PRACTITIONERS' BROAD VIEW

INVULNERABLE – INFORMED ABOUT VULNERABILITIES!

Florin BUŞTIUC*

Abstract:
A hostile intelligence entity is trying to identify or create behavioural vulnerabilities – professional dissatisfaction, unrealistic expectations, gambling, spending/borrowing beyond means, expensive lifestyle, financial difficulties, so as to exploit them to influence the person to reveal confidential information or to adopt certain decisions.

One of the ways of counterintelligence protection of data and decision is the awareness by individuals of vulnerabilities and reality that can be exploited by a hostile entity. And the purpose of a test on vulnerabilities is to evaluate the level of awareness and, implicitly, self -protection.

Keywords: *hostile intelligence entity, vulnerabilities, self-control, non-public/ confidential data.*

Introduction

The aim of this paper is to address the vulnerabilities of a person with access to classified and sensitive information in order to straighten the awareness and *self –protection*. The objective of a hostile intelligence entity[1] is to deliberately obtain certain information about people or organizations (projects, negotiations, research, contracts, etc.) that creates disadvantages for the latter, i.e. it affects their interests.

Frequently, a hostile intelligence entity carries out activities under the cover of a journalist, researcher, businessman, participant in a scientific event, member of a delegation, etc. – thus, the "presence and

* 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 official delegations, private companies, scientific institutes, media organizations, etc.

A hostile intelligence entity builds a relationship with the person of interest, and the existence of vulnerabilities facilitates influencing him to divulge (involuntarily) or engage (voluntarily) in illegal data collection activities.

Vulnerabilities refer to those psycho-social personality characteristics – behaviours, motivations, situations, connections with certain persons / organizations / states – on the basis of which a hostile intelligence entity maximizes his chances of influencing that person. We exemplify the following vulnerabilities:

- **personal difficulties** – divorce, bankruptcy, medical problems, addiction are factors that create the possibility of exerting influence by interested entities;
- **lack of loyalty** – belonging to different organizations of the underworld, the appropriation or use of large sums of money (large-scale financial frauds), the self-interested exploitation of security knowledge to establish possible deficiencies, the provoking and maintenance of a tense atmosphere in the collective, generating suspicion and mistrust among employees, exploiting curiosity and indiscretion or negligence and lack of interest;
- **gossip/boasting** – indiscretions committed through telephone conversations or telegrams or by discussing confidential professional issues in public, in circles of friends or in the family; the imprudence/indifference of officials who describe, with too much luxury of detail, at the various international meetings or specialized publications, the nature of their work, research, discoveries etc.;
- **immoral behaviours or behavioural deviations** that can generate the risk of the person being vulnerable to blackmail or pressure – as a rule, there are "sensitive" situations related to intimate life or things that affect the family climate or social image. In some cases, people are blackmailed by threats to their physical integrity or by exploiting their feelings. Vulnerability to blackmail refers both to the targeted person

and to family or close members, friends, collaborators or other people who enjoy a special condition (children, neighbours, colleagues, etc.);

- **connections with persons who could exert acts of pressure / blackmail**, respectively which could generate exploitable vulnerabilities by hostile foreign intelligence services and organized crime groups;
- **the need for money** – covering expenses related to solving some health problems; payment of debts resulting from gambling, loans from various "friends"; the amazing lifestyle, the satisfaction of personal pride;
- **mental or emotional disorders/alcohol consumption affecting discernment** – equivocal, disorganized behaviour. These people can be used for direct criminal purposes – by subordinating the will – or indirectly, by exploiting the "gray" in their area of responsibility;
- **ideology** – some individuals adhere to certain values/ideas, which, in their view, "are not respected" in the social practices and actions of the institution, and therefore disclose information. (Brown, 2011; NATO Standard, 2016)

In this context, *threats* represent people who directly support the objectives of some entities (intelligence entities or interest groups) to have access to confidential information and create security breaches, and *risks* are acts of collection, transmission, destruction, unauthorized modification of information. In the absence of vulnerabilities, the person resists to influence and refuses involvement in illegal activities. But when there are vulnerabilities, the capacity for resistance decreases, and *the paradox is that in most cases the person does not realize that he/she has a vulnerability or has the illusion that they are in control.*

Being aware of vulnerabilities creates the possibility to give up certain behaviours, to cancel or reduce motivational anchors, to avoid involvement in situations and connections with certain people/ organizations/ states. Consequently, the possibility of diversifying options and professional development is preserved, in the context of an institutional assessment of vulnerabilities in some cases, when access to

non-public data is necessary, and that assessment could result in refusal of access to information.

*

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 vulnerable person and to address this issue appropriately, and we propose the following questionnaire[2]. There are 27 sentence-statements regarding motivations, behaviours, situations, connections with certain persons/organizations/states, which can constitute vulnerabilities. Determine which is true or false.

1. The feeling of frustration, professional dissatisfaction, feelings of revenge and punishment of the "guilty": the institution/professional management.

□True □False

2. Connections with persons – relatives, friends or business partners – who have residence in a (hostile) state that has been established to be actively involved in gathering information about/from Romania.

□True □False

3. Existence of situations or involvement in activities that could affect public image if disclosed (for example, extramarital affairs).

□True □False

4. The tendency to believe that the interlocutor is in good faith and that he has no hidden interest, a tendency that determines the formulation of detailed answers to questions, even when they are related to professional activity.

□True □False

[2] The instrument is the author's view. Other tools are presented in Florin Buștiuc, (2015). *Minighid de pregătire și protecție contrainformativă – factorul uman & organizația*, Bucharest, Semne Publishing House.

5. Scientific collaboration or consultancy with any person or organization on topics related to professional activity, which has been approved.

□True □False

6. Deliberate omission, concealment or falsification of aspects in biographical statements and official forms.

□True □False

7. Deliberate provision of false or distorted data to an employer or state institutions.

□True □False

8. Connections with a person, group or organization that may create a conflict of interest with regard to the obligation to protect information that is of interest to those entities.

□True □False

9. Fraud, theft from the employer, use of false loan statements.

□True □False

10. Exaggerated optimism, with underestimation of the possibility that one may be a target for information gathering.

□True □False

11. Irresponsible spending and excessive indebtedness.

□True □False

12. Borrowing significant sums to participate in gambling or to pay gambling debts.

□True □False

13. A controlled consumption of alcohol, so that discernment is not impaired.

□True □False

14. Consumption of substances that affect discernment.
□True □False

15. The tendency to propagate negative, exaggerated, tendentious comments about people or situations, which can lead to the disclosure of data about possible dysfunctions in the field of security in the organization.
□True □False

16. Pathological gambling, betting on ever-higher stakes.
□True □False

17. Tendency to discuss work-related matters with family members or friends.
□True □False

18. The cautious attitude and the application of the principle that it is not obligatory to answer all questions, respectively to reveal everything you know in relation to subjects related to professional activity.
□True □False

19. Disregarding or ignoring an organization's information protection rules.
□True □False

20. Participation in various events or magazines with articles or materials related to the professional activity that were previously presented to be approved by the competent factors.
□True □False

21. Talkativeness and boasting that materialize in indiscretions.
□True □False

22. Pride, the tendency to always be right and demonstrate competence.

□True □False

23. The feeling of gratitude, the moral or financial obligations to persons, groups, organizations or states that may create a conflict of interest regarding the obligation to protect information that is of interest to those entities.

□True □False

24. Very high financial needs due to difficult situations – divorce, medical expenses, bankruptcy, etc.

□True □False

25. The belief that we are superior and that the (security) rules don't apply to us because we are different.

□True □False

26. The greed for compliments and sympathy that can lead to the disclosure of some aspects related to the professional activity, in order to recognize the "value, importance, merits" and preserve the relationships.

□True □False

27. Very high lifestyle / standard of living, which cannot be supported by legal income.

□True □False

ANSWERS

The scores are calculated upon the relevance for the vulnerabilities and the sum is 27 points (where false is not in the following table, the score is 0):

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

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

1-9p – Some would characterize you as a "naïve" person, for your opinion that it is not moral for someone to exploit certain negative aspects of the personality. Besides, you don't perceive these aspects as vulnerabilities, but as traits or "events" that need to be accepted by others, and the person counselled to modify them. This option is also possible, but you must be aware that, in relation to professional activity, it is appropriate to interpret reality through the lens of vulnerabilities. A hostile intelligence entity will exploit these traits or "events", and everyone is responsible for being aware of vulnerabilities and developing self-control.

10-18p – As a rule, you identify only "serious" vulnerabilities, such as consumption of prohibited substances, falsification of documents, gambling, significant irrational spending, etc. You are less attentive to the aspects that manifest themselves in the process of inter-human relations and which are subtler, more difficult to accept – to admit that you are a "talker", that you want to be right and impress with professional knowledge, etc.

19-27p – You know very well what the vulnerabilities are, but also the strong points of the personality. You have a very good self-protective attitude, i.e. you anticipate from the beginning that getting involved in certain situations, establishing connections or developing certain behaviours can degenerate into vulnerabilities. You have very good self-control and the ability to manage situations and relationships where information is sought.

Conclusion

Thus, reasonable explanations are invented so that these aspects are no longer perceived as vulnerabilities – you are not a talker, you are a very sociable person who energizes events; you do not disclose matters related to your professional activity, but you are an honest person who presents others with the correct version of a subject, etc. But you have

the ability to accept that your interpretations are wrong and that some aspects of your personality are vulnerabilities.

References:

1. Brown, Andrew. (2011). *The Grey Line: Modern Corporate Espionage and Counter Intelligence,* Kindle Edition, Amur Strategic Research Group, retrieved on June 27, 2022 from https://www.scribd.com/read/206815606/The-Grey-Line-Modern-Corporate-Espionage-and-Counter-Intelligence

2. Buștiuc, Florin. (2015). *Minighid de pregătire și protecție contrainformativă – factorul uman & organizația,* Bucharest, Semne Publishing House.

3. NATO Standard AJP-3.9. *Allied Joint Doctrine for Joint Targeting*. Edition A Version 1. 2016, retrieved on June 30, 2022 from https://www.nato.int/cps/su/ natohq/publications.htm