PRACTITIONERS’ BROAD VIEW

SELFIE.ORG – SELF INTEREST EVALUATION OF FOREIGN INTELLIGENCE ENTITIES FOR ORGANIZATIONS

Florin BUȘTIUC[*]
Daniel DINU[*]

Abstract:

The pro-security attitude is necessary in an organization, for its survival from an economic and functional-administrative point of view. Therefore, an assessment of the existence of some situations may indicate an interest – incipient or developed – from some adverse/foreign intelligence entities, an assessment that subsequently determines the implementation and activation of some mechanisms for protecting values, such as personnel, facilities, information, equipment, networks and systems. As a principle, it is necessary for the organization to carry out a general verification of vulnerabilities, risks and threats through its own security structure, respectively through cooperation with state institutions.

Keywords: *economic espionage methods; sensitive information; security indicators; insider threat.*

Introduction

The state and private adversary intelligence structures target the institutions/organizations where information of interest of a political-diplomatic, military, social, administrative-legislative and economic nature is concentrated (and where strategies and decisions related to these areas are configured). If an adversary entity collects non-public information from the economic domain[1] (industrial espionage/

[*] Independent researcher, florinnn11@yahoo.com.

[*] Fellow at EuroMed Academy, daniel.dinu90@gmail.com.

[1] Sensitive information: *personally identifiable information* (personal details, identification numbers, digital identities, biometric records, personal characteristics or preferences); *financial information* (banking information, credit and debit card information,

corporate espionage, economic espionage), the following negative effects[2] may occur:

- *financial deficit* – compromising economic data correlates in most cases with significant financial losses (reputational damage and legal problems can also erode market shares and reduce profits).
- *loss of competitive advantage* – an adversary's access to non-public information can be transformed into the development of similar products or strategies.
- *reputational damage* – a successful attack by an adversary can erode the trust of customers and potential partners, investors.
- *legal implications* – in some cases, lawsuits may arise from investors or partners, who have also suffered from the espionage attack on your organization.
- *national security risks* – in some cases, the theft of information related to defence technologies or government projects could represent a threat to national security.

Information security, but also of other values – equipment, technologies, plans/strategies/decisions, people, etc. – is a necessity for the survival of an organization. Given that some of these values are also essential elements for national security, it follows that security becomes a necessary element at the organizational (private) and institutional (state) levels.

The general methods (*Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*) in which economic information is collected are the following:

1. *requesting information through e-mail or letters* – most requests are indirect, with reference to data available on websites, in advertisements, in articles in trade magazines and

transaction details, income and tax information, investment information); *health information* (medical history, diagnostic information, treatment records, health insurance data, family health history, lifestyle information); *business-sensitive information* (trade secrets, client information, employee information, strategic plans and research, contracts and legal documents, financial records, intellectual property); *high-risk data* (national identification numbers, biometric data, legal information, sensitive government information, sensitive corporate information), accessible to https://www.sealpath.com /blog/types-of-sensitive-information-guide/

[2] See more on https://www.ekransystem.com/en/blog/prevent-industrial-espionage

in marketing materials. Data collection (and as documentation for subsequent information requests) refers to publications and annual reports, patents, websites, marketing materials, conferences and exhibitions, professional contacts through membership in various associations – because there may be (inadvertently) sensitive/restricted information that becomes a support for directing the efforts to identify the connections of government entities with specific technologies and activities (AGGROS-aggressive open-source collection). Adverse information requests[3] are characterized as: a) initially legitimate questions that deviate into questions that clearly target sensitive, classified information, b) initially "banal" requests for price lists, catalogues, published works, research assistance, job counselling that become suspicious when they are characterized by insistence, persistence and focus on details, come from embargoed states, induce the idea of avoiding security and export control procedures.

2. *exploiting internet discussion groups* – the anonymity of the Internet is used in email-based discussion groups on various topics of interest related to recommendations for research activities and specific technical challenges (which may involve sensitive information and dual-use technologies).
3. *exploiting multinational conferences, business information exchanges or joint ventures* – such contexts represent an excellent pretext for gathering information (directly or through follow-up contacts) and for identifying and evaluating experts (in some cases, with specific cultural, ethnic, etc. backgrounds) in a particular field of interest.
4. *misleading open-source collection* – real interest, affiliation or location is camouflaged through "false associations" that create legitimacy/credibility of relationships, requests and reduce the likelihood of being identified as suspicious and reported/ ignored: use of the Internet from public libraries and educational institutions; routing e-mail through one or more countries to

[3] Adverse information requests – requests that, under the appearance of the normality of a relationship involving technical and psychological methods, ultimately aim to collect data of interest (sensitive, classified data).

hide the area of origin; use of contacts established within professional organizations and conferences.

5. *acquisition of export-controlled technologies* – the illegal acquisition of these types of technologies is carried out through: the use of front companies, transportation to an undeclared end user with forged certificates, the acquisition of an exportable version of a product and subsequent modification in the manufacturing process.
6. *theft of trade secrets, critical technologies, and critical information* – is carried out through classical intelligence services, state-sponsored educational and scientific institutions, private entities. But the current higher level of economic/ industrial espionage activities does not imply the disappearance of classical clandestine espionage – abroad, business people are potential targets, respectively, excessive elicitation is carried out at border crossings, hotel rooms are "searched", briefcases and laptops are "controlled".
7. *agent recruitment, co-optees and volunteers* – some people involuntarily become facilitators by arranging visits by foreign citizens to circumvent official procedures, present papers abroad, etc., and others voluntarily become agents[4].

Currently, courses are publicly provided on the use of HUMINT, including with reference to files and psychological profiles of potential sources; elicitation techniques; debriefing methodologies; information exploitation methods carried out at conferences and meetings. As a rule, human targets are[5]:

- *developers:* scientists, researchers, engineers who research and apply new materials/processes;

[4]Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, *https://irp.fas.org/ops/ci/docs/fecie_fy00.pdf; and https://apps.dtic.mil/sti/tr/pdf/ADA465107.pdf; and https://www.travelsecurity.ch/Annual_Report_to_Congress_on_Foreign_Economic_Collection_and_Industrial_Espionage.html. See details on https://www.jlab.org/intralab/security/ EconomicEspionageFactSheet.pdf and https://www.dcsa.mil/Portals/128/Documents/CI/DCSA_CI_Best_Practices_booklet.pdf*

[5] See more on https://www.dcsa.mil/Portals/128/Documents/CI/DCSA_CI_Best_ Practices_booklet.pdf

- *technicians:* engineers or specialists who operate, test, maintain, repair technical systems;
- *production personnel*: personnel on production lines or in the supply chain area;
- *IT personnel:* system administrators, people with access to networks and knowledge of security protocols;
- *business development personnel:* marketing and sales representatives;
- *human resources personnel:* people with access to personnel and applicant records;
- *facility employees:* personnel who have access to spaces/ locations where information of interest is circulated, such as security personnel, cleaning personnel, etc.

The specific methods by which economic information is collected are as follows[6]:

1. *theft*: the theft of information or products;
2. *blackmail:* the use of threat or intimidation to provide information;
3. *mole planting:* the placement of a double agent in a competing company;
4. *eavesdropping/corporate communication intercepts*: ranges from telephone interception to the interception of Wi-Fi signals and emails;
5. *seduction:* a timeless technique that uses emotional elements to obtain information*;*
6. *bribery:* influencing an individual by offering money for information or to carry out illegal actions;

[6] Learning from the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, *https://www.travel-security.ch/Annual_Report_to_Congress_on_Foreign_Economic_Collection_and_Industrial _Espionage.html. See details on DHS&CISA* - Chemical Security Summit *(2022), https://www.cisa.gov/sites/default/files/2022-12/summit-2022-intellectual-property-508.pdf and* Păstrarea unui secret comercial – Partea II [Keeping a Trade Secret – Part II], *https://ccir.ro/wp-content/uploads/2014/11/P%C4%83strarea-unui-secret-commercial-I.pdfß*

7. *foreign intelligence recruits:* some private entities recruit former intelligence officers to carry out data collection activities of interest*;*
8. *hiring competitors' employees*: valuable employees are hired;
9. *bogus job interviews:* conducting fake interviews with candidates solely to gather key information about the employer and activities*;*
10. *social intelligence relationships*: developing "friendships" with various employees at professional meetings; dialogues with salespeople, distributors, loading and transporting personnel, former associates; eliciting former schoolmates, knowledge from various professional associations;
11. *bogus purchase negotiations:* some entities present themselves as "buyers" to obtain key information;
12. *research under false pretences:* the "author" uses the research paper to obtain key information;
13. *trade fair conversations:* establishing contacts at fairs, especially with experts. It correlates with capitalizing on: a) the tendency to provide excessive technical data/details during a conference presentation or during business meetings or negotiations with potential partners, suppliers, contractors, licensees, customers, b) project proposals or proposals that may contain sensitive, valuable information;
14. *dumpster diving:* searching for materials thrown in the trash;
15. *naturalized citizens:* requests addressed to naturalized citizens to provide information for patriotic or loyalty reasons (or threatening family members in the state);
16. *repatriating naturalized citizens:* attracting said persons to the state of origin to take over processes and methods;
17. *government debriefing:* interviewing one's own citizens upon their return from a foreign state to obtain information*;*
18. *outsourcing/offshoring:* outsourcing activities to foreign entities/offshoring can affect data security (for example, in some countries copyright laws do not apply);
19. *front companies and organizations:* foreign competitors pose as software vendors or even non-profit organizations in order to access trade secrets;

20. *joint venture & bidding process:* foreign buyers may require the provision of a large amount of data in the bidding process*;*
21. *"close proximity":* strategic partnerships and alliances create the opportunity for their own personnel to be exploited for information;
22. *mergers & acquisitions:* through these processes, technologies, innovations, etc. are acquired;
23. *front companies* (import-export front): the illegal export of documents, data or other sensitive items is carried out;
24. *altered products or false certifications:* companies from one's own state are exploited as intermediaries for the export of controlled products to a hidden end user through falsification of documents;
25. *university research:* private/state intelligence structures place agents in university research units;
26. *"excessive" negotiation:* excessive requests for information are made during negotiations;
27. *third-party acquisition:* the final recipients are individuals, companies or states that can obtain technologies, equipment, etc. only through such diversion*;*
28. *luggage or laptop theft:* luggage/electronic equipment from hotel rooms is "searched/taken" (in some cases, customs representatives "seize" laptops, tablets or mobile phones to copy data);
29. *Cyber Espionage methods:* exploiting website/browser vulnerabilities; attacking the supply chain, directly on primary partners or indirectly through Joint Venture; infecting third-party software application updates; distributing digital monitors accessible via wireless/external ports; requesting sensitive information through social engineering, phishing, compromising business emails, etc. (by choosing targets from lower/middle-level personnel, who are less likely to be suspicious).

In the context of presenting the general and specific methods of gathering information (from the economic area), we consider it appropriate to also present separately the internal organizational threat – the insider, who is the person who has or has legitimate access to or knows the resources, including personnel, facilities, information, equipment, networks and systems.

The insider is represented by the current employee, contractual partners, temporary personnel engaged in the activities of the organization (out-sourcing contracts, internships, experience exchange, etc.), former employee, as follows[7]:

- a person in whom the organization trusts, including employees, members of the organization and those to whom the organization has provided sensitive information and access;
- a person who has received a badge or access device, which identifies him as a person with regular or continuous access (for example, an employee or member of an organization, contractor, salesperson, caretaker, repairman);
- a person to whom the organization has provided a computer and/or network access;
- a person who develops the organization's products and services, including those who know the secrets of the products that give value to the organization;
- a person who knows the fundamentals of the organization, including prices, costs and its strengths and weaknesses;
- a person who has knowledge of the organization's strategy and business objectives and is entrusted with future plans and the means to support the organization and to ensure the well-being of its employees;
- in the context of government functions, we have people with access to protected information, which, if compromised, could cause harm to national security and public order (*Insider Threat Mitigation Guide,* 2020, p. 9.).

The directions of action of the insider are represented by espionage, sabotage (physical or electronic), unintentional disclosure of information (to a third party or the media), facilitating access by a third party to the values of an organization (locations, information, personnel),

[7] Processed version of some aspects of the material *The human factor as a threat from within. Insider – understanding and approaches* (2023), related to the research activity within ANIMV.

theft of intellectual property, fraud by corrupting processes (altering internal processes, procedures and systems for financial or other purposes) (*Insider Threat Detection Study, 2018*).

Security indicators

The idea that, from an economic point of view, threats manifest themselves at the state and private level (but with effects in terms of national security) also correlates with the dimension of identifying a potential interest/ information gathering activity on the part of an adverse entity, a dimension that is circumscribed by security indicators.

Security indicators refer to observable behaviours, situations or circumstances that reveal that potential espionage or terrorist activities are being carried out, or other activities of gathering, transmitting, using, or disclosing unauthorized information. Reported to the insider, from the material *Analytic Approaches to Detect Insider Threats* (2015, pp. 14-24), two general types of indicators result, provided by *technical components* (systems/ computer programs, surveillance mechanisms and databases) and *non-technical* (data from security forms, self-declarations, personnel files, reports from colleagues and professional management).

Technical indicators (associated with the IT and physical surveillance system) (*Analytic Approaches to Detect Insider Threats*, 2015, pp. 14-24**):**

a. **authentication and authorization.** It is performed to access relevant resources of the organization, especially those considered fundamental to the organization's activity. These resources include data, services and capabilities and are available in operational systems, but also in backup systems. Failure to authenticate or attempted unauthorized access indicates an interest in data that is not related to professional duties.
b. **data access pattern** (specific time and frequency of access to relevant data). Changes in the access pattern indicate an interest in resources that were not previously associated with professional needs, potentially for unauthorized purposes. Access inconsistent with the user's class/level, related to

information that is not usually accessed in professional activity, may signal unethical purposes.

c. **network access/usage patterns** (specific protocols, source and destination, data packet sizes and frequency of sessions associated with user applications/operations). Changes in patterns (deviations from usual behaviour) signal changes in the user's goals, attitude and skills. It is a primary indicator for financial fraud and conjunctive data theft. Patterns inconsistent with the user's class/level (deviations from usual network traffic) may indicate possible disinterest or abusive behaviour. It is a primary indicator for accidental leaks, espionage and conjunctive data theft.

d. **data exfiltration** (unexpected or unauthorized movement of sensitive data from the organization's systems). A large/ unusual volume or certain types of data that "leave" the institution through printing services, e-mail or memory media is detected.

e. **unauthorized data access methods** (unauthorized or unusual connections to facilitate access or movement of data from the institution's official systems). Unauthorized connections of devices or between systems or unauthorized activities related to the movement/transmission of data are identified.

f. **system state changes with errors.** These are rapid changes in the system configuration that result in a state of insecurity, followed by attempts to repair the system to the initial configuration/state. It reveals inadequate training or system testing (unusually rapid changes in commands or a defensive posture associated with user errors and attempts to resolve these errors) and is a primary indicator for misuse and conjunctive data theft, and a correlation indicator for accidental data leaks and product alteration attacks.

g. **(inappropriate) use of commands**. Repeated occurrences of unexpected or unusual commands, related to the activity of colleagues, indicate a lack of training or testing of the system's response. It can be a correlation indicator for detecting accidental data leaks.

h. **access knowledge.** Efforts to acquire excessive knowledge, in contradiction with professional duties, may indicate "negative" goals of the user. Changes in data search patterns, including massive searches and directory browsing or access to a wide range of data, especially those not related to professional activity, are primary indicators for espionage, abuse and contextual data theft, and correlation indicators for financial fraud.

i. **change in audit logins.** The modification or deletion of security data or audit logins is detected.

j. **changes in pattern of access time**. Unexplained or unusual changes in a user's work schedule (logging into internal resources without credentials or multiple days of continuous access) could indicate an attempt to perform an activity while avoiding observation by colleagues or managers/ administrators.

k. **changes in pattern of access location**. Unexplained or unusual changes in the location(s) from which a user typically accesses a system indicate attempts to circumvent audit or security mechanisms, or to avoid observation by colleagues or managers/administrators.

l. **defect/error detection** (product defects or creation of unauthorized functionality). A pattern or history of product defects that do not correspond to the user's skill level may indicate negligence or an attempt to diminish or damage an organization's reputation, or to facilitate attacks against the organization's customer base. It is a primary indicator for sabotage attacks and could be a correlator for system misuse or workplace violence.

m. **malware execution**. Unauthorized installation/execution of an unauthorized program is an indicator for espionage, system misuse or sabotage.

n. **removal or modification of data or infrastructure**. Unauthorized deletion or change of data indicates behaviour that is likely intended to cause harm. It is a primary indicator for financial fraud, system misuse and product tampering.

o. **recovery (acts of unusual data recovery).** Recovering corrupted or deleted data from backup or archive indicates that data has been inadvertently deleted, or that there is an attempt to cover up traces of temporary changes or deletions. It is an indicator for conjunctive data theft and a correlator for accidental data leaks, financial fraud and system misuse.

p. **security breaches.** These are unauthorized activities that impact the security of an organization. Change in breach patterns - changes in the frequency or severity of security breaches are detected. Duration and regularity - monitoring incidents over time. Unauthorized or inappropriate use of tools, such as network analytics tools, that are specifically detrimental to the business/institution (installation of unauthorized functionality).

Non-technical indicators (personal, social and professional):

a. **competitor analysis**. It analyses capabilities or products that seem to indicate an advantage derived from knowledge of data that has not been made public. It identifies unexpected developments correlated with potential losses related to intellectual property. It is a primary indicator for espionage and system misuse.

b. **media analysis.** It identifies that unauthorized data has been disclosed. It is a primary indicator for espionage, system misuse or physical theft, and it is an indicator of correlation of accidental data leaks.

c. **recent increase in criminal activities.** Criminal activity can damage the reputation of an organization or pose a threat to the organization or its employees.

d. **violence outside the workplace.** Stress and violent behaviour outside the workplace can indicate an increased likelihood of violence against the organization or colleagues.

e. **major life events**. Major life events (e.g., change in marital status, birth of a child, or death of a relative) can impact work behaviours and create tensions that precipitate inappropriate decisions.

f. **changes in financial and material possibilities** (unexpected resources or debts). *Observable changes over time* – a sudden influx could indicate that an individual is being bribed or influenced to carry out a harmful activity; sudden and excessive debts may be associated with stress that can impair rational capacity. *Changes in comparison with colleagues* – differences can create tensions that impact decision-making. *Financial reports* – significant changes reported by financial reports or other external sources may indicate hidden wealth or financial stress.

g. **salary withholdings**. Legal actions to collect debts indicate financial stress that may warrant additional scrutiny of an individual related to financial fraud attacks.

h. **unusual contacts** (contacts with individuals or groups carrying out potentially negative/harmful activities, which may indicate that those relationships have an inappropriate influence on the employee). *Unusual business trave*l – changes in business travel to foreign countries not usually visited in the normal course of business, or meetings with representatives of these countries. *Personal travel* – discovery of frequent travel to foreign countries not usually visited in the normal course of business, or meetings with representatives of these countries (this is noted if the employee has attempted to conceal the travel). *Unauthorized or inappropriate associations* with hostile groups or participation in their actions may indicate a change in loyalty/belief/mentality, which may precede acts of deterioration of an organization's values.

We supplement the security indicators related to insider (which focus on the internal perspective of the threat) with indicators[8] that

[8] Indicators processed from the *Mini-guide for Counter-Information Training and Protection* (2015, Buștiuc Florin), Bucharest, SemnE Publishing House, and capitalizes on the following materials: *Department of the Army*. (1993). *Army Regulation 381–12. Military Intelligence Subversion and Espionage Directed Against the U.S. Army (SAEDA) and* Counterintelligence Office of the Defence Investigative Service. (2000). *Suspicious indicators and security countermeasures for foreign activities directed against the US Defence Industry*, https://irp.fas.org/doddir/army/ar381-12-1993.pdf; Department of Commerce - Office of Security. (2006). *Suspicious Indicators and Security Countermeasures*

highlight the *relational dynamics of insider-suspicious activities of a foreign entity*.

Indicators that the organization's personnel are in the attention of an adverse information structure (Buștiuc, 2015):

a. some employees receive (unusual) congratulations or other correspondence from the embassy of the country of origin;
b. some employees receive invitations to visit the country of origin, to give a scientific presentation or to receive an award;
c. foreign visitors try to selectively relate to personnel who show similarities (cultural, ethnic, religious, etc.);
d. some employees from sensitive sectors of the organization are insistently and frequently sought out by former colleagues.

Indicators that the organization is the subject of intelligence gathering activities (Buștiuc, 2015):

a. application for employment: some individuals offer their services under minimal financial conditions, stating that a foreign state/company bears the costs; the field in which the person chooses to work is related to a military component or involves classified technology.
b. assistance/partnership activities: provision of software products and assistance from "offshore" states; offering government or "business" scholarships; invitations for intercultural exchanges, through individual partnerships or within a general program.
c. co-opting of former employees: a former employee is employed by a company with the same field of activity; the former employee actively maintains contacts with some members of the organization.
d. activities within contract negotiations: unjustified requests for access to the internal computer network; requests for unrestricted physical access; requests to transmit a large volume of technical data in order to subsequently cancel the contract; sending a disproportionate number of representatives.

for Foreign Collection Activities Directed against the United States, https://apps.dtic.mil/sti/tr/pdf/ADA470350.pdf; Defence Security Service. *Counterintelligence CI Best Practices for Cleared Industry*, https://security.research.ucf. edu/Documents/CI/Counterintelligence%20Best%20Practice%20for%20Industry.pdf

e. *foreign visits:* people added to the visitor list at the last minute; visitors ask questions that go beyond the topics set for discussion (they rely on polite answers); visitors ask for a lot of data and in return provide general explanations; some visitors do not have the necessary experience/qualification in the field; "lost" visitors, who appear offended when explanations are asked about their presence in a space other than the designated one; a visitor who is very curious about employees, programs and work areas that were not included in the agenda.
f. *exhibitions, seminars:* the topics are related to classified topics; the state or organization sponsoring the seminar previously requested visiting some objectives but a refusal was made; invitations to present a specific topic, which include all costs paid; requesting a summary of the paper 6-12 months in advance and requesting development/detailing of some aspects; conversations during and after these events in which other professional aspects are attempted to be addressed.
g. *actions of personnel exploitation*: technical means of surveillance are introduced in hotel rooms, meeting spaces; attempts are made to create compromising situations; excessive requests for assistance and advice.

Information, technology, people, reporting/signalling methods are the fundamental elements for a threat identification and mitigate program – each element can independently provide a suspicious aspect, but the correlation/integration of the elements reveals the significant aspect indicating the existence of an internal and/or external threat. In this context, we consider the SELFIE.org questionnaire useful as a tool for organizational self-assessment of the interest of adversary/ foreign entities.

There are 45 questions that refer to situations that signal a potential informational interest of an adverse entity (natural person & legal entity, state) – organization, institution, competitor/adversary state or potential partner, adverse state intelligence service, adverse private intelligence structure (and their representatives). The questionnaire is intended to be completed by decision-makers – since an attempt was made for the questions to cover situations valid simultaneously for state and private organizations, regardless of the situation, it is mandatory to select an answer related to the viability of the situation for one's own organization (even in particular/ atypical cases).

Annex 1: The SELFIE.org questionnaire

1. Do employees frequently report that there are adverse entities that are interested in obtaining classified/non-public information?
□Yes □No
2. Do employees frequently report that at various conferences/meetings, topics are addressed that demonstrate knowledge of data that has not been made public?
□Yes □No
3. Do employees report that during meetings/conferences they are asked "innocent/camouflaged" questions in order to collect sensitive information?
□Yes □No
4. Are there any signs that some of the competitors are aware of negotiation strategies/objectives?
□Yes □No
5. Does non-public information about your organization appear in the media or specialized publications?
□Yes □No
6. Does an adversary entity eliminate you from different markets, fields, partnerships, negotiations, etc. with similar products and services?
□Yes □No
7. Do adversary/foreign entities carry out recruitment procedures for their own experts by conducting "interviews" for a possible employment, in which explanations, details related to sensitive data are atypically requested?
□Yes □No
8. Do employees report that they have been asked by adversary/foreign entities to carry out "extra-professional" studies, syntheses, translations, etc. related to sensitive data?
□Yes □No
9. Do laptops, documents, USBs containing important information disappear in uncertain situations?
□Yes □No

10. Before/during the steps associated with the act of resignation, does one or more employees avoid, do not make concrete references to the new job?
□Yes □No
11. Are there constant, unusual requests for planning visits to the organization's headquarters or different branches?
□Yes □No
12. Are there unannounced requests for information (in the form of questionnaires, market studies, etc.) by e-mail/telephone and are they addressed in most cases to people who are not part of the responsible specialized department (public relations etc.)?
□Yes □No
13. Are topics addressed that were not included in the discussion program, is the list of visitors changed at the last minute, are visitors accompanied by embassy officials who try to protect their identity and minimize the expression of an official position?
□Yes □No
14. Does an adversary issue invitation to attend international seminars, meetings, after failing to plan a visit to your organization's headquarters?
□Yes □No
15. At (international) seminars/meetings, do some participants carry incomplete or false identification marks?
□Yes □No
16. Do foreign visitors select staff who have a similar cultural/ethnic background, in order to network, socialize or carry out a joint professional activity?
□Yes □No
17. In the context of official visits, do some visitors seem to not have the same level of expertise as others, are they not attentive/not focused on the agenda of the visit?
□Yes □No
18. In the context of official visits, does a "lost/confused" visitor feel offended when asked for explanations regarding his presence in a space other than the one designated for visitors?
□Yes □No
19. During trips abroad, are attempts made to create compromising situations (staging a theft, an accident, drug possession, a situation of infidelity etc.)?
□Yes □No

20. Have been received emails requesting information about your organization or an employee's professional activity?
□Yes □No
21. During the hiring process, do some individuals offer their services at minimal financial terms, stating that a foreign state/organization is covering the costs?
□Yes □No
22. During the hiring process, is the field in which the individual chooses to work related to a military component, dual-use or export-restricted technology, or classified topics?
□Yes □No
23. During assistance/partnership activities, are products and software support provided from "offshore" states?
□Yes □No
24. During assistance/partnership activities, are government or "business" scholarships offered?
□Yes □No
25. During assistance/partnership activities, are invitations made for intercultural exchanges, through individual partnerships or as part of a general program?
□Yes □No
26. Are several former employees employed by an organization with similar fields of activity?
□Yes □No
27. Do a former employee(s) actively maintain contacts with some members of the organization?
□Yes □No
28. During negotiation activities/professional exchanges, are there unjustified requests for access to the internal computer network?
□Yes □No
29. During negotiation activities/professional exchanges, are there requests for unrestricted physical access?
□Yes □No
30. During negotiation activities/professional exchanges, are there requests to transmit a large volume of data in order to subsequently cancel the conclusion of the contract?
□Yes □No

31. During negotiation activities/professional exchanges, are there a disproportionate number of representatives from an adverse entity sent?
□Yes □No
32. During visits by foreign delegations, are there people added to the visitor list at the last minute?
□Yes □No
33. During visits by foreign delegations, do visitors appear who ask questions that go beyond the topics set for discussion?
□Yes □No
34. During visits by foreign delegations, do visitors appear who request a lot of data and instead provide general explanations?
□Yes □No
35. During visits by foreign delegations, a visitor who is very curious about employees, programs and work areas that were not included on the agenda?
□Yes □No
36. During visits by foreign delegations, is assistance and advice excessively requested?
□Yes □No
37. Are the topics proposed/addressed during exhibitions, seminars, meetings related to sensitive, classified topics?
□Yes □No
38. An adversary entity that was denied meetings, visits to objectives, transmission of certain data, etc., subsequently sends invitations to exhibitions, seminars that it organizes/sponsors?
□Yes □No
39. Does an adversary entity send invitations to exhibitions, seminars, etc. where it pays all the costs paid, but with the express request to present certain topics?
□Yes □No
40. When organizing exhibitions, seminars, is a summary of the material previously requested and then, in a phased manner, the development/ detailing of certain aspects?
□Yes □No

41. When organizing exhibitions, seminars, do conversations occur during and after these events in which other professional aspects are attempted to be addressed?
□Yes □No
42. During trips abroad, do employees report that they had the feeling that they were being watched/there were technical means of surveillance in hotel rooms, meeting spaces?
□Yes □No
43. Is employee/some employees involved in unauthorized Internet discussion groups where various topics of interest related to professional activity are addressed?
□Yes □No
44. Has employee/employees been requested information about colleagues, professional activity, etc. by foreign authorities at border crossings or in the context of incidents on the territory of the respective foreign state?
□Yes □No
45. Does employee/employees perform (massive) data searches and consult directories that are not correlated with professional activity?
□Yes □No

How to interpret the scores (the sum of the Yes answers):
1-15 – normally, an organization is a target for an adversary/competing entity, and the score highlights that you are within the normal limits of a "probing". The recommendation is to implement or specifically activate a mechanism for awareness and reporting by all employees of security indicators, respectively physical and IT mechanisms for identifying intentions to access unauthorized spaces, equipment and data.
16-30 – is a signal that there is an active, sustained interest from an adversary entity. The recommendation is to ask the security structure to re-evaluate the effectiveness of security policies and rules, physical and IT protection mechanisms, to apply security questionnaires to assess the level of knowledge and training of personnel, respectively to conduct training sessions in different specific areas. It is also necessary for the security structure to carry out various exercises to test the application of the rules and the functioning of the mechanisms, respectively to ensure

that the signalling of security indicators is working. At the level of decision-makers, it is necessary to define the appropriate responses/ reactions at the administrative and legal level to eliminate vulnerabilities and risks.

31-45 – it is necessary for the organization to carry out a general verification of vulnerabilities, risks and threats (compliance with security rules, IT access, personnel re-evaluations, and interviews with personnel, etc.) through its own security structure, respectively through cooperation with state institutions.

References:

1. Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. https://irp.fas.org/ops/ci/docs/fecie_fy00.pdf and* https://www.travel-security.ch/Annual_Report_to_Congress_on_Foreign_ Economic_ Collection_and_Industrial_Espionage.html

2. *Buștiuc, Florin. (2015).* Mini-guide for Counter-Information Training and Protection*, Bucharest, SemnE Publishing House.*

3. *Buștiuc, Florin. (2023).* The human factor as a threat from within. Insider – understanding and approaches*.*

4. *Cybersecurity and Infrastructure Security Agency. (2020)*. Insider Threat Mitigation Guide, *p. 36, https://www.cisa.gov/sitesdefault/files/publications/ Insider%20Threat%20Mitigation%20Guide_Final_508.pdf*

5. *Defence Security Service. (n.d.).* Counterintelligence CI Best Practices for Cleared Industry*.https://security.research.ucf.edu/Documents/ CI/Counterintelligence%20Best%20Practice%20for%20Industry.pdf*

6. *DHS&CISA* – Chemical Security Summit. *(2022). https://www.cisa.gov/ sites/default/files/2022-12/summit-2022-intellectual-property-508.pdfß*

7. *Department of the Army. (1993).* Army Regulation 381–12. Military Intelligence Subversion and Espionage Directed Against the U.S. Army (SAEDA). *Counterintelligence Office of the Defence Investigative Service. (2000).* Suspicious indicators and security countermeasures for foreign activities directed against the US Defence Industry*, https://irp.fas.org/doddir/army/ar381-12-1993.pdf*

8. *Department of Commerce – Office of Security. (2006).* Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed against the United States*, https://apps.dtic.mil/sti/tr/pdf/ADA470350.pdf*

9. Insider Threat Detection Study. *(2018). NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf*

10. Learning from the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage. *https://www.travel-security.ch/Annual_Report_to_Congress_on_Foreign_Economic_Collection_and_Industrial_Espionage.html*

11. Păstrarea unui secret comercial – Partea II [Keeping a Trade Secret – Part II], *https://ccir.ro/wp-content/uploads/2014/11/ P%C4%83strarea-unui-secret-commercial-I.pdfß*

12. Software Engineering Institute. (2015). *Analytic Approaches to Detect Insider Threats,* pp. 14-24. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=451065