PRACTITIONERS' BROAD VIEW

HOW TO TAKE SECURITY SELFIEs – *SELF INTEREST EVALUATION OF FOREIGN INTELLIGENCE ENTITIES*

Florin BUŞTIUC[*]

Abstract:

The pro-security attitude is stimulated by (self) asking questions such as: Have there been negative experiences regarding information security? Where is the institution's greatest security vulnerability? Where is the resistance to implementing security procedures (and why)? Is the need to protect the organization realized? Are employees within the structures on topic regarding their role and responsibility in protecting the organization's assets?

Through awareness it is possible to focus on threats – the identification of FIEs that created/can create the breach in the "security wall". The security self-questioning restructures the individual's thinking system, which accepts, in its subjective reality, the existence of threats generated by FIEs that affect the economic, social, political or military interests of the state[1].

Keywords: *Foreign intelligence entities, FIEs, intelligence, counterespionage, targeting, access***.**

Introduction

Foreign intelligence entities/FIEs are permanently active in gathering information – at any time, in any place, from any person of interest – which takes place under different "official covers", such as those of a journalist, businessman, researcher, student, participant in a scientific event, member of a delegation etc., thus exploiting the

[*] PhD, "Mihai Viteazul" National Intelligence Academy, email: florinnn11@yahoo.com

[1] Some aspects have been taken from the doctoral thesis *Pregătirea contrainformativă a persoanelor cu acces la informații clasificate/nepublice* defended in 2021 at the "Mihai Viteazul" National Intelligence Academy.

legitimate activities of delegations, private companies, scientific institutes, and media organizations.

The principles of intelligence activity highlight that an adversary will use all means, ethical and unethical, legal and illegal, to obtain information. In order to achieve their objectives, the adversary entities identify, prioritize and select targets (persons, groups, organizations) according to their importance, capabilities, accessibility, intentions and vulnerabilities (NATO Standard AJP-3.9, 2016).

FIEs aim to make contacts that allow them to be inserted into relational circles in order to interact with people (targets) of interest (NATO Standard AJP-3.9, 2016) considering their access: a) directly to the data of interest; b) the areas where this information is circulated; c) people, such as colleagues, chiefs, friends who handle that data (Buștiuc, 2015, p. 15).

The first step of FIEs is to identify a person who has access to data of interest (or belongs to a specific relational environment) and to make a profile from CVs posted on the institution's page, articles published in magazines, dialogues with former/ current colleagues etc. (Loch, 2010, pp. 312-313) At this stage the most important and difficult step foe FIEs is to answer the question *How to establish a connection?* (Sulick, 2007), and the pretext is a scenario with identity and functions, socio-professional roles specially manufactured for the purpose of accepting and building a relationship (Hadnagy, 2011, pp.111-112). A catalyst factor in building the pretext is the invocation of a common hobby, cultural, ethnic, religious similarity etc. (Ostrovsky and Claire, 1993, p. 213)

FIEs – as an individual – is a "sociable and friendly" person who carries out apparently "normal and natural" activities, disguising his purpose to obtain the information of interest; tries to capitalize on any "reasonable" situation that allows him to relate to persons of interest and constantly evaluates his "intelligence potential (access to information, persons, and locations)".

Direct contact with a target is done undercover – salesmen, businessmen etc. – being a pragmatic way to determine strengths and vulnerabilities in the event of a recruitment (a personal connection is also built). The contact can also be indirect, through:

a) employees from lower/middle levels (assistants, IT experts, etc.), who have information about other employees;

b) people from outside the organization (consultants, spouses, friends etc.), who can provide (voluntarily or involuntarily) data of interest or signal potential problems of the target (Brown, 2011, pp. 67-68).

Direct access to information or systems is crucial, but people with indirect access can also be selected (consultants, lawyers, IT experts, assistants, archivists, Xerox operators, etc.), because they can access certain data without generating suspicion (Brown, 2011).

A significant amount of private information has become public, because the use of social media platforms requires the creation of an account associated with personal information – identity data, date of birth, geographic location, hobbies etc. (Social-media-privacy-issues, 2020)

In order to insert themselves into a social environment where they can identify potential targets (or make a contact), the FIEs study the "rituals" (activities and lifestyle) of the individuals and the group, respectively establish common places and interests that can justify the initiation of the relationship. So, FIEs observe the posts of people (targets) on the Facebook page, LinkedIn, etc., from where patterns can be figured out from various purchases, vacations, membership groups, etc. – for example, the photos from the home/hotel room and the selection wardrobes can become indicators of lifestyle (Brown, 2011, p.60).

Moreover, the existence of personal data on social networks (CVs, opinions, posts and comments, relational circle, photos, etc.) can facilitate the identification of a person who can be influenced to reveal information, ways to approach that person (common interests, motivation, etc.) or to outline vulnerable aspects (Brown, 2011, p.59). For FIEs, human sources represent the most valuable "tool", and they will use covers that facilitate the presence in different situations and environments to identify and relate to "a target" (Buştiuc, 2015).

Targeting activities (identification of persons of interest who have access to data, environments, locations) are not geographically limited – an adversary will carry out such activities in his state (where it has more resources and has greater freedom of movement) but,

depending on the needs, also in foreign states where the person is living or traveling.

An objective of counterespionage is to identify the "antidote" specific to each of the clandestine information gathering techniques, developing measures to prevent the activities of FIEs. But the prevention effort must be a common one, assumed by counterespionage and by people who have access to information, environments, locations etc. (*Intelligence* no. 30) In this context, we appreciate that it is relevant for a person to have the possibility to verify through a questionnaire/test if he is a potential target of FIEs ("is targeted"), and in affirmative case to report this aspect to the competent institutions.

*

There are 27 sentences-statements related to **situations that can signal that a person is being targeted by FIEs**, considering the pretexts, behaviours and interests shown by the interlocutors. Determine which is true or false.

1. During some discussions, an unjustified interest appears for non-public subjects from various fields (political, military, economic, social, and administrative).

□ True □ False

2. The interlocutor requests that all meetings must be official and you should communicate them at your workplace.

□ True □ False

3. Intentionally false statements about some aspects of the professional field and the request for "detailed explanations".

□ True □ False

4. The frequent approach of some subjects under the pretext that they are of common interest, but which are related to the professional field.

□ True □ False

5. Questions about income, professional satisfaction and rewards, personal problems, about family members, friends, colleagues, etc.
□ True □ False

6. Requesting personal points of view, in addition to official statements.
□ True □ False

7. At seminars, scientific congresses, delegations, etc., there are people who have incomplete, vague identification data on their badges or/and who have an interest in certain topics.
□ True □ False

8. Atypical, inexplicable, unusual difficulties or situations at the time of arrival/departure at the customs point (interviews conducted by non-customs personnel; under various pretexts, detention, checking of the phone, laptop, memory sticks, devices electronics, etc.).
□ True □ False

9. Difficulties or atypical / inexplicable / unusual situations during the trip abroad (obvious surveillance actions; acts of intimidation, physical restraint for various reasons; attempts to stage thefts, accidents, etc.).
□ True □ False

10. The request, outside the official framework, for consultancy, support for the writing of articles, reports, translations, etc., related to the professional activity, with financial reward.
□ True □ False

11. Requesting data that are circulated only within the institution, such as the organizational chart, staffing scheme, internal telephone directory etc.
□ True □ False

12. Unusual invitations to seminars or scientific congresses, exchanges of experience, etc., where all costs are paid.
□ True □ False

13. Repeated attempts to determine excessive alcohol consumption during meetings, associated with questions about the personal area and the professional field.
□ True □ False

14. Participation in conferences, symposia, workshops, delegations, etc. of people who are not familiar with the field and unconvincingly motivate their presence, but are very active in terms of social relations and availability for further contacts.
□ True □ False

15. It is found that the luggage, laptop, among the documents in the room were searched at the hotel.
□ True □ False

16. It is found that some people, compared to the functions and studies invoked, have a superior knowledge/training.
□ True □ False

17. An interlocutor hides the fact that he knows your language or other foreign languages.
□ True □ False

18. Re-contacting by people met in different contexts abroad, who claim that they currently work in a field related to your professional activity.
□ True □ False

19. During business trips abroad, frequently the host accommodates you at the same hotel and even in the same room.
□ True □ False

20. The request to borrow your computer, tablet, phone, storage devices for copying or accessing materials, programs.

□ True □ False

21. An interlocutor demonstrates that he has knowledge about aspects of your personal life and professional activity, but only in relation to those that appear in open sources.

□ True □ False

22. Unconvincing, unjustified requests from some individuals to be introduced at official or private events where colleagues or people who have access to data of interest (political, military, economic, social, administrative) are present.

□ True □ False

23. Receiving an email requesting data about the organization or the professional activity.

□ True □ False

24. During some meetings, it is found that the interlocutors are familiar with aspects that were not discussed in their presence.

□ True □ False

25. The interlocutor does not have a problem with the interpersonal relationship being known at work, in the family or in the circle of friends.

□ True □ False

26. Asking for explanations and details about topics and aspects that the interlocutor should already know through his professional and academic training.

□ True □ False

27. The interlocutor presents / has presented you with false facts about jobs, positions or studies.

□ True □ False

ANSWERS
How scores are calculated

1-T-0,5p	7- T-1p	13- T-1p	19- T-1p	25-F-0,5p
2-F-0,5p	8- T-0,5p	14- T-1,5p	20- T-1p	26- T-1p
3- T-1p	9- T-0,5p	15- T-1p	21-F-0,5p	27- T-0,5p
4- T-1p	10- T-1,5p	16- T-1p	22- T-1p	
5- T-1,5p	11- T-0,5p	17- T-1p	23- T-1p	
6- T-1p	12- T-1p	18- T-1,5p	24- T-1p	

How to interpret scores (the sum of the matching answers points-**p**)

***1-9p* –** Only in obvious, atypical situations, which you did not initiate – for example, an incident at customs or while traveling – you have the feeling that "something is wrong", but usually you ignore the red flags. As for interpersonal relationships, if the interlocutor is pleasant in communication and motivates you in any way for his requests, you stop paying attention to the fact that they may be unjustified or that the explanations are not convincing. The recommendation is to participate in a counterintelligence training to make you aware that targeting exists and that in some situations it is even possible to have/have had a FIEs as your interlocutor.

10-18p – If obvious, atypical situations arise, which you did not initiate - for example, an incident at customs or while traveling - then your alarm system is activated, you become more vigilant and you are attentive to subsequent events, noticing in most cases that "something is not right".

In the case of social interactions, in most cases you notice that "something is not right" if the people are unknown. But if you have developed a relationship over time, then you fail to realize that there may be an interest, a hidden objective of the interlocutor. It is recommended

that you attend a counterintelligence training with practical exercises to practice your ability to recognize that you are the target.

19-27p – You are a person who pays attention to details, you have a very good ability to notice that "something is not right". You have very well-developed prudence, you want details, you ask questions, you do not believe in the declared sincerity of the interlocutor. You have the ability to make correlations between various aspects and determine that there is an interest, hidden objective. In most cases you realize that you are a target.

References:

1. Brown, Andrew. (2011).*The Grey Line: Modern Corporate Espionage and Counter Intelligence,* Kindle Edition, Amur Strategic Research Group, retrieved from https://www.scribd.com/read/206815606/The-Grey-Line-Modern-Corporate-Espionage-and-Counter-Intelligence

2. Buştiuc, Florin*.* (2015). *Minighid de pregătire şi protecţie contrainformativă – factorul uman & organizaţia,* Bucharest, Semne Publishing House.

3. Hadnagy, Christopher. (2011). *Social Engineering: The Art of Human Hacking*, SUA, Wiley Publishing, Inc.

4. Johnson, Loch. (2010). *Evaluating "Humint": The Role of Foreign Agents in U.S. Security*, Comparative Strategy, 29:4, 308-332, DOI: 10.1080/01495933.2010.509635

5. Sulick, Michael J. (2007). *Human Intelligence*, retrieved from http://www.pirp.harvard.edu

6. Ostrovsky, Victor, Claire, Hoy. (1993). *Mossad-Academia înşelăciunii*. Bucharest, Globus Publishing House.

7. NATO Standard AJP-3.9. *Allied Joint Doctrine for Joint Targeting*. Edition A Version 1. 2016, retrieved from https://www.nato.int/cps/su/natohq/publications.htm

8. *Key social media privacy issues*, retrieved from https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020

9. *Intelligence,* no. 30, retrieved from https://www.sri.ro/fisiere/publicatii/Revista_Intelligence_nr_30.pdf