ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / **https://doi.org/10.47459/cndcgs.2026.66**

Analysis of the Complex System for Information Conflict Interaction Modelling

Igor Samoilenko[1], Anatolii Nikitin[2,3*], Bohdan Krasiuk[2], Andrii Prus[2]

[1]*Taras Shevchenko National University of Kyiv, Kyiv, Ukraine*
[2]*National University of Ostroh Academy, Ostroh, Ukraine*
[3]*Jan Kochanowski University of Kielce, Kielce, Poland*

Correspondence: * anatolii.nikitin@oa.edu.ua

Abstract
The expanding significance of the information domain in today's "information society" highlights the necessity of efficient information security and governance. The distribution of dangerous information has become more accessible due to the quick development of information dissemination technologies; therefore, a thorough understanding of information dissemination mechanisms is necessary to create effective countermeasures. An established and successful method for resolving these problems is modelling. This study aims to explore the information warfare paradigm further and how it relates to the idea of conflict, a topic covered in several related publications. The ultimate goal of this article is to develop a comprehensive system that uses software tools to assess the dynamics of internal conflict using the information warfare paradigm.

KEY WORDS: *information warfare model, conflict interaction, decision support system*

Citation: Samoilenko, I.; Nikitin, A.; Krasiuk, B., Prus A. *Analysis of the Complex System for Information Conflict Interaction Modelling*. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 07-10 September 2026. ISSN 2538-8959, https://doi.org/10.47459/cndcgs.2026.66

1. Introduction

Given the growing impact and dissemination of negative information, studying the mechanisms of conflict and information warfare in contemporary society is crucial [1-3]. One helpful approach to researching these processes is modelling. The paper highlights how vital it is to have a thorough grasp of the information dissemination processes and to implement practical safeguards for information security.

The fixed qualities (intensity) of information influence and the classical model's incapacity to account for abrupt and unexpected occurrences that impact information consumers' thoughts are the primary drawbacks of the model [4]. Of course, in the modern world, where information is rapidly shared and simultaneously reaches a vast audience, it is necessary to consider such uncommon but potent variables. We propose a model in the form of a dynamic system that accounts for the occasional random spikes that temporarily but considerably alter the number of "adherents" of the critical concepts and the random influence of the environment on the intensity of information broadcast.

In addition, it was decided to create a software implementation for the process described above to simplify the decision-making process and visualise the results obtained. Python was chosen as the programming language, and the Matplotlib package was used to visualise the calculations. It was also decided to refrain from using ready-made solutions for basic calculations to ensure complete control over constructing a numerical solution.

2. Information warfare model

Let's examine the information warfare model in more detail. The Lotka-Volterra equations characterize the model in the "classical" version [13]:

$$\begin{cases} \frac{dN_1}{dt} = (\alpha_1 + \beta_1 N_1(t))(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t)) \\ \frac{dN_2}{dt} = (\alpha_2 + \beta_2 N_2(t))(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t)) \\ \vdots \\ \frac{dN_n}{dt} = (\alpha_n + \beta_n N_n(t))(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t)) \end{cases} \quad (1)$$

where: $N_1(t_0 = 0) = N_1(0) \geq 0$, $N_2(t_0 = 0) = N_2(0) \geq 0$, $N_n(t_0 = 0) = N_n(0) \geq 0$

Let us consider the main assumptions of the model (1). Each of the information flows, $I_1, I_2, \dots, I_n$, is distributed in the community through two different information channels:

1. The first channel, which is considered to be "external" to the community, is characterised by the propagation rate parameters $\alpha_1 > 0, \alpha_2 > 0, \dots, \alpha_n > 0$. These parameters are assumed to be time-independent.
2. The second channel, "internal", is interpersonal communication between members of a social community. The intensity of this channel is described by the parameters $\beta_1 > 0, \beta_2 > 0, \dots, \beta_n > 0$, which are also independent of time. Within this channel, individuals who have already perceived information source "1" $(N_1(t))$ contribute to the recruitment of those who have not yet been exposed to any source $(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t))$

The rate of change in the number of followers, $N_1(t) + N_2(t) + \cdots + N_n(t)$, which represents the number of people recruited by information flows $I_1, I_2, \dots, I_n$ per unit of time, is a combination:

1. external recruitment coefficients, which are proportional to the product of the parameters $\alpha_1, \alpha_2, \dots, \alpha_n$ by the number of active members $(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t))$, i.e. $\alpha_1(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t))$, $\alpha_2(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t))$, ..., $\alpha_n(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t))$ for $I_1, I_2, \dots, I_n$, respectively.
2. Internal recruitment rates, which are proportional to the products of the parameters $\beta_1, \beta_2, \dots, \beta_n$ multiplied by the number of active followers $N_1(t), N_2(t), \dots, N_n(t)$ and the number of unrecruited individuals $(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t))$, i.e., $\beta_1 N_1(t)(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t))$, $\beta_2 N_2(t)(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t))$, ..., $\beta_n N_n(t)(N_0 - N_1(t) - N_2(t) - \cdots - N_n(t))$ for $I_1, I_2, \dots, I_n$, respectively.

In addition, the number of uninvolved community members, N_0, should be taken into account, minus those who have received both types of information (i.e. the sum of $N_1(t) + N_2(t) + \cdots + N_n(t)$). It should be noted that the parameters $\alpha_1, \alpha_2, \dots, \alpha_n$, $\beta_1, \beta_2, \dots, \beta_n$ determine not only the intensity of information influence, but also the propensity of individuals to simultaneously perceive information. Larger values of these parameters indicate faster perception of information by a hypothetical "average" community representative who initially takes a neutral position in relation to $I_1, I_2, \dots, I_n$. In addition, even if the influence of I_1 is stronger than that of I_2 (i.e. $\alpha_1 > \alpha_2$, $\beta_1 > \beta_2$), some community members may still perceive I_2, which indicates that one type of information does not have a complete monopoly over the other.

It is worth noting that the previously mentioned model has been updated to include costings that consider the variability of the environment, as explained in the papers [10,16,19].

The conflict under consideration involves a set of p different types of information, denoted as $I_1, I_2, \dots, I_n$, in the context of a certain community. In order to integrate this conflict into a practical model, we position this community within a certain territory and further divide it into regions. Within this community, individuals can be classified as supporters of $I_1, I_2, \dots, I_n$, or as neutral actors.

Furthermore, we define a conflict as a physical system in which substances $A_1, A_2, \dots, A_n$ compete for control over a common field of interest denoted as Ω. This field Ω is divided into separate regions, represented as Ω_i, and each substance A_i seeks to dominate these regions. The presence of each substance in these regions is quantified through non-negative coordinate vectors, given by $A_i = (A_{i1}, A_{i2}, \dots, A_{im})$, which reflect their influence in these regions. The development of the conflict and its impact on the substance A_i is a discrete dynamic process (2):

$$\{A_1^N, \dots, A_n^N\} \xrightarrow{*} \{A_1^{N+1}, \dots, A_n^{N+1}\}, \quad N = 0,1, \dots, T \quad (2)$$

where N is the number of discrete time steps.

The map $*$ symbolises an unknown law of conflict interaction between substances A_i. We aim to depict a model of internal conflict information struggle similar to the cyclic Lotka-Volterra migration [4]. To represent migration, our law of interaction, we adopt a discrete-time conflict model involving indestructible rivals [5], which is consistent with the assumptions of our struggle model.

The model is based on the concept of discrete conflict between indestructible systems [12,13]. The law of conflict interaction has an alternative nature of presence in disputed positions: only one of the systems can be present in each position at any given time with some probability [14].

Let us clearly explain this law. The alternative systems (adversaries), indicated by A and B, each claim a finite set of positions, which we can write as $\Omega = \{\omega_1, \dots, \omega_N\}, N \geq 2$. First, let $P_A(\Omega) = P_B(\Omega) = 1$. An arbitrary distribution of the likelihood of having systems A and B in distinct places determines the conflict's beginning state: $P_B(\Omega_i) = r_i \geq 0, i = 1, \dots, N$, and $P_A(\omega_i) = p_i \geq 0$. $\sum_{i=1}^{N} p_i = 1 = \sum_{i=1}^{N} r_i$ in this instance. The inability of adversaries A and B to both occupy an arbitrarily disputed position at the same time is the fundamental component of the interaction of an alternative conflict. The systems thus engage in a kind of battle that causes the starting probabilities $p_i^{(0)} := p_i, r_i^{(0)} := r_i$ for each of the places ω_i to redistribute. The law of redistribution is generally unknown. In the initial step, we suggest using the following formulas (3) to ascertain the composition of the alternative conflict [6,7]:

$$p_i^{(1)} = \frac{p_i^{(0)}(1 - \alpha r_i^{(0)})}{1 - \alpha \sum_{i=1}^{N} p_i^{(0)} r_i^{(0)}}, \quad r_i^{(1)} = \frac{r_i^{(0)}(1 - \alpha p_i^{(0)})}{1 - \alpha \sum_{i=1}^{N} p_i^{(0)} r_i^{(0)}} \qquad (3)$$

where coefficient $\alpha \neq 0, -1 \leq \alpha \leq 1$ determines intensity of interaction. It is clear that this conflict's composition is non-commutative. The composition is expressed in terms of stochastic vectors $\mathbf{p}^0 = (p_1^{(0)}, \dots, p_N^{(0)}), \mathbf{r}^0 = (r_1^{(0)}, \dots, r_N^{(0)})$, or vectors with unit l_1 norm, as follows:

$$\mathbf{p}^1 = \mathbf{p}^0 * \mathbf{r}^0, \quad \mathbf{r}^1 = \mathbf{r}^0 * \mathbf{p}^0$$

where the coordinates of the new stochastic vectors, $\mathbf{p}^1, \mathbf{r}^1$, are provided in (3). Likewise, the subsequent phases of the dispute:

$$\mathbf{p}^n = \mathbf{p}^{n-1} * \mathbf{r}^{n-1} \equiv \mathbf{p}^0 *^n \mathbf{r}^0, \quad \mathbf{r}^n = \mathbf{r}^{n-1} * \mathbf{p}^{n-1} \equiv \mathbf{r}^0 *^n \mathbf{p}^0$$

with coordinates:

$$p_i^{(n)} = \frac{p_i^{(n-1)}(1 - \alpha r_i^{(n-1)})}{z_n}, \quad r_i^{(n)} = \frac{r_i^{(n-1)}(1 - \alpha p_i^{(n-1)})}{z_n}$$

where the principle of indestructibility is guaranteed by the normalizing factor $z_n = 1 - \alpha(\mathbf{p}^{n-1}, \mathbf{r}^{n-1})$ ((.,.) indicate a scalar product in $\mathbf{R}^N$): $||\mathbf{p}^n||_{l_1} = ||\mathbf{r}^n||_{l_1} = 1$ [8].

3. **Modeling and Software Implementation**

The information warfare model, as we have formulated it, is as follows: it provides a broad framework for analyzing many facets of information warfare, encompassing a variety of variables and dynamics. The model offers a much more detailed description of the information warfare process by looking at general trends, conflict, and conflict interaction [17-19].

A greater comprehension of the underlying mechanisms and potential mitigation methods is made possible by the model's structured approach to examining the intricacies present in information warfare scenarios [11].

Python 3.11 was chosen as the programming language for the software implementation because of its adaptability and capacity to utilize pre-made solution packages for simple tasks. A portion of the visualization was produced with the help of the Matplotlib 3.6.2 library package, which is renowned for producing graphical representations that are easy to read and comprehend.

By not using commercially available calculation tools, we were able to achieve precise numerical solutions that were customized to meet our unique needs with more flexibility. Python offers numerous libraries that expedite the coding process for tasks like generating number series according to the normal distribution law or processing operations with arrays and tabular data, which was done with the numpy 1.26.3 package. This is despite using something other than pre-made solutions for basic calculations.

Not only does using these libraries expedite development, but it also guarantees the dependability and effectiveness of our implementation. The development environment used is JetBrains PyCharm Community Edition 2023.3, which has shown to be a dependable and quick tool for creating Python software applications.

First, let's look at a simple case for combating three information threats without conflict interaction. The model is defined by the following parameters:
$N = 8000$, $N_0 = 60000$, $N_1(0) = 0$, $N_2(0) = 0$, $N_3(0) = 0$, $\alpha_1 = 0.000012$, $\alpha_2 = 0.000014$, $\alpha_3 = 0.000011$, $\beta_1 = 0.00000001$, $\beta_2 = 0.00000002$, $\beta_3 = 0.000000009$

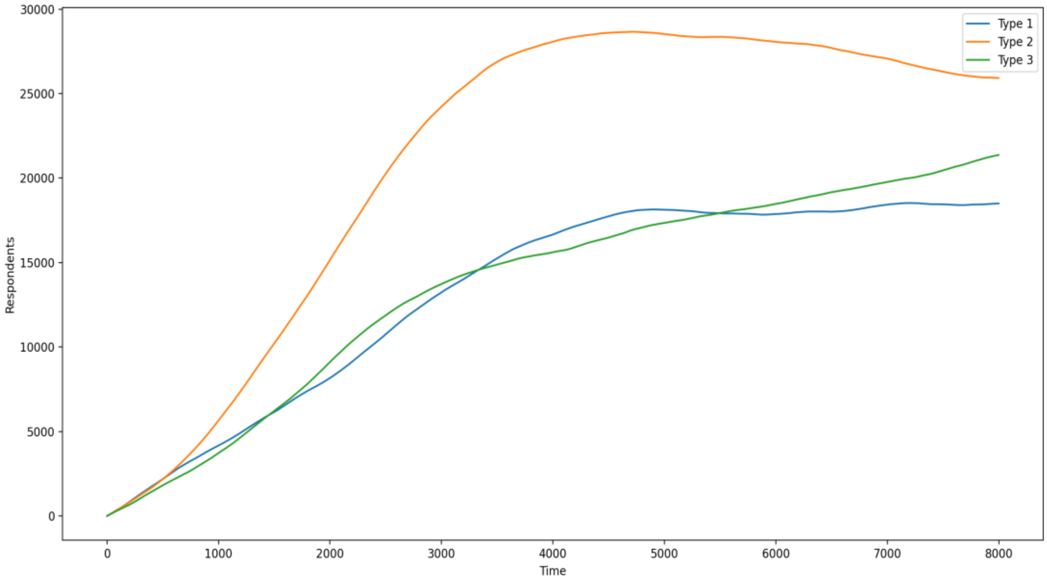

Fig. 1 Combating three types of information threats without conflict

As we can see from the graph “Fig. 1”, the second type of information threat was expected to win, as the values of the coefficients of information threat through internal and external channels are higher than those of other information threats.

Now, let’s consider a similar situation with the addition of a conflict interaction between the first and second information threats. Let’s start with a small value of the interaction intensity coefficient $\alpha_{(1)(2)} = -0.9$.

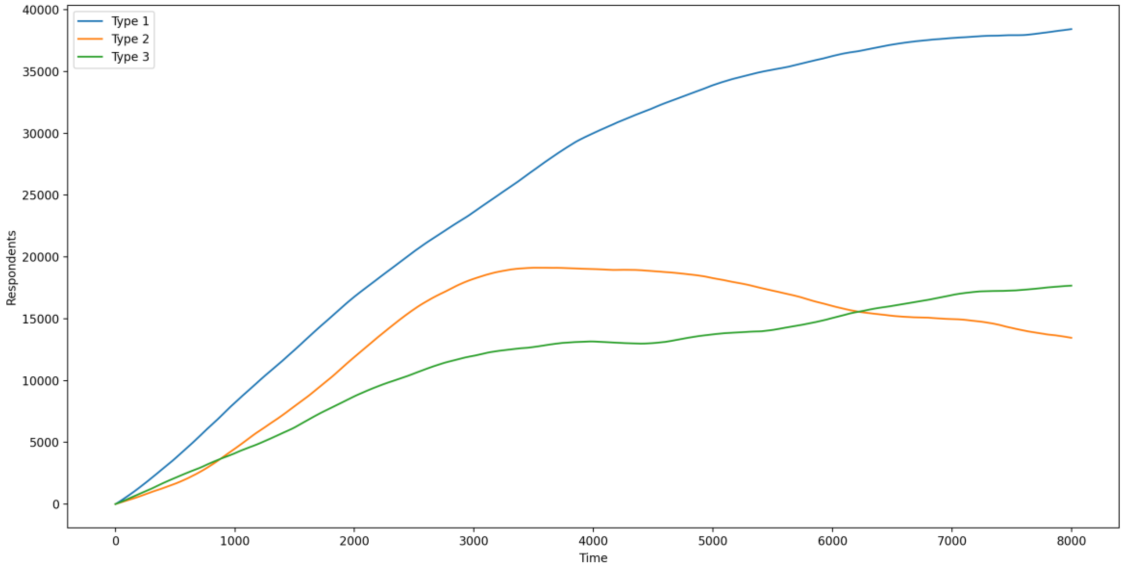

Fig. 2 Combating three types of information threats with conflict interaction

As we can see “Fig. 2”, the main statement is confirmed: conflict interaction leads to the fact that the adherents of the second information threat are moving to the first.

As a result, despite the higher values of the coefficients of information dissemination through internal and external channels, the first type of information threat was the winner.

Of course, if the strength of the conflict interaction is increased $\alpha_{(1)(2)} = -0.7$, the results will be even more pronounced “Fig. 3”.

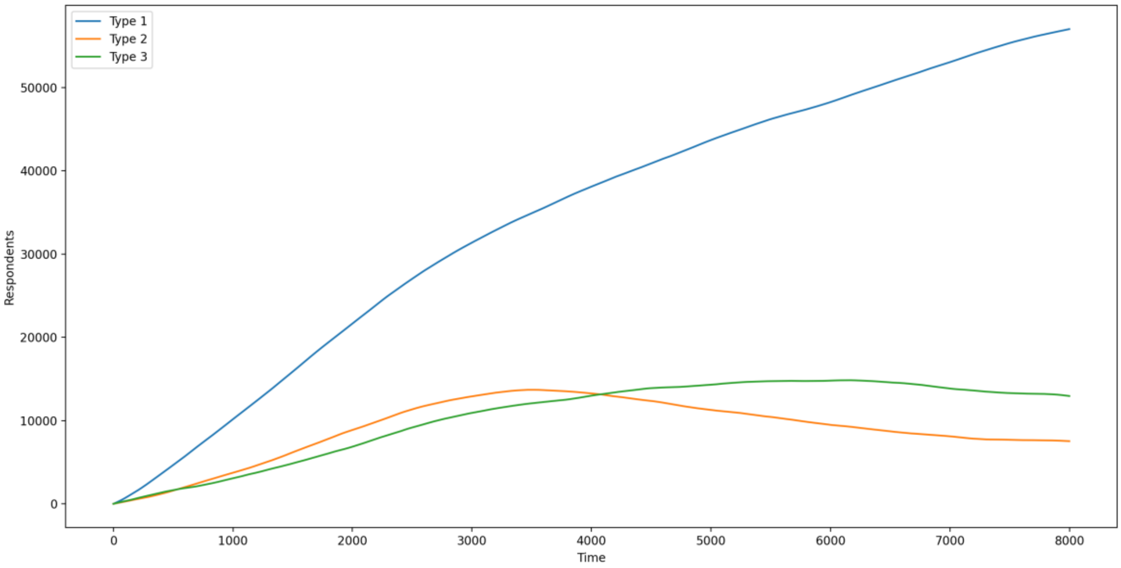

Fig. 3 Combating three types of information threats with higher intensity of conflict interaction

Let's also turn the conflict interaction in favour of the second information threat $\alpha_{(1)(2)} = 0.1$ to verify the calculations' correctness. That is, we will further strengthen the type of information threat that is already stronger than others, taking into account the coefficients of information dissemination through internal and external information channels.

As we can see from the chart "Fig. 4", as the adherents of one type of information threat are reinforced, they flow into the other. The second type of information has become the undisputed winner.

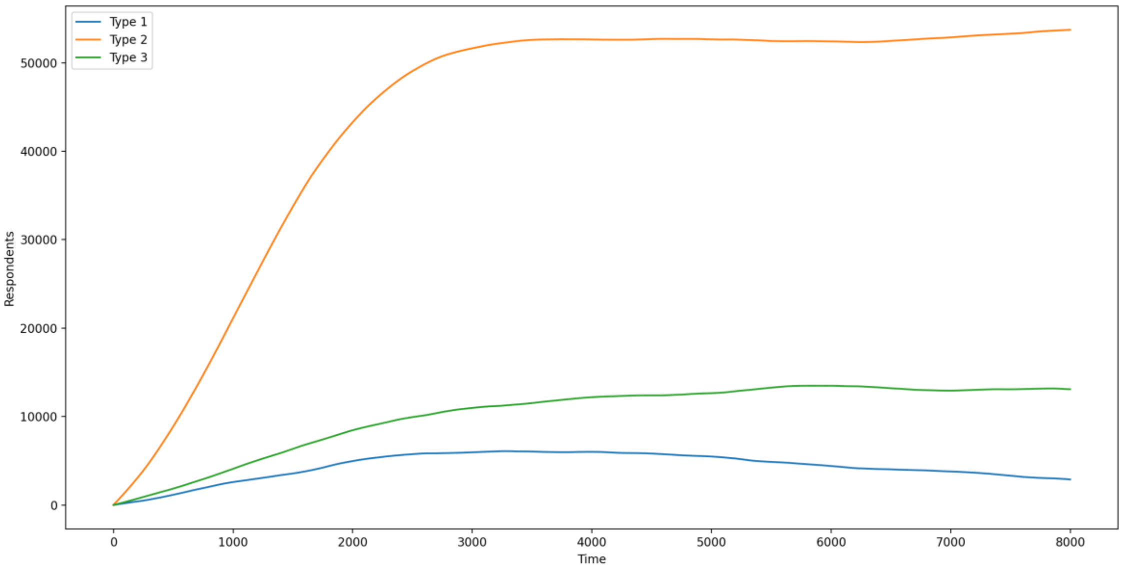

Fig. 4 Combating the three information threats with conflictual interaction in favour of the second information threat

As noted earlier, the developed software solution allows for simultaneous calculations for n-information threats. This also applies to the calculation of conflict interaction. This means that we can pairwise set the intensity of conflict interaction for several information threats participating in the fight at the same time.

Let's look at the case where conflict interaction is considered for five information threats. To begin with, let's see what the situation looks like without conflict interaction. The model parameters are as follows:
$N = 8000$, $N_0 = 60000$, $N_1(0) = 0$, $N_2(0) = 0$, $N_3(0) = 0$, $N_4(0) = 0$, $N_5(0) = 0$, $\alpha_1 = 0.000012$, $\alpha_2 = 0.000014$, $\alpha_3 = 0.000011$, $\alpha_4 = 0.000012$, $\alpha_5 = 0.000014$, $\beta_1 = 0.00000001$, $\beta_2 = 0.00000002$, $\beta_3 = 0.000000009$, $\beta_4 = 0.00000001$, $\beta_5 = 0.00000002$

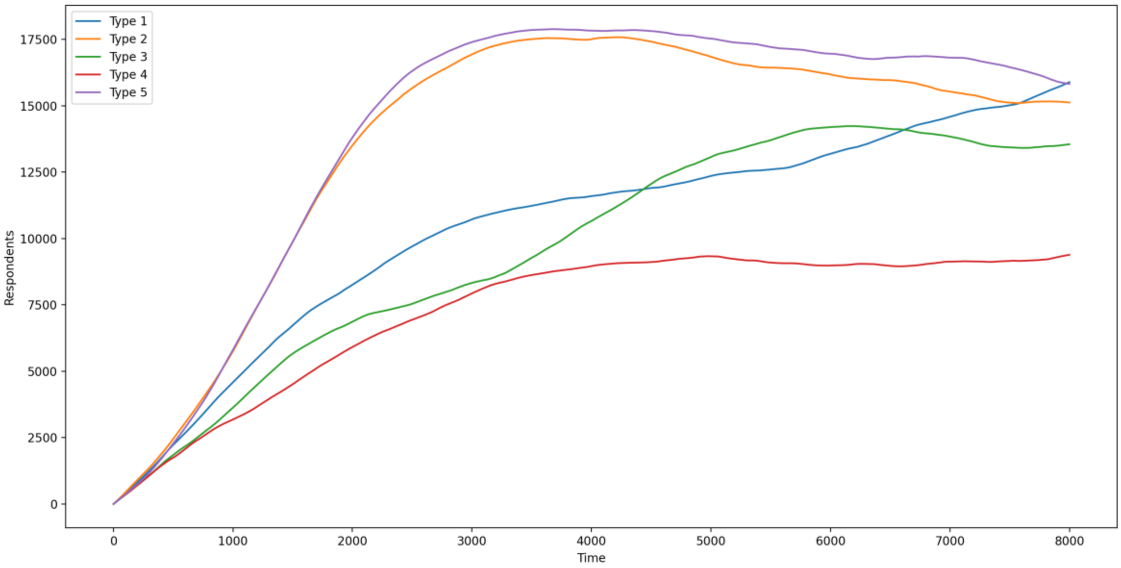

Fig. 5 Combating the five information threats without conflict interaction

As we can see from the graph "Fig. 5", the winning positions share the second and fifth types of information threat.

The next step is to add a conflict interaction between the fifth type of information threat ($\alpha_{(5)(1)} = -0.95$) and the first, in favor of the fifth.As we can see from the graph "Fig. 6", the situation has changed significantly. The fifth type of information threat is now the winner. From this, it follows that sometimes, by ensuring the flow of adepts from one thought to another, it is possible to influence the general outcome, ensuring its leadership.

Therefore, it is essential to keep track of the latest trends in information security and take proactive measures to prevent potential risks and protect sensitive information from falling into the wrong hands.

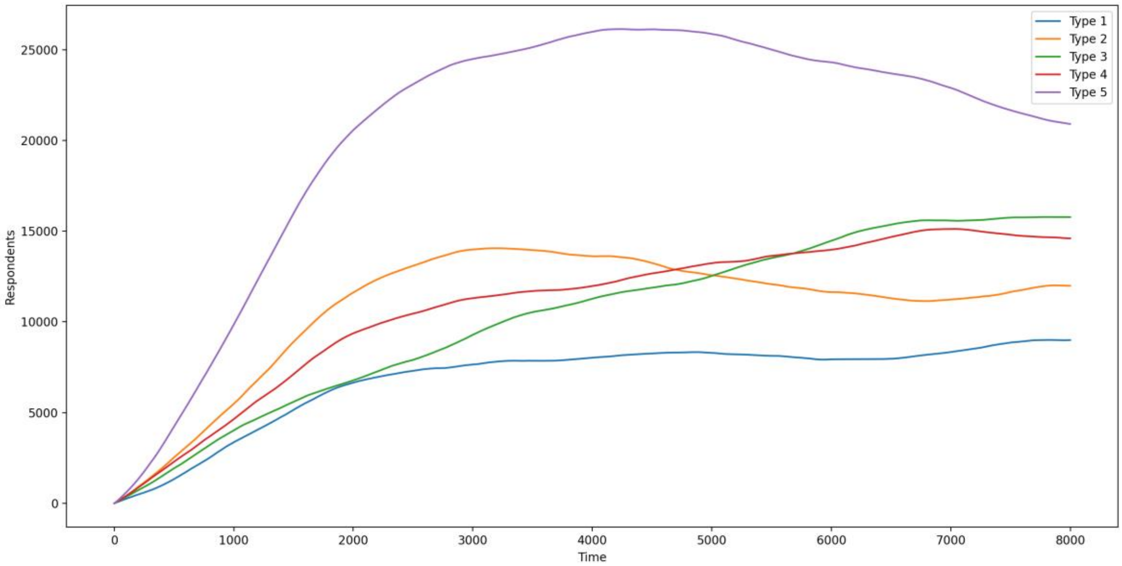

Fig. 6 Combating the five information threats with conflict interaction between the fifth and first information types in favor of the fifth

Finally, let's see an example where we have multiple conflict interactions at the time. We keep the previous conflict relation for the fifth and first information threats and add an extra one a bit stronger for the second and fourth in favor of second ($\alpha_{(2)(4)} = -0.9$).

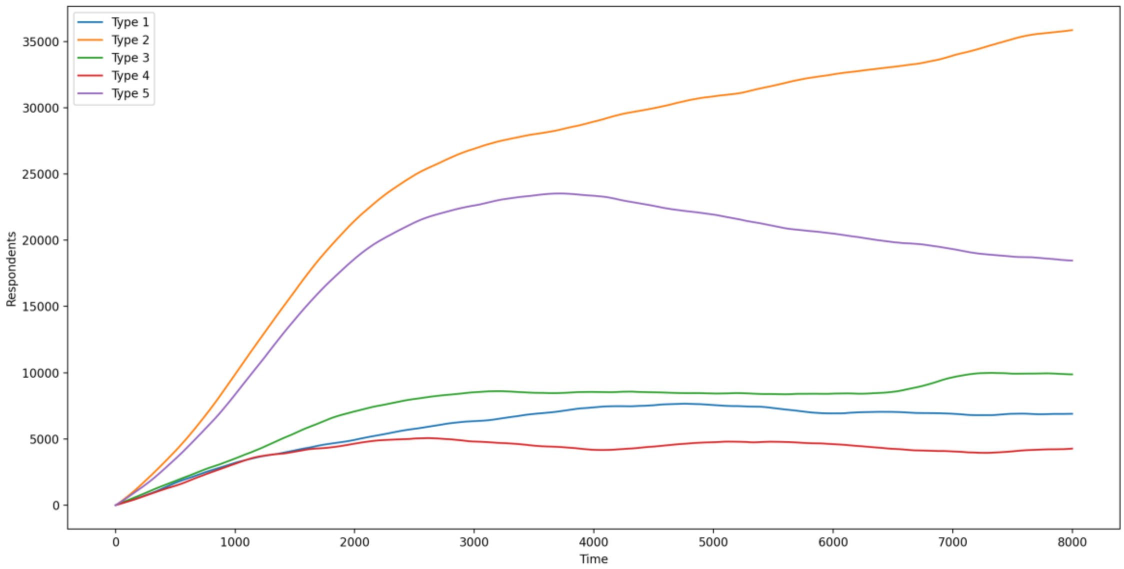

Fig. 7 Combating the five information threats with conflict interaction between the fifth and first, fourth and second information types in favor of the fifth

Based on the data depicted in the graph "Fig. 7", it can be inferred that the reinforcement measures implemented were effective in ensuring the success of information threat two in the information struggle. The graph demonstrates a clear trend showcasing the increased dominance of information threat two over time, which can be attributed to the reinforcement efforts that were put in place. These efforts may have included enhanced cybersecurity protocols, improved data protection measures, and more robust threat monitoring systems. Overall, the graph serves as evidence of the effectiveness of the reinforcement measures and their impact on the outcome of the information struggle.

4. Conclusions

This study provides a thorough examination of the challenges involved in creating a model that addresses n different kinds of information threats while accounting for conflict interaction. Estimating the rate of information threat spread and incorporating it into the creation of countermeasures is the major objective.

The suggested model, which considers the conflict interplay between information threats, has observable advantages over traditional methods. It gives decision-makers the data they need to create more potent reaction plans by accurately measuring the pace of spread. Furthermore, identifying trends and projecting future dangers are made easier by the model's capacity to analyze temporal variations in the dissemination of information threats.

The developed software solution allows to check the behaviour of information threats in various scenarios. Adherence to current trends in software development guarantees further extensibility, security and stability of the solution.

Thus, the developed model represents a significant step forward in understanding and mitigating information threats. Its ability to take into account conflict interactions and accurately analyse the dynamics of information spread positions it as a valuable tool for policymakers and security professionals to develop proactive and effective response strategies. Importantly, ongoing research and experimentation will continue to refine and test the model's effectiveness in different contexts and scenarios, ensuring its relevance and applicability in the ever-evolving landscape of information threats.

Acknowledgements. Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

References

1. Bekesiene, S., Samoilenko, I., Nikitin, A., & Meidute-Kavaliauskiene, I. (2022). The complex systems for conflict interaction modelling to describe a non-trivial epidemiological situation. Mathematics, 10(4), 537.
2. Nikitin, A., Bekešienė, S., Hošková-Mayerová, Š., & Krasiuk, B. (2024). Multidimensional Model of Information Struggle with Impulse Perturbation in Terms of Levy Approximation. Mathematics, 12(8), 1263.
3. Samoilenko, I., Nikitin, A., Salo, N., Samoilenko, T., Verovkina, G., & Krasiuk, B. (2024). Information Warfare Model with Internal Conflict. Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 11-13.
4. Brass F.M. A New Product Growth for Model Consumer Durables. *Management Science*, 1969, 15 (5), p. 215–227.
5. Albeverio, S.; Koshmanenko, V.; Samoilenko, I. The conflict interaction between two complex systems. Cyclic migration. *J. Interdiscip. Math.* 2008, 11(2), 163–185.

6. Albeverio, S.; Bodnarchyk, M.; Koshmanenko, V. Dynamics of discrete conflict interactions between non-annihilating opponents. *Methods Funct. Anal. Topol.* 2005, 11(4), 309–319.
7. Bodnarchuk, M.V.; Koshmanenko, V.D.; Samoilenko, I.V. Dynamics of conflict interactions between systems with internal structure. *Nonlinear Oscillations* 2007, 9(4), 423–437.
8. Koshmanenko, V. The theorem of conflict for probability measures. *Math. Meth. Oper. Res.* 2004, 59(2), 303–313.
9. Nikitin, A.; Krasiuk, B. Construction features, asymptotic analysis and computer implementation for a multidimensional model of information warfare under Poisson approximation. *Int. Sci. Tech. J. "Problems of Control and Informatics"* 2024, 69(1), 24–33.
10. Korolyuk, V.S.; Limnios, N. Stochastic Systems in Merging Phase Space. World Scientific, 2005, pp. 330.
11. Korolyuk, V.S.; Limnios, N.; Samoilenko, I.V. Levy and Poisson approximations of switched stochastic systems by a semi-martingale approach. *Comptes Rendus Mathematique* 2016, 354, 723–728.
12. Jacod, J.; Shiryaev, A.N. Limit theorems for stochastic processes. Springer-Verlag, Berlin, 2003.
13. Korolyuk, V.S.; Korolyuk, V.V. Stochastic Models of Systems. Kluwer, Dordrecht, 1999.
14. Anisimov, V.V. Switching processes in queuing models. Wiley-ISTE, London, 2008.
15. Chabanyuk, Y.; Nikitin, A.; Khimka, U. Asymptotic Analyses for Complex Evolutionary Systems with Markov and Semi-Markov Switching Using Approximation Schemes. Wiley-ISTE, November 2020, 240 pages.
16. Lotka, A.J. Relation between birth rates and death rates. *Science* 1907, 26(653), 21–22.
17. Takahashi, K.I.; Salam, K.Md.M. Mathematical model of conflict with non-annihilating multi-opponent. *J. Interdisciplinary Math.* 2001, 9, 459–473.
18. Tufto, J. Effects of releasing maladapted individuals: a demographic evolutionary model. *The American Naturalist* 2001, 158(4), 331–340.
19. Samoilenko, I.V.; Nikitin, A.V.; Verovkina, G.V. Peculiarities of Construction and Analysis of the Information Warfare Model with Markov Switchings and Impulse Perturbations Under Levy Approximation Conditions. *Cybernetics and Systems Analysis* 2021, 57(4), 621–628.