theory of Hybrid. School of

15. Advanced Military Studies United States Army Command and General Staff College, AY 2014-01, Fort
16. Leavenworth, Kansas.
17. **Hoffman, F.G.** Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict.
18. Strategic Forum 240. 2009.
19. ICAO SHELL Model, https://www.skybrary.aero/index.php/ICAO_SHELL_Model. Accesed 28th January 2020
20. **Embrey, David E.** "Incorporating management and organisational factors into probabilistic safety assessment." Reliability Engineering & System Safety 38.1-2 (1992): 199-208.
21. RR679 - Review of human reliability assessment methods. https://www.hse.gov.uk/research/rrhtm/rr679.htm
22. **Cacciabue, P. C.** "Human factors impact on risk analysis of complex systems." Journal of Hazardous materials
23. 71.1-3 (2000): 101-116.
24. **Haver, S., Winterstein Steven R.** "Environmental contour lines: A method for estimating long term
25. extremes by a short term analysis." Transactions of the Society of Naval Architects and Marine Engineers 116
26. (2009): 116-127.
27. **Rotman, D. A.**, et al. "Global Modeling Initiative assessment model: Model description, integration, and testing
28. of the transport shell." Journal of Geophysical Research: Atmospheres 106.D2 (2001): 1669-1691.
29. **Berzinš, J.** Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy. 2014
30. Policy Paper no 02 April, Riga: National Defense Academy of Latvia.
31. **Wiener, Earl L.; Nagel, David C.** (ed.). Human factors in aviation. Gulf Professional Publishing, 1988.
32. **Takahashi K, Ikeda R., Okada Y.**, An evaluation of human factors on confirmation/check task in organizational Factors, Edited by:Peter Vink, AHFE Conference, 2014
33. **Sandom C., Harvey R.S.,** Human Factors for Engineers, IET, London, 2004
34. Swain A.D., Guttmann H.E., Handbook of human reliability analysis with emphasis on nuclear power plant aplications. US Nuclear Regulator Commision, Washington, 1983
35. **Kozuba J., Pila J.** Safety of complex aircraft ergatic systems, Transport Problems Vol. 14, Issue: 2, Gliwice 2019, pp.101-111, ISSN: 1896-0596
36. **Samani, R.,** Beek, Ch. Updated BlackEnergy Trojan Grows More Powerful, https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/
37. Updated BlackEnergy Trojan Grows More Powerful. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/
38. Dragonfly 2.0: Hacking group infiltrated Europian and U.S power Facilities: https://thehackernews.com/2017/09/dragonfly-energy-hacking.html
39. APT28, Pawn Storm, Sofacy Group, Sednit a STRONTIUM, https://cs.wikipedia.org/wiki/Fancy_Bear
40. Cyber Firm Rewrites Part of Disputed Russian Hacking Report, https://www.voanews.com/usa/cyber-firm-rewrites-part-disputed-russian-hacking-report
41. Defense ministry denies reports of alleged artillery losses because of Russian hackers' break into software, https://en.interfax.com.ua/news/general/395186.html
42. **Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L.** Gender difference and employees' cybersecurity behaviors Comput. Human Behav., 69 (2016), pp. 437-443
43. National Vulnerability Database [online]. [cit. 2019-06-21]. Dostupné z: https://nvd.nist.gov/
44. Common Vulnerability Scoring Systém SIG [online]. [cit. 2019-06-21]. Dostupné z:
45. https://www.first.org/cvss/
46. Severity Levels for Security Issues [online]. [cit. 2019-06-21]. Dostupné z: https://
47. www.atlassian.com/trust/security/securityseverity- levels
48. **Palmers, T.** Implementing a vulnerability management process. SANS Institute:
49. Information Security Reading Room. 2, 20
50. **Foreman, P.** Vulnerability management. Boca Raton: Auerbach Pub., c2010.
51. ISBN 978-1-4398-0150-5.
52. OWASP Vulnerability Management Guide [online]. [cit. 2019-06-21]. Dostupné z: https://www.owasp.org/index.php/ OWASP_Vulnerability_Management_Guide
53. **Herath, T., Rao, H.R.** Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness Decis. Support Syst., 47 (2) (2009), pp. 154-165
54. **Lawrence K. Gershwin.** The Statement for the Record to the Joint Economic Committee, the Central Intelligence Agency's National Intelligence Officer for Science and Technology, 21 June 2001.