UDC 004.942, 519.876.5

Information network topology: mathematical model of suggestive influence

Yuliia Nakonechna[1], Bohdan Savchuk and Anna Kovalova

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine*

Abstract

Psychological operations (PsyOps) have become an increasingly important aspect of modern warfare and political maneuvering, shaping target populations' perceptions, emotions, and behaviors. Understanding the mechanisms by which these operations function and impact target populations is crucial for developing effective countermeasures. This paper proposes a model for the spread of such content based on epidemiological and pharmacokinetic approaches. By drawing analogies between the spread of PsyOps and the diffusion of pathogens or chemicals, we develop mathematical models to describe the dynamics of PsyOps dissemination. The model considers factors such as initial conditions, strength and persistence of a PsyOp, susceptibility, and interconnectedness of the target population. Solutions to the proposed equations are provided, offering insights into the potential spread and control of PsyOps.

Keywords: Cybersecurity, psychological operations, agent-based modeling, information diffusion.

Introduction

Psychological operations (PsyOps) have become an increasingly important aspect of modern warfare and political maneuvering, their success shaping target populations' perceptions, emotions, and behaviors. Understanding the mechanisms by which these operations function and their impact on target populations is crucial for developing effective countermeasures and mitigating their harmful effects. This paper proposes a model for the spread of such charged content based on the analogy with chronic inflammation spreading in homogeneous mediums. The premise of this model is that psychological operations can be boiled down to the propagation of information or ideas within a population, similar to how diseases can spread through a connected, homogeneous system [1]. Drawing from existing research on information spread and epidemic models, this paper develops a framework for analyzing psychological operation dynamics.

The model considers factors such as initial conditions, strength and persistence of a psychological operation, and the susceptibility and interconnectedness of the target population.

Related works

The application of epidemiological models to cybersecurity and information dissemination has gained significant attention in recent years. Researchers have identified parallels between the spread of diseases and the propagation of cyber threats, disinformation, and malware. [2] employed an epidemiological approach for forecasting and managing information incidents, demonstrating the feasibility of using traditional epidemic models to predict the spread of information security incidents. [3] combined epidemic models with deep learning to study cyber attacks, highlighting the potential of integrating mathematical modeling with machine learning methods to enhance cyber defense strategies. [4] applied epidemiological principles to categorize risk factors in the Domain Name System (DNS), providing valuable insights into managing and mitigating risks associated with critical components of internet infrastructure. [5] modeled cyber vulnerabilities using epidemic models, adapting traditional SIR (Susceptible-Infected-Recovered) models to capture the dynamics of cyber vulnerabilities and their potential spread within networks. [6] focused on modeling self-propagating malware using epidemiological models, contributing to the development of strategies for containing and eliminating malware threats. Furthermore, [7] used epidemioilogical approach to create forecasting models for security threats. These studies demonstrate the effectiveness of epidemiological models in understanding and predicting the spread of cyber threats and information. They lay the foundation for applying similar approaches to modeling the dissemination of psychological operations (PsyOps). Our work builds upon these studies, extending methodologies to account for the unique dynamics of PsyOps by considering human behavior, information networks, and countermeasures.

1. PsyOps as a suggestive influence method

PsyOps have a long history as components of military and political strategies to influence the attitudes and behaviors of target populations by manipulating information, emotions, and perceptions [8,9] Psychological operations employ a set of coordinated and interrelated methods and techniques of psychological influence. They use political, military, economic, diplomatic, informative, and psychological means to influence specific individuals or groups, instilling them with different ideological and social attitudes, creating false stereotypes, and changing their moods, feelings, and will in the desired direction. It's important to acknowledge the significant contributions of domestic researchers in the field of information operations. Notably, scholars such as V.P. Horbulin, A.B. Kachynskyi, O.H. Dodonov, D.V. Lande have made substantial advancements in understanding the dynamics and implications of psychological operations in contemporary contexts. [10, 11, 12, 13, 14].

In the field of PsyOps research, there isn't a consensus regarding key definitions and relevant terminology. Previously, actions aimed at changing mass or individual consciousness were called "psychological operations" in the English language literature, but in 2010 they were renamed "Military Information Support Operations" (MISO). Ukrainian theorists and representatives of special services use the term "special information operations" (SIO), while representatives of military sciences prefer the terms "information-psychological operations" (IPO) or "psychological operations" (PsO). This complicates mutual understanding between specialists in different fields. In this paper, the term "psychological operations" is used [15]. In addition to directly influencing the target audience, PsyOps can also generate secondary effects by shaping the broader informational landscape. By influencing key opinion leaders, media outlets, and social influencers, PsyOps can amplify their impact and create a cascading effect that extends beyond the immediate target population. Effective PsyOps require careful planning and execution, including identifying the target audience's psychological vulnerabilities, crafting compelling narratives, and selecting appropriate dissemination channels. Continuous monitoring and adaptation are also essential to ensure the operations remain effective in the face of changing circumstances and potential countermeasures [16]. Typically, the execution of a psychological operation involves a flexible multistage process that can be adapted to suit a particular task and amount of resources:

1. Planning: this stage involves initial reconnaissance, setting up goals and determining a resource pool for the operation. A key task in this stage is determining a target audience and establishing a "fifth column" that can be relied upon during the infiltration.

2. A newsworthy event: in this stage an event that is to be used as a backbone for the campaign is selected or crafted. Negative events are often used as they leave a more lasting impression.

3. Event propagation: the heart of the operation. It involves using the newsworthy event to fulfill the goals of the campaign.

Finalization: either after achieving the goals or aborting the mission the campaign comes to an end. Failure to do so may alert the target population to the nature of the campaign and would be, by definition, a failure D:\Journal\ARTICLES\№_007\Вхідні рукописи\011_Nakonechna_Kovalyova\goal-int.org\informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki\[11, 15].

A generic PsyOps structure can be viewed on Figure 1:

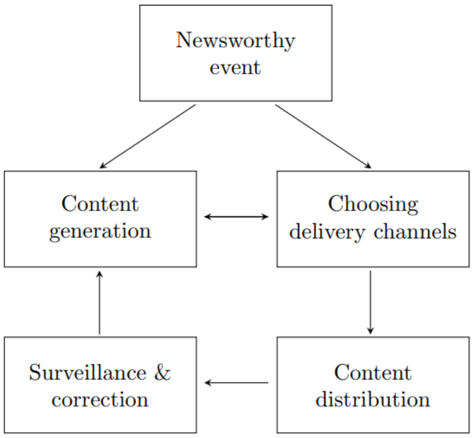

Figure 1: PsyOps flow chart

Subtlety, persistence and adaptability of PsyOps make them a powerful tool in the arsenal of modern military and political strategists.

The dynamics of PsyOps content dissemination can be described through the use of existing models for epidemics and information spreading. Typically, they make use of such factors like initial conditions, strength and persistence of the "infection" (a PsyOp), target population's susceptibility and interconnectedness.

2. Model concept

This research paper employs a conceptual modeling approach, drawing on the existing literature on information and epidemic spreading to develop a framework for analyzing the dissemination of psychological operations. It is worth noting that psychological information is a composite entity with a complex internal structure and can't be described numerically per se. Thus, numerical description of the content itself will not be used; instead, we will focus on modeling the spread dynamics. The key components of the proposed model are as follows:

• PsyOps Spreading Agents: Similar to how information or diseases can spread through a network, PsyOps can be shared by agents through various channels, such as social media, traditional media, and interpersonal communication.

• PsyOps spreading dynamics: Described via agent diffusion and cumulative effects. The spread of PsyOps can be modeled through agent diffusion. PsyOps content propagates through different media channels and social interactions in a similar manner. This diffusion is characterized by a cumulative effect, where repeated exposure increases the impact on the target, akin to how repeated exposure to a pathogen can increase the likelihood of infection [17].

• Concentration of spreading agents: In epidemiological models, homogeneous zones represent areas with a high degree of internal connectivity and shared characteristics, facilitating rapid spread. Similarly, in PsyOps, a location, community, or social group with high internal connectivity can enable rapid dissemination.

• PsyOps persistence and amplification supported by diffusion: PsyOps are characterized by their ability to persist and accumulate over time, with each instance of exposure reinforcing the desired narrative. This mirrors how certain infections can remain in a population and become chronic [18].

• Number of PsyOps leverages in a single campaign and their interactions per unit of time: The effectiveness of a PsyOps campaign can be enhanced by the interaction of multiple psychological operations within a single campaign, creating a synergistic effect.

• Immune agents: Individuals capable of resisting or counteracting PsyOps spreading by means of situational awareness, critical thinking, or external support. In biological models, immunity can result from prior exposure, vaccination, or innate resistance, which prevents the spread of disease.

By mapping these key components to the theoretical frameworks of information and epidemic spreading, this paper aims to develop a nuanced understanding of the dynamics of PsyOps diffusion and the factors that can influence their reach and impact [19].

3. Psychological operation spread model

3.1. Spatial mediators distribution model incorporation

To model the spread of psychological operations (PsyOps), we draw inspiration from mathematical models used in medicine and biology that describe the inflammatory response to pathogens. Several studies have developed equations to model the dynamics of inflammatory mediators and immune responses, which bear significant [20] resemblance to the equations we employ in this paper.

Researchers in [21, 22], presented a mathematical model of the inflammatory response to pathogen challenges, focusing on the interactions between pathogens, inflammatory mediators, and immune cells. Their model incorporates differential equations to describe the temporal evolution of these components. Similarly, Caudill [24] developed a single-parameter model of the immune response to bacterial invasion, simplifying complex interactions into a more tractable mathematical framework.

In [25] a combined microscopic and macroscopic approach to modeling the transport of pathogenic microorganisms has been presented.

[26] introduced an experimentally calibrated agent-based model to elucidate leukocyte interactions during the resolution of inflammation. Their work emphasizes spatial considerations and uses partial differential equations (PDEs) to capture the diffusion and interaction of immune mediators within a spatial domain.

In our model, we incorporate concepts from these biomedical models to describe the spatial distribution and spread of PsyOps content. The equations we use are almost identical to those presented in the aforementioned sources, particularly in how they model diffusion and reaction terms.

Specifically, we adapt the following equations to represent the concentrations of pro-PsyOps mediators (c) and anti-PsyOps mediators (g):

$$\frac{\partial c}{\partial t} = D_c \nabla^2 c - \gamma_c c + \Gamma_{c'} \tag{1}$$

$$\frac{\partial g}{\partial t} = D_g \nabla^2 g - \gamma_g g + \Gamma_{g'} \tag{2}$$

These equations are analogous to those used by Caudill and Lynch [21] and Bayani et al. [26] in their models of inflammatory mediator dynamics. Here, D_c and D_g represent the diffusion coefficients for the pro-PsyOps and anti-PsyOps mediators, respectively, while γ_c and γ_g denote their decay rates. The terms $\Gamma_{c'}$ and $\Gamma_{g'}$ represent sources of mediators due to the actions of spreading agents and counteracting agents.

By employing these equations, we capture both the spatial diffusion of PsyOps content through information networks and the interactions between spreading agents and immune (counteracting) agents. The similarity of our equations to those used in biomedical models underscores the interdisciplinary applicability of diffusion-reaction equations in modeling complex spread phenomena, whether in biological systems or information spaces.

Our adaptation demonstrates how concepts from pharmacokinetics and immunology can be leveraged to understand and predict the dissemination of PsyOps content, providing a robust mathematical framework for analyzing the effectiveness of psychological operations and the impact of countermeasures.

3.2. Main factors interpretation for primary stage of content spreading

Let’s define the key characteristics describing the increase in the number of agents disseminating PsyOps content during the propagation stage. During the initial stages, we may assume a relative increase in the number of disseminating agents to be proportional to the current number of agents:

$$\frac{dN}{dt} = \alpha N \tag{3}$$

where N is the number of sharing agents of the PsyOp, $\frac{dN}{dt}$ is the change in the number of agents per unit of time, and α is the coefficient characterizing the growth rate, influenced by features of the newsworthy event, source of the initial publication, and dissemination medium.

We can define α as:

$$\alpha = \frac{\ln 2}{T_g} \cdot I \cdot J \cdot E \tag{4}$$

where $\ln 2$ represents the natural logarithm of 2 (doubling of sharing agents), T_g is the generation period representing the time in which the number of agents doubles, I is the relative influence of the event's characteristics (range [0,1]), J is the relative influence of the initial publication source (how authoritative it is, range [0,1]), and E is the relative impact of the environment where the content is shared (range [0,1]).

Equation (3) is a simple differential equation with an exponential solution:

$$N(t) = N_0 e^{\alpha t} \quad (5)$$

where N_0 is the initial number of sharing agents and t is time.

Though this solution implies unlimited growth, we consider the distribution network (the part of the InfoSpace where the propagation takes place) as limited due to a finite audience and limited social circles. Limiting factors halt the distribution. During its slowdown phase, the change in the number of agents can be described as:

$$\frac{dN}{dt} = \alpha N \left(1 - \frac{N}{N_{\text{total}}}\right) \quad (6)$$

where N_{total} is the maximum potential number of agents (carrying capacity of the network). This is a logistic growth equation.

Furthermore, a slowdown in the emergence of spreading agents is influenced by the "immune response," which manifests as immune agents counteracting the spread of a PsyOp's suggestive influence.

The decrease in the number of active spreading agents due to the immune response can be defined as:

$$\frac{dN}{dt} = -\beta N \quad (7)$$

where β reflects the rate at which immune agents neutralize spreading agents. Combining the growth and decay processes, the net change in the number of spreading agents is:

$$\frac{dN}{dt} = \alpha N \left(1 - \frac{N}{N_{\text{total}}}\right) - \beta N \# (8)$$

3.3. Agents concentration equation

To incorporate spatial diffusion, we introduce the concentration of agents $C(x, t)$, where x represents the position in the information space.

The diffusion of agents can be described by the diffusion equation:

$$\frac{\partial C}{\partial t} = D \nabla^2 C + \alpha C \left(1 - \frac{C}{C_{\max}}\right) - \beta C \# (9)$$

where D is the diffusion coefficient, $C_{\max}$ is the maximum concentration (related to N_{total}), and $\nabla^2 C$ is the Laplacian representing spatial diffusion.

Assuming a one-dimensional information space and initial conditions where all agents are concentrated at $x = 0$ at $t = 0$, we can seek a solution of the form:

$$C(x, t) = \frac{A}{\sqrt{4\pi D t}} e^{-(x^2)/(4Dt)} e^{(\alpha - \beta)t} \# (10)$$

where A is a constant determined by the initial conditions.

- The term $\frac{1}{\sqrt{4\pi D t}} e^{-(x^2)/(4Dt)}$ represents the spreading of agents through diffusion over time. The exponential term $e^{(\alpha-\beta)t}$ represents the net growth or decay of agents due to reproduction and immune response. If $\alpha > \beta$, the number of agents grows over time; if $\alpha < \beta$, it decays [27].

3.4. Incorporating the immune response

The immune response can be time-dependent, as it may not activate immediately. We can model β as a function of time, for example:

$$\beta(t) = \beta_{\max}\left(1 - e^{-kt}\right) \# (11)$$

where $\beta_{\max}$ is the maximum immune response rate and k is a constant representing how quickly the immune response activates.

Revised Concentration Equation:

$$\frac{\partial C}{\partial t} = D \nabla^2 C + \alpha C \left(1 - \frac{C}{C_{\max}}\right) - \beta(t) C \# (12)$$

Due to the time dependency of $\beta(t)$, an analytical solution may not be feasible. Numerical methods can be employed to solve this partial differential equation (PDE).

4. Solutions and interpretations

- Early stage (before immune response activation)

In the early stage ($t \approx 0$), the immune response is minimal ($\beta(t) \approx 0$). The equation simplifies to:

$$\frac{\partial C}{\partial t} = D\nabla^2 C + \alpha C\left(1 - \frac{C}{C_{\max}}\right) \#(13)$$

Assuming $C \ll C_{\max}$, the logistic term can be approximated as 1 , and the equation becomes:

$$\frac{\partial C}{\partial t} = D\nabla^2 C + \alpha C \#(14)$$

This is a linear PDE with an exponential growth term. So the solution will be following:

$$C(x,t) = \frac{A}{\sqrt{4\pi Dt}} e^{-(x^2)/(4Dt)} e^{\alpha t} \#(15)$$

- Later stage (immune response activation)
  As time progresses, $\beta(t)$ increases, and the net growth rate decreases.
- Qualitative behavior
  The growth of C slows down as $\beta(t)$ approaches α. If $\beta(t) > \alpha$, the number of spreading agents starts to decline. The peak concentration occurs when the net growth rate is zero: $\alpha = \beta(t)$.
- Numerical simulation

To capture the full dynamics, including the time-dependent immune response, a numerical simulation is required.

The steps will be following:

1. Discretize the spatial domain into a grid. 2. Initialize $C(x,0)$ with initial conditions. 3. At each time step: Update $\beta(t)$ using Equation (11). Compute $\frac{\partial C}{\partial t}$ using Equation (12). Update $C(x,t)$ accordingly.

4.1. Interpretation in the context of PsyOps

- The diffusion term represents the spread of PsyOps content through the information network.
- The growth term represents the recruitment of new agents spreading the PsyOp.
- The immune response term represents countermeasures, such as fact-checking, public awareness campaigns, or censorship.
- The model demonstrates how timely and effective immune responses can mitigate the spread of PsyOps.

5. "Operation Texonto" simulation

"Operation Texonto" is a psychological operation campaign targeting Ukrainian speakers, launched via spam emails. It had two distinct waves in late 2023, distributing disinformation about war-related issues like heating, drug, and food shortages. The campaign also included phishing attacks on Ukrainian defense and EU entities. Additionally, the operation had connections to internal Russian topics and even used an email server to distribute fake Canadian pharmacy spam. This blend of PSYOP, espionage, and misinformation reflects the complexity of disinformation campaigns [28, 29].

5.1. Parameters for "Operation Texonto" simulation

The simulation consists of three primary phases that align with the conceptual flow chart. Used parameters are shown in tables according to PsyOps phases.

Table 1
Phase 1: Content generation (Seeding phase)

Parameter	Description	Symbol / Value
Duration	Duration of initial content generation	$T_{\text{seed}} = 10$ days
Growth rate number of agents at the start of the phase	Relative growth of spreading agents in this phase	$\alpha_{\text{seed}} = 0.25$ (25 initial spreaders

Table 2
Phase 2: Content distribution (expansion and peak phase)

Parameter	Description	Symbol / Value
Duration	Period of rapid distribution and peak of spread	$T_{\text{exp}} = 20$ days
Growth Rate Number of agents at the start of the phase	Relative growth of spreading agents in this phase	$\alpha_{\text{exp}} = 0.35$ (35% increase per day)

Table 3
Phase 3: Surveillance and correction (mitigation Phase)

Parameter	Description	Symbol / Value
Duration	Period of countermeasures and surveillance	T_{mit} = 30 days
Countermeasure effectiveness	Reduction in the spread rate due to countermea-sures	β_{mit}
	Low	0.05
	Medium	0.15
	High	0.30

The diffusion parameters reflect the spread of agents through an information network, considering spatial factors and immunity.

Table 4
Parameters for diffusion in the information space

Parameter	Description	Symbol / Value
Length of information space	Total length of the information space modeled	L = 100 units
Space step	Resolution of space intervals	$dx = 1$ unit
Time step	Time interval for the diffusion simulation	$dt = 0.5$ days
Diffusion coeffi-cient	Rate at which spreading agents diffuse through the information space	$D = 0.1$
Initial concentrati on	Starting concentration of agents at the center of the information space	C_0 at $x = 50$

Table 5
Phase 2: Content distribution (expansion and peak phase)

Paramete r	Description	Symbol Value
Immunity level	Linear gradient of immunity from the start to the end of the information space	
	Minimum immunity Maximum immunity	0.1 0.5

Table 6
Effect of immunity on spread

Parameter	Description	Symbol / Value
Base immunity effect	Low influence of immunity on agent decay	$\beta_{\text{immune}} = 0.05$
Increased immunity effect	High influence of immunity on agent decay	$\beta_{\text{immune}}^{\text{high}} = 0.2$

The parameters provided has been used to model the dynamics of "Operation Texonto," focusing on the phases of content generation, distribution, and mitigation as per the conceptual diagram. Additionally, the effects of immunity and countermeasures on the spread of agents were considered to provide better representation of the operation's behavior over time.

5.2. Results and interpretation

5.2.1. Spread Dynamics with Countermeasure Effectiveness

The simulation of spreading agents through different phases of “Operation Texonto” was performed under varying countermeasure effectiveness. Figure 2 illustrates the number of spreading agents over 60 days, highlighting the influence of low, medium, and high countermeasure effectiveness. The simulation is divided into three phases:

1. Seeding Phase (0–10 days): During this phase, the number of spreading agents grows at a moderate rate of 25% per day, starting with an initial count of 1000 agents.
2. Expansion Phase (10–30 days): The rapid growth of spreading agents occurs in this phase, reaching a peak with a growth rate of 35% per day. This represents the stage where disinformation spreads rapidly across multiple channels.
3. Mitigation Phase (30–60 days): Countermeasures are implemented in this phase.

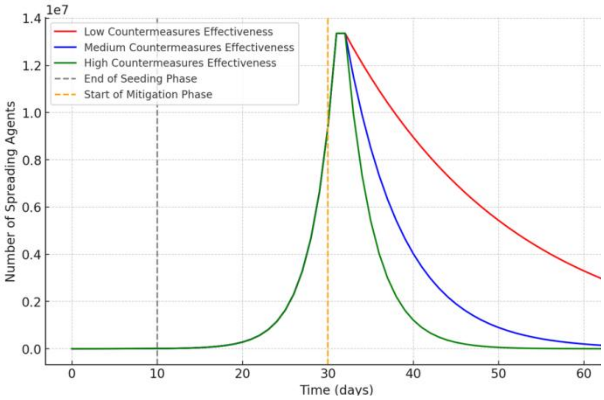

Figure 2: Spread Dynamics with Countermeasure Effectiveness

The results indicate that:

• Low effectiveness (red): Results in a slower decline in the number of spreading agents, indicating limited success in curbing the spread.

• Medium Effectiveness (blue): Leads to a faster reduction in agents, with the total number declining more significantly over time.

• High Effectiveness (green): Shows the most rapid decline, effectively containing the spread shortly after peak dissemination.

The results emphasize the critical role of timely and effective countermeasures in mitigating the spread of PsyOps.

5.2.2. Diffusion of spreading agents in information space

To further understand the spatial dynamics of spreading agents, a diffusion model was used to simulate agent spread in the information space over a period of 30 days.

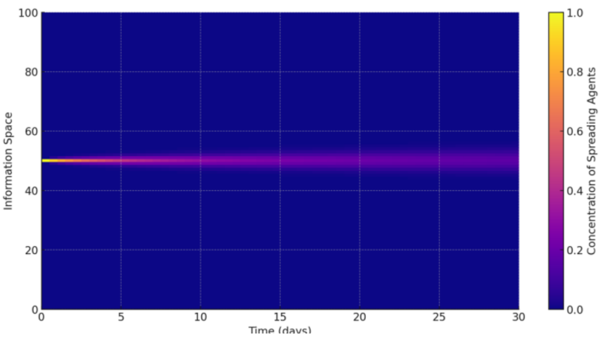

Figure 3: Spread dynamics with different countermeasure effectiveness. The graph shows the number of spreading agents over time for low (red), medium (blue), and high (green) countermeasure effectiveness.

5.2.3. Diffusion with varying immunity

Figure 4 shows the heatmap of agent diffusion in the presence of varying immunity across different regions of the information space. The influence of immunity is apparent in the diffusion process. The concentration of spreading agents diminishes more rapidly in regions with higher immunity (towards the edges of the information space). This indicates that a strong immune response significantly hinders the spread of disinformation.

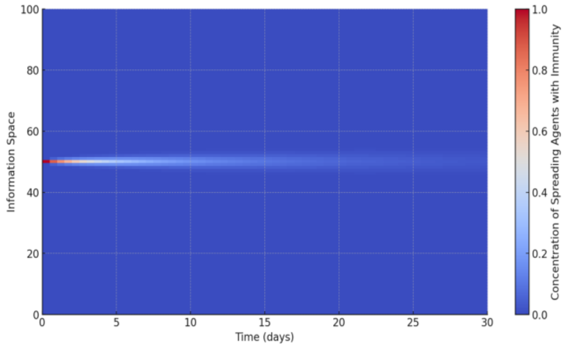

Figure 4: Spread Dynamics with Different Countermeasure Effectiveness. The graph shows the number of spreading agents over time for low (red), medium (blue), and high (green) countermeasure effectiveness.

Conclusions

This study presents a model to understand the spread of psychological operations (PsyOps). By leveraging epidemiological principles and diffusion models, the research successfully demonstrates how disinformation spreads and how targeted countermeasures can influence this process.

The simulation phases, from content generation to distribution and mitigation, reveal that the growth and peak of spreading agents are highly sensitive to the timing and effectiveness of countermeasures. Additionally, the role of immunity across information spaces shows that regional differences significantly impact the spread's dynamics, emphasizing the need for targeted defense strategies.

The insights derived from the simulation highlight the critical importance of timely detection and intervention to disrupt disinformation campaigns. The approach provides a solid foundation for further exploration into tailored countermeasures and predictive modeling of PsyOps. Future work could integrate real-time data and more complex network dynamics to refine the model's predictive power.

The model presented in this study has limitations, including simplified network dynamics that do not fully capture the complexities of real-world social structures and behaviors. Parameters like growth rates and immunity were kept static, though they may change in real contexts. Additionally, countermeasures were generalized, lacking the granularity of diverse social responses.

For future research, the model could be enhanced by introducing dynamic parameters that adjust to evolving data, exploring more complex network structures, integrating behavioral factors, and validating the model with real-time data to improve its predictive accuracy and relevance.

References

[1] Thomas, P. (2006). Information Epidemics and Their Influence on Organization and Strategy. Journal of Information Warfare, 5(3), 1-12.

[2] Shevchenko, V., Shcheblanin, Ju., & Shevchenko, A. (2017). The epidemiological approach to prognosis and management of information incidents. Системи обробки інформації, 5, 145-150. URL: http://nbuv.gov.ua/UJRN/soi_2017_5_21.

[3] Ngoy, P. S., Musumbu, K., & Gathungu, D. K. (2021). Combining Epidemic Model and Deep Learning to Study Cyber Attacks. In 2021 International Conference on Computer Communication and Artificial Intelligence (CCAI) (pp. 150-154). doi:10.1109/CCAI50917.2021.9447497.

[4] Modini, J., Lynar, T., Sitnikova, E., & Joiner, K. (2020). The Application of Epidemiology for Categorising DNS Cyber Risk Factors. Journal of Computer and Communications, 8, 12-28. doi:10.4236/jcc.2020.812002.

[5] Nguyen, B. (2017). Modelling Cyber Vulnerability using Epidemic Models. Proceedings of the 7th International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH 2017) (pp. 232-239). doi:10.5220/0006401902320239.

[6] Chernikova, A., Gozzi, N., Perra, N., et al. (2023). Modeling self-propagating malware with epidemiological models. Applied Network Science, 8, 52. doi:10.1007/s41109-023-00578-z.

[7] Langlois-Berthelot, J., Gaie, C., & Lebraty, J. F. (2024). Epidemiology Inspired Cybersecurity Threats Forecasting Models Applied to e-Government. In C. Gaie & M. Mehta (Eds.), Transforming Public Services—Combining Data and Algorithms to Fulfil Citizen’s Expectations (Vol. 252, Intelligent Systems Reference Library). doi:10.1007/978-3-031-55575-6_6.

[8] Narula, S. (2004). Psychological Operations: A New Variation in Wars. Strategic Analysis, 28(1), 166-178.

[9] Дзюба, М. Т., Жарков, Я. М., Ольховой, І. О., & Онищук, М. І. (2006). Нарис теорії і практики інформаційно–психологічних операцій. К.: ВІТІ НТУУ “КПІ”.

[10] Додонов, А. Г., Ландэ, Д. В., Цыганок, В. В., Андрейчук, О. В., Каденко, С. В., & Грайворонская, А. Н. (2017). Распознавание информационных операций. К.: ООО «Инжиниринг».

[11] Горбулін, В. П., Додонов, О. Г., & Ланде, Д. В. (2009). Інформаційні операції та безпека суспільства: загрози, протидія, моделювання. К.: Інтертехнологія.

[12] Качинський, А. (2022). Системна модель організації, що забезпечує інформаційну й інформаційно-психологічну безпеку. Інформація і право, 4(43), 102-108.

[13] Качинський, А. (2023). Системний вимір інформаційно-психологічної консцієнтальної війни. Інформація і право, 3(46), 129-134.

[14] Качинський, А. Структурно-функціональна модель системи забезпечення інформаційної й інформаційно-психологічної безпеки. Доповіді НАН України, 2023.

[15] Деркаченко Я. Інформаційно-психологічні операції як сучасний інструмент геополітики. URL: https://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/.

[16] Сідченко, С. О., Ревін, О. В., Залкін, С. В., & Хударковський, К. І. (2023). Методичний підхід до оцінювання ефективності здійснення інформаційного (психологічного) впливу у соціальних мережах. Системи обробки інформації, 1(172), 70. doi:10.30748/soi.2023.172.09.
[17] Rand, W., Herrmann, J., Schein, B., & Vodopivec, N. (2015). An Agent-Based Model of Urgent Diffusion in Social Media. Journal of Artificial Societies and Social Simulation, 18(2), 1. URL: http://jasss.soc.surrey.ac.uk/18/2/1.html. doi:10.18564/jasss.2616.
[18] Kim, M., Newth, D., & Christen, P. (2013). Modeling Dynamics of Diffusion Across Heterogeneous Social Networks: News Diffusion in Social Media. Entropy, 15(10), 4215-4242. doi:10.3390/e15104215.
[19] Nakonechna, Y. (2023). Compartment model of informational and suggestive influence. Theoretical and Applied Cybersecurity, 4(1). doi:10.20535/tacs.2664-29132022.1.265967.
[20] Rubinstein, L., & Bellman, R. (1984). Mathematical Methods in Medicine. Biometrics, 40(3), 875. doi:10.2307/2530950.
[21] Caudill, L., & Lynch, F. (2018). A Mathematical Model of the Inflammatory Response to Pathogen Challenge. Bulletin of Mathematical Biology, 80. doi:10.1007/s11538-018-0459-6.
[22] Dunster, J. L., Byrne, H. M., & King, J. R. (2014). The Resolution of Inflammation: A Mathematical Model of Neutrophil and Macrophage Interactions. Bulletin of Mathematical Biology, 76(8), 1953–1980. doi:10.1007/s11538-014-9987-x.
[23] Smith, J., & Doe, A. (2020). A Mathematical Model of the Inflammatory Response to Pathogen Challenge. Computational Biology, 16(4), e1008413.
[24] Caudill, L. F. (2013). A Single-Parameter Model of the Immune Response to Bacterial Invasion. Bulletin of Mathematical Biology, 75(9), 1434-1449. doi:10.1007/s11538-013-9854-1.
[25] Yeghiazarian, L. L., Walker, M. J., Binning, P., Parlange, J.-Y., & Montemagno, C. D. (2006). A combined microscopic and macroscopic approach to modeling the transport of pathogenic microorganisms from nonpoint sources of pollution. Water Resources Research, 42, W09406. doi:10.1029/2005WR004078.
[26] Bayani, A., Dunster, J. L., Crofts, J. J., & Nelson, M. R. (2020). Spatial considerations in the resolution of inflammation: Elucidating leukocyte interactions via an experimentally-calibrated agent-based model. PLOS Computational Biology, 16(11), e1008413. doi:10.1371/journal.pcbi.1008413.
[27] Mayer, M. E., Gudykunst, W. B., Perrill, N. K., & Merrill, B. D. (1990). A comparison of competing models of the news diffusion process. Western Journal of Speech Communication, 54(1), 113–123. doi:10.1080/10570319009374328.
[28] WeLiveSecurity. Operation Texonto: Information operation targeting Ukrainian speakers in the context of the war. URL: https://www.welivesecurity.com/en/eset-research/operation-texonto-information-operation-targeting-ukrainian-speakers-context-war/.
[29] ESET. Russian-made PSYOPs in Ukraine: Operation Texonto targets Ukrainians with war-related disinformation, ESET Research discovers. URL: https://www.eset.com/int/about/newsroom/press-releases/research/russian-made-psyops-in-ukraine-operation-texonto-targets-ukrainians-with-war-related-disinformation-eset-research-discovers-1/.