UDC 519.7 *doi: 10.30970/vam.2023.31.00000*

INFORMATION THREAT. COMBATING N-TYPE INFORMATION THREATS

B. Krasiuk

National University "Ostroh Academy",
2, Seminarska str., 35800, Ostroh, Rivne Oblast
e-mail: bohdan.krasiuk@oa.edu.ua

The article underscores the significance of acquiring a profound comprehension of information dissemination processes and implementing effective measures to safeguard information security. Given the increasing impact and proliferation of detrimental information, there is a need to investigate the mechanisms of information warfare and conflicts within contemporary society. Modeling serves as a practical approach to analyze these processes.

The modern information society is experiencing rapid development of technologies and information flows, which opens up new opportunities for disseminating various types of information. The article proposes a software implementation of decision support for the information warfare model of n-type information threats. The relevance of such a method of assessing information warfare is substantiated.

The developed program allows, in addition to performing calculations for n-types of information threats, to dynamically change the input parameters of both the environment and each individual type of information. The model, in combination with the application, allows you to monitor how quickly this or that information spreads, check the reaction of the speed of spread to changes in the parameters of the environment, which in turn will allow you to effectively respond to threats.

Key words: information threat, nonlinear dynamic system, conflict situation.

1. Main part

An information threat is any activity aimed at violating the integrity, confidentiality or availability of information in order to cause harm to a person, organization or state [1].

In the context of information warfare, information threats can be used to discredit opponents, reduce public confidence in certain individuals or organizations, or even interfere with electoral processes [7].

Information threats in information warfare can take different forms, for example, fake news and information: the dissemination of false or speculative information to influence public opinion. Speaking of information threats, it is also worth noting the category of cyber threats. A cyber threat or cybersecurity threat is a malicious act aimed at damaging data, stealing data, or disrupting digital life in general [6]. To combat information threats in the context of information warfare, effective security measures must be developed. Thus, the necessity and relevance of studying the spread and perception of information threats at the present stage of development does not require additional evidence.

For simplicity, let us consider the case when we have a social community of size N_0, which can be influenced by several information flows $(I_1, I_2, \dots, I_n)$ [1]. At the initial time $t_0 = 0$, all information sources start broadcasting their streams to this community, which leads to the spread of information flows among the community.

Given that the information flows are different, this process can be viewed as an information struggle. The goal is to create a mathematical model of this struggle in order to obtain the dynamics of its development over time (dependence on time t of the values $N_1(t), N_2(t), \ldots, N_n(t)$ – the number of "adherents" who received information from sources), as well as to determine the final result – a "winner" or a "loser". The "winner" will be the one who was able to disseminate his information among more community members than his rivals before the full coverage of the community, i.e. the number will be greater than $\frac{N_0}{n}$.

The main assumptions will be [1]:

1. Each stream is distributed to the community through two information channels
   a) One of the sources of information can be considered "external" to the community. The propagation rate I_i, $i = 1, ..., n$ through this channel is characterised by the parameter $\alpha_i > 0$, $i = 1, ..., n$. These parameters are assumed to be time independent;
   b) The second channel can be considered "internal" and is interpersonal communication between members of a social community. Its intensity for I_i, $i = 1, ..., n$ is characterised by the parameters $\beta_i > 0$, $i = 1,...,n$, which do not depend on time, and so on. As a result of this communication, the "adherents" I_i, who have already been recruited by the idea, influence the members who have not yet been recruited (their number is equal to $N_0 - N_1(t) - N_2(t) - ... - N_n(t)$), making their "personal" contribution to the recruitment process.
2. Rate of change in the number of "followers" $N_1(t) + N_2(t) + ... + N_n(t)$ (i.e. the number of those recruited per unit of time $I_1, I_2, ..., I_n$) consists of:
   a) the rate of external recruitment (proportional to the products of the parameters α_1, α_2, ..., α_n by the number of active members $(N_0 - N_1(t) - N_2(t) - ... - N_n(t))$, i.e., the values $\alpha_1(N_0 - N_1(t) - N_2(t) - ... - N_n(t)$, $\alpha_2(N_0 - N_1(t) - N_2(t) - ... - N_n(t), ..., \alpha_n(N_0 - N_1(t) - N_2(t) - ... - N_n(t)$, respectively, for $I_1, I_2, ..., I_n$;
   b) the rate of external recruitment (proportional to the products of the parameters $\beta_1, \beta_2, ..., \beta_n$ by the number of active adherents $N_1(t), N_2(t), ..., N_n(t)$ and the number of not yet recruited $(N_0 - N_1(t) - N_2(t) - ... - N_n(t))$, i.e., $\beta_1 N_1(t)(N_0 - N_1(t) - N_2(t) - ... - N_n(t))$, $\beta_2 N_2(t)(N_0 - N_1(t) - N_2(t) - ... - N_n(t))$, ..., $\beta_n N_n(t)(N_0 - N_1(t) - N_2(t) - ... - N_n(t))$ for $I_1, I_2, ..., I_n$ respectively.

A neutral "average" member of the unrecruited part of the community (who has no relation to $I_1, I_2, ..., I_n$) accepts information faster if the values of $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n$ are larger. Even if a particular I_x has more influence than another I_y (i.e. $\alpha_x > \alpha_y$ and $\beta_x > \beta_y$), some members of the community still accept I_y (i.e. there is no complete monopoly of one type of information over another) [1], [4].

Summing up the assumptions, we get a model:

$$\begin{cases} \frac{dN_1}{dt} = (\alpha_1 + \beta_1 N_1(t))(N_0 - N_1(t) - N_2(t) - ... - N_n(t)), N_1(t_0 = 0) = N_1(0) \geq 0 \\ \frac{dN_2}{dt} = (\alpha_2 + \beta_2 N_2(t))(N_0 - N_1(t) - N_2(t) - ... - N_n(t)), N_2(t_0 = 0) = N_2(0) \geq 0 \\ ... \\ \frac{dN_n}{dt} = (\alpha_n + \beta_n N_n(t))(N_0 - N_1(t) - N_2(t) - ... - N_n(t)), N_n(t_0 = 0) = N_n(0) \geq 0 \end{cases}$$

Given the known parameters $N_0, \alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n$ and the initial values of the number of adherents, all the desired characteristics can be found analytically or numerically.

$$\beta_{i+1}N_{i+1}(t) = C_i(\alpha_i + \beta_i N_i(t)) - \alpha_i + \frac{\beta_{i+1}}{\beta_1}$$

$$C_i = [\alpha_{i+1} + \beta_{i+1}N_i(0)]/[\alpha_i + \beta_i N_i(0)],$$

where $i = 1, 2, ..., N-1$.

1.1. Model problem

The solution of the system, with initial conditions for the constants $N_n(0) = 0$ for the initial values $(n = 4)$ in the two cases, will be as follows:

$$\begin{cases} \frac{dN_1}{dt} = (\alpha_1 + \beta_1 N_1(t))(N_0 - N_1(t) - N_2(t) - N_3(t) - N_4(t)), \\ \frac{dN_2}{dt} = (\alpha_2 + \beta_2 N_2(t))(N_0 - N_1(t) - N_2(t) - N_3(t) - N_4(t)), \\ \frac{dN_3}{dt} = (\alpha_3 + \beta_3 N_3(t))(N_0 - N_1(t) - N_2(t) - N_3(t) - N_4(t)), \\ \frac{dN_4}{dt} = (\alpha_4 + \beta_4 N_4(t))(N_0 - N_1(t) - N_2(t) - N_3(t) - N_4(t)), \end{cases}$$

where $N_1(0) + N_2(0) + N_3(0) + N_4(0) < N_0$.

For the solution and visualisation, we used a discrete-time model with the approaches to construction described in [2], [3], [5], all calculations were performed in the PyCharm programming environment using the Python language.

Consider the first example, for three vectors. The initial conditions were chosen as follows: $N_0 = 30000$, $N_1(0) = 140$, $N_2(0) = 180$, $N_3(0) = 100$, with the following coefficients: $\alpha_1 = 0.000012$, $\alpha_2 = 0.000015$, $\alpha_3 = 0.000018$, $\beta_1 = 0.00000012$, $\beta_2 = 0.00000009$, $\beta_3 = 0.0000001$.

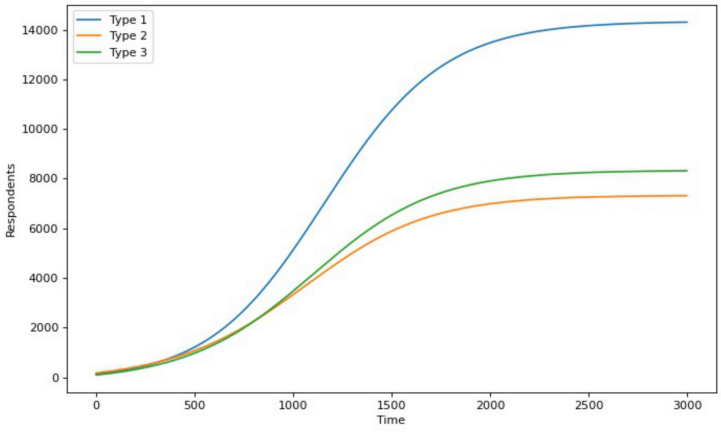

Fig. 1. Example for three vectors and initial conditions

As you can see from the graph, the first type of information threat won the fight.

Consider the following example, for four-vectors and the following initial conditions: $N_0 = 30000$, $N_1(0) = 140$, $N_2(0) = 180$, $N_3(0) = 100$, $N_4(0) = 129$ with the following

coefficients: $\alpha_1 = 0.000012$, $\alpha_2 = 0.000015$, $\alpha_3 = 0.000018$, $\alpha_4 = 0.000015$, $\beta_1 = 0.00000012$, $\beta_2 = 0.00000009$, $\beta_3 = 0.0000001$, $\beta_4 = 0.00000012$.

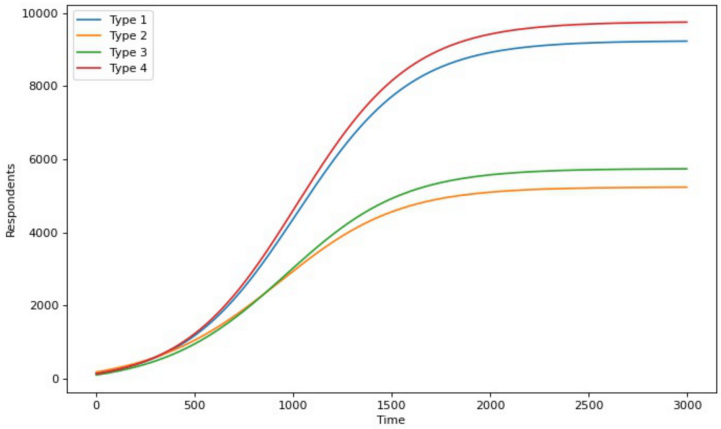

Fig. 2. Example for four-vectors and initial conditions

As can be seen from the graph, despite the initially larger number of supporters of the first type of information threat, it still lost to the second type, because the relevant parameters guaranteed it a faster increase in the number of supporters.

Let's consider a similar example, but for a zero initial number of supporters of each information threat.

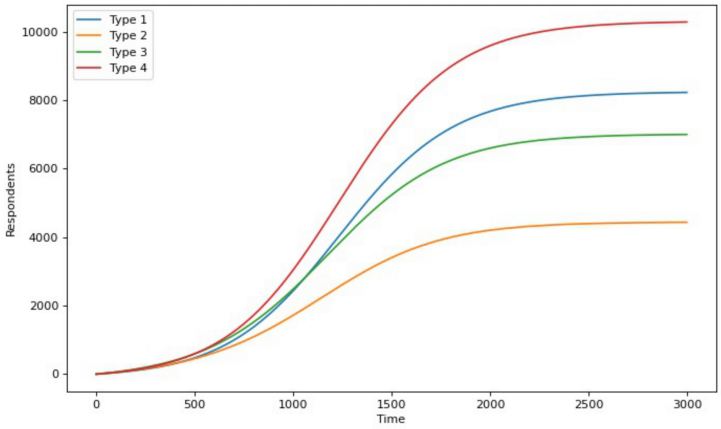

Fig. 3. Example for a zero initial number of supporters of each information threat

As can be seen from the graph, in the case of a zero start, the information threat of the fourth type wins.

2. Conclusion

This article describes the peculiarities of building a model with discrete time and analyses its behaviour in the case of $n = 4$. The main idea of the model is that we can track the speed of information threats and consider this when developing countermeasures. The use of a discrete-time differential model is an important aspect in analysing information threats, as it allows us to consider the real nature of the spread of these threats.

One of the main advantages of the proposed model is the ability to conduct a more accurate and detailed analysis of the spread of information threats. This makes it possible to determine the pace of their spread and ensure an effective response to them. The model can also be helpful in analysing changes in the spread of threats over time, which allows for identifying trends and predicting future directions of development of countering information threats.

To test the effectiveness of the proposed model, experiments were conducted based on data related to the spread of a specific information threat. A software solution was developed that allowed to dynamically change the input parameters of the model and each of the information threats.

For further development of this model, it is possible to consider considering a wider range of parameters and using more complex data analysis algorithms.

References

1. Mykhaylov A.P. Models of the information struggle / A.P. Mykhaylov, N.A. Marevtseva // Mat. modeling. – 2011. – Vol. 23, No. 10. – P. 19–32.
2. Albeverio S. The conflict interaction between two complex systems. Cyclic migration / S. Albeverio, V. Koshmanenko, I. Samoilenko
3. Albeverio S. Dynamics of discrete conflict interac-tions between non-annihilating opponents / S. Albeverio, M. Bodnarchuk, V. Koshmanenko
4. Samoilenko I.V. Peculiarities of Construction and Analysis of the Information Warfare Model with Markov Switchings and Impulse Per-turbations Under Levy Approximation Conditions / I.V. Samoilenko, A.V. Nikitin, G.V. Verovkina // Cybern Syst Anal. – 2021. – Vol. 57. – P. 621–628. – doi: 10.1007/s10559-021-00387-1.
5. Bekesiene S. The Complex Systems for Conflict Interaction Modelling to Describe a Non-Trivial Epidemiological Situation / S. Bekesiene, I. Samoilenko, A. Nikitin, I. Meidute-Kavaliauskiene // Mathematics. – 2022. – Vol. 10. – 537 p. – doi: 10.3390/math10040537.
6. Gavenaite-Sirvydiene J. Algita Miecinskiene / J. Gavenaite-Sirvydiene // River Publishers. Journal of Cyber Security and Mobility. – 2023. – Vol. 12.
7. Paduraru M. Sociology Of Security As An Opportunity For Social Security / M. Paduraru / 35th IBIMA Conference, Seville, Spain.

Article: received 17.05.2023
revised 21.06.2023
printing adoption 05.07.2023

ІНФОРМАЦІЙНА ЗАГРОЗА. БОРОТЬБА N-ТИПІВ ІНФОРМАЦІЙНИХ ЗАГРОЗ

Б. Красюк

Національний університет "Острозька академія",
вул. Семінарська 2, Острог, Рівненська область
e-mail: bohdan.krasiuk@oa.edu.ua

Запропоновано програмну реалізацію підтримки прийняття рішень для моделі інформаційної боротьби n-типів інформаційних загроз. Обґрунтувано доречності подібного способу оцінки інформаційної боротьби.

Розроблена програма дає змогу крім того, що проводити обчислення для n-типів інформаційних загроз, також динамічно змінювати вхідні параметри середовища та кожного, окремо взятого типу інформації. Модель в комбінації із застосунком допомагає моніторити як швидко розповсюджується та чи інша інформація, перевіряти реакцію швидкості розповсюдження на зміну параметрів середовища, що також дасть змогу ефективно відповісти загрозам.

Ключові слова: інформаційна загроза, нелінійна динамічна система, конфліктна ситуація.