Mathematical and Computer Models of Non-Permanent Information Warfare

NUGZAR KERESELIDZE
Faculty of Mathematics and Computer Science
Sukhumi State University
61, A. Politkovskaya street, Tbilisi
GEORGIA
nkereselidze@sou.edu.ge http://www.kereseli.sou.edu.ge

Abstract: - The paper deals with the system of Non-Permanent Information Warfare, in which the opposition of the antagonistic parties is due to a certain event. For it, both mathematical and computer models are constructed. The models take into account different scenarios for the development of the system after the occurrence of some event. On the basis of a computer experiment with various values of system parameters, a forecast is made of the further course of the Information Warfare. The question of the system's controllability by the peacekeeping side and the definition of recommendations for the completion of the Information Warfare by third-party efforts are studied.

Key-Words: - System, Information Warfare, Information Attack, Mathematical Model, Computer Model, Computer experiment, Controllability.

1 Introduction

Information confrontation in the era of intensive penetration of information technologies in all spheres of human activity sometimes acquires such a ruthless and rigid character that it has the right to be called Information Warfare. In the XXI century, "Word" has become an effective weapon in the confrontation of the parties. With its help, they try to manipulate the minds of the masses, forcing them, for example, to vote in elections for those candidates, who are desirable to the enemy. This result is achieved with the help of the "Word", which brings misinformation, discreditation, lies, fakes and so on. The national security strategies of countries now necessarily speak of information security. At the same time, specific actions are planned in governments to repel Information attacks. For example, in the Council of Europe, a special task force has been created - East StratCom, with a stable and considerable budget, the purpose of which is to monitor and identify misinformation against the policy of the European Council and its disavowal (https://euvsdisinfo.eu/). Thus, on the one hand we are dealing with a subject that reflects an Information attack and on the other hand we have a subject who prepares these attacks. I.e. there's confrontation between the parties with the help of the "Word" and we will, from here on out, call this opposition of the parties the "Information Warfare".Naturally, before state officials began to turn their attention to the "Information Warfare", scientists were interested in it. From a wide arsenal of methods for researching the Information Warfare, some scientists chose modeling - mathematical and computer. When modeling Information Warfares, the following processes and actors can be identified - these are the parties - participants spreading information flows, calculated for the subjects, in order to turn them into their adepts. These models can be classified depending on which participant or information warfare event is in focus of the model.

Among the models of the Information Warfare, we can distinguish the so-called models of adepts, in which, generally, the change in the number of persons who perceived the widespread information is simulated [1]. A considerable number of scientific works on information warfare's adept type models is based on the idea set forth in [2] and concerns modeling of an advertising campaign.

Considerable scientific interest is modeling only the volumes of information flows in the Information Warfare [3-6]. In these models, as a rule, three participants of the Information Warfare are considered. Two of them are antagonistic against each other and spread relevant information. The third party is the peacemaking side, which also spreads the flow of information aimed at reconciling the antagonistic sides. In some information flow models of Information Warfare, the restriction on

the flow of information due to the level of Information Technology development of the parties [7-8] is taken into account. Recently, efforts have been made to combine models of type adepts and information flows. As a result, there is a possibility of a comprehensive study of both the number of distributed information flows and the number of people, who have or not have perceived this information [9-11].

All of these three types of models have the following commonality: the course of the Information Warfare on the observed time interval $[0;T]$ has no features. This means that any point in time $t \in [0;T]$ is no different from any other point in time $\xi \in [0;T]$. Meanwhile, often informational opposition is confined to some event tied to a certain point in time. For example, the opposing parties may wage the Information Warfare due to the success of the presidential elections that are appointed at time $\tau \in [0;T]$. As a rule, in these cases, antagonistic parties increase the intensity of Information Attacks by time point τ, and then after a while either reduce the intensity of the attacks, or dramatically increase it. For the given example, a decrease in the intensity of Information Attacks occurs if the parties accept the election results; if the parties or at least one of the parties does not recognize the election results, then the intensity of the Information Attacks increases. Parties or one of the parties can prepare an information background for the revolutionary development of events. Thus, the Information Warfare is not proceeding permanently, but is timed to a certain event, and after the occurrence of this event, the Information Warfare may fade away, or receive a new impulse and continue in an aggravation mode. In the latter case, the role and responsibility of the peacemaking side especially increases, and the question is raised whether it can prevent, and at what activity, the Information Warfare taking place in an aggravated mode.

In this paper, we will try to build a model of a Non-Permanent Information Warfare, and solve the task of its controllability. The presented work is created with the help of Shota Rustaveli National Science Funding of Georgia Grant YS17_78.

2 Problem Formulation

At the first stage, we will try to build an information flow mathematical model of Non-Preventive Information Warfare. The process of Non-Preventive Information Warfare will be observed on the time interval $[0;T] \subset R$, where R is the set of real numbers. On this segment we define the time moment $\tau \in [0;T]$, where $0 < \tau < T$, and in which some event takes place, to which antagonistic parties are trying to gain superiority in this Information Warfare. It is natural to assume that by the time point τ the antagonistic sides increase the intensity of information attacks. Let's mark the amount of information that the first antagonistic side spreads at time t with $x(t)$ and for the second antagonistic side, they spread $y(t)$ amount of information at time t. The third peacekeeping party participating in the Information Warfare disseminates information calling for the antagonistic parties to stop information attacks in the amount equal to $z(t)$. When constructing a mathematical model, we will assume that the antagonistic sides only stick to their tactics of conducting Information Attacks, without taking into account the activity of the other antagonistic side. At the same time, each of the antagonistic parties to a certain extent listens to the appeals of the third peacemaking side. Readiness to listen to a third party will be called peacekeeping readiness of the party. We will note it with $\beta_1(t)$ and $\beta_2(t)$, respectively, for the first and second sides. The intensity of Information Attacks of the antagonistic parties depends on the aggressiveness index of each of the parties, respectively - $\alpha_1(t)$ and $\alpha_2(t)$, it also depends on the Information Technology development level of the parties. The development level of the Information Technologies of the parties will be determined by their ability to spread the maximum amount of information and we will mark it with I_1 and I_2, respectively, for the first and second sides. The development level of third party Information Technologies is denoted by I_3. The activity of the third party also depends on its peacekeeping intensity, provoked by each of the antagonistic sides and having value $\gamma_1(t)$ and $\gamma_2(t)$. Now the mathematical model of the Information Warfare as a Cauchy problem for a system of ordinary differential equations can be written in the following way:

$$\begin{cases} \dfrac{dx(t)}{dt} = \alpha_1(t)x(t)\left(1-\dfrac{x(t)}{I_1}\right) - \beta_1(t)z(t), \\ \dfrac{dy(t)}{dt} = \alpha_2(t)y(t)\left(1-\dfrac{y(t)}{I_2}\right) - \beta_2(t)z(t), \\ \dfrac{dz(t)}{dt} = \left(\gamma_1(t)x(t)+\gamma_2(t)y_2(t)\right)\left(1-\dfrac{z(t)}{I_3}\right). \end{cases} \quad (1)$$

$$x(0)=x_0 \quad y(0)=y_0 \quad z(0)=z_0 \quad (2)$$

In the mathematical model of the Information Warfare (1), (2), the second line (2) represents the initial conditions for each of the parties.

Meanwhile, if there is a system's information security task, then it can be achieved by the activity of the peacekeeping side. With proper activity of the peacekeeping side, the antagonistic parties can stop information attacks and thus the Information Warfare will end. In addition, each of the antagonistic parties can complete information attacks at different points of time, which are not predetermined. Taking into account these notes, the following conditions should be introduced in the mathematical model of the Information Warfare completion: there are such arbitrary moments of time $t^*, t^{**} \in [0;T]$ during which we have the execution of:

$$\begin{cases} x(t^*)=0, \quad x(t)\le 0 \quad \forall t \in [t^*;T], \\ y(t^{**})=0, \quad y(t)\le 0 \quad \forall t \in [t^{**};T]. \end{cases} \quad (3)$$

Thus, the mathematical model of the Information Warfare completion turns from the Cauchy problem into a problem with special boundary conditions (1), (2), (3), which is sometimes called the Chilker problem [12-14]. We can obtain a mathematical model of a Non-Preventive Information Warfare from model (1)-(3) by selecting special functions for aggressiveness of the antagonistic parties.

3 Problem Solution

Let us consider two possible scenarios for the development of Non-Preventive Information Warfare. As we have determined, in a Non-Preventive Information Warfare at some point in time a certain event occurs, to which the intensity of Information Attacks is increased. However, after the onset of this event, Information attacks decrease or increase. We will separately examine these two scenarios for the development of the Information Warfare course.

3.1 Non-Preventive Information Warfare with Mutual Fading.

In order to obtain a mathematical model of the Non-Preventive Information Warfare with Mutual Fading from (1)-(3) models, we select the aggressiveness functions of the antagonistic sides in the system (1). Since the information attacks of antagonistic parties increase to the moment of time τ and then decrease, for example, to zero, it is logical that the intensity index in the system (1) has the form of a bell shaped function. As such functions, it is possible to, for example, select certain trigonometric functions or a parabola at a certain interval and so on. In system (1), we consider specific functions and assume that $\alpha_1(t)=\alpha_2(t)=\alpha(t)$. Let us suppose that there is an inclusion $[0;2\tau]\subseteq[0;T]$. Then we can suppose, that $\alpha(t)=A\sin\left(\dfrac{\pi}{2\tau}t\right)+\varepsilon$, where A, ε are positive constants. In this case, we will assume that ε is an arbitrarily small number. Let's assume that the following values are also constant: $\beta_1(t)=\beta_2(t)=\beta$, $\gamma_1(t)=\gamma_2(t)=\gamma$.

Then the system (1) will have the form:

$$\begin{cases} \dfrac{dx(t)}{dt} = \alpha(t)x(t)\left(1-\dfrac{x(t)}{I_1}\right) - \beta z(t), \\ \dfrac{dy(t)}{dt} = \alpha(t)y(t)\left(1-\dfrac{y(t)}{I_2}\right) - \beta z(t), \\ \dfrac{dz(t)}{dt} = \gamma\left(x(t)+y_2(t)\right)\left(1-\dfrac{z(t)}{I_3}\right). \end{cases} \quad (4)$$

The Cauchy tasks (4), (2) will be investigated using a computer experiment. We will also be interested in the question of system controllability, I.e. the ability to transfer the system from state (2) to state (3) using the selection of values for γ, I_3. The Information Warfare System is described using the mathematical model (4). We will conduct a computational experiment in the MatLab Application Software environment.

For a Non-Preventive Information Warfare with Mutual Fading, as the computer experiment showed in the general form of the system controllability tasks, it is not worth. Since the Information Attacks of the first and second sides become zero, i.e. Information Warfare ends with low third-party peacekeeping activity. For example, at the observation interval [0; 40], the initial conditions -

$x(0)=10$, $y(0)=15$, $z(0)=19$, and $A=1.8$, $\varepsilon=0.001$, $\tau=12$, $\beta=0.05$, $\gamma=0.05$, $I_1=155$, $I_2=150$, $I_3=200$ the first antagonistic side stops the Information Attack at time point $t^*=29.8845$, the other – at time point $t^{**}=29.8168$. See Fig. 1.

For the computer experiment, the program code was used with the ode15s solver, calculated for the numerical solution of hard systems. The program code is shown in Listing.

Listing. Program code to solve the model of non-preventive information warfare with mutual fading and peacekeeping activity.

```
x0=[10 15 19];
[T,Y]=ode15s('zat_not_perman_iwit',[0 40],x0);
plot(T,Y,'LineWidth',3.2); title('inf warfare');
xlabel('time'); ylabel('amount of information')
legend('X','Y','Z'); grid on
%ode- right side of the system i
function dxdt=zat_not_perman_iwit(t,x)
dxdt=zeros(3,1);a=1.8;b=.05;g=0.05;i1=155;i2=150;
i3=200;ut=12;ep=0.001;
dxdt(1)=a*(sin(pi*t/(2*ut))+ep)*x(1)*(1-x(1)/i1)-
b*x(3);
dxdt(2)=a*(sin(pi*t/(2*ut))+ep)*x(2)*(1-x(2)/i2)-
b*x(3);
dxdt(3)=g*(x(1)+x(2))*(1-x(3)/i3);
end
```

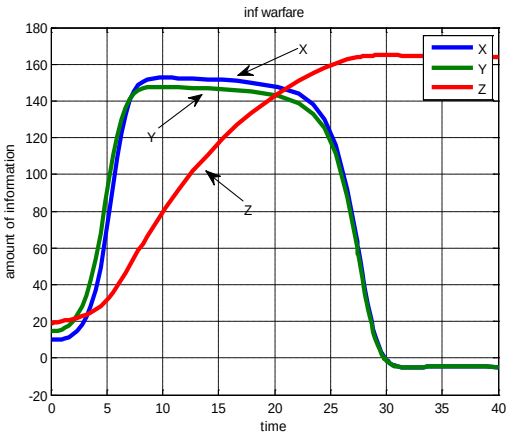

Fig. 1 Non-Preventive Information Warfare with Mutual Fading and peacekeeping activity

Non-Preventive Information War with Mutual Fading can actually end even when the peacekeeping side is not showing any activity. So for example, if in the program code given in Listing 1, we exclude the activity of the third party and equate its initial value to zero, I.e. assume that $\gamma=0.0$ and $z(0)=0.0$, then from the results of solving models (4), (2) it is clear that Information attacks of antagonistic parties become arbitrarily small, I.e. almost equal to zero, which is equivalent to the end of the Information Warfare, see Fig. 2.

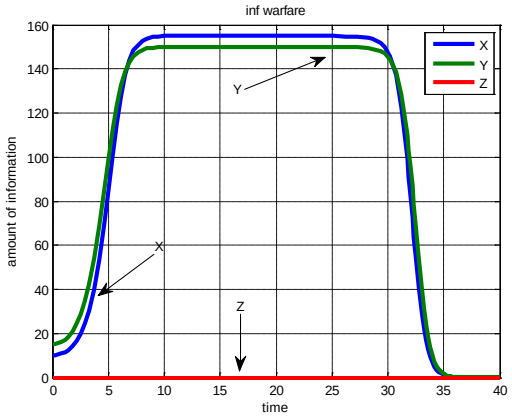

Fig. 2 Non-Preventive Information Warfare with Mutual Fading and without peacekeeping activity

The performed numerical experiment allows us to conclude that the Non-Preventive Information Warfare with fading described by the model (4), (2) is completed even without any efforts of the peacekeeping side. The peacekeeping effort is only necessary when the task is to complete the Information Warfare strictly by a certain point in time.

3.2 Non-Preventive Information Warfare with Aggravation

In order to obtain a mathematical model of the Non-Preventive Information Warfare with aggravation from (1)-(3) models, we select the aggressiveness functions of the antagonistic sides in the system of ordinary differential equations (1). Since the information attacks of antagonistic parties increase to the moment of time τ , and this process continues further, it is logical that the intensity index in system (1) should be monotonously increasing (non-decreasing) functions. As such functions, for example, one can choose an exponential function or a power function with an odd index, etc. The Cauchy problem of the Non-Preventive Information Warfare with aggravation will also be examined using a computer experiment. We will be interested in the question of system controllability In this case as well, I.e. the ability to transfer the system from state (2) to state (3) using the selection of values for γ, I_3 This computational experiment is also conducted in the environment of MatLab. We will consider the Non-Preventive Information Warfare with aggravation taking into account two scenarios. In the first scenario, both antagonistic sides resort to aggravation. In the second scenario,

only one of the parties has resorted to aggravation, the second is either neutral or operates in the mode of fading. Let's separately consider each scenario of the event.

3.2.1 Non-Preventive Information Warfare with Mutual Aggravation

In system (1), we consider specific functions and assume that $\alpha_1(t)=\alpha_2(t)=\alpha(t)$. Let's say we picked up $\alpha(t)=A\left((t-\tau)^3+\tau^3\right)$, where A is a positive constant. We will assume that the following parameters of system (1) are also constant: $\beta_1(t)=\beta_2(t)=\beta$, $\gamma_1(t)=\gamma_2(t)=\gamma$.

Then system (1) will have the form (4). The Cauchy task (4), (2) will be solved numerically for the observation interval [0; 40], the initial conditions: $x(0)=10$, $y(0)=15$, $z(0)=19$, and $A=1.8$, $\tau=12$, $\beta=0.05$, $\gamma=0.5$, $I_1=155$, $I_2=150$, $I_3=200$. With these values of the model, the first and second antagonistic sides soon reach their ultimate regime of Information Attacks. I.e. information Warfare does not stop, the third party is unable to extinguish it and also reaches the ultimate regime of information dissemination, due to the level of Information Technology. See Fig. 3.

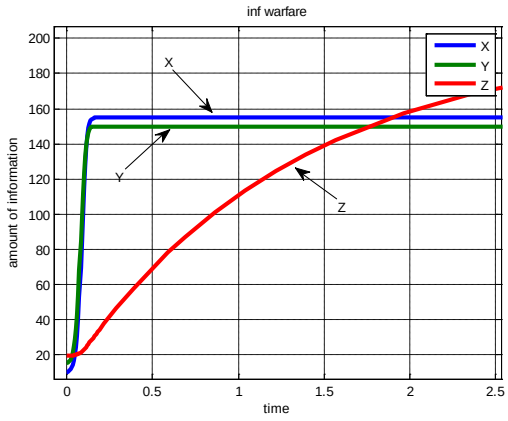

Fig. 3 Non-Preventive Information Warfare with Mutual Sharp Aggravation.

The problem of controllability with mutual aggravation is quite complex and difficult to achieve. For example, to stop the Information Warfare, it is necessary to increase the intensity of third-party peacekeeping activity γ by several folds: from 0.5 units to 200.5. At the same time, the level of third-party Information Technology was also increased. Under these conditions, the first and second antagonistic sides stop Information Attacks, respectively, at time points: $t^*=0.0585$, $t^{**}=0.082$. See Fig. 4, at the following values of model parameters: $x(0)=10$, $y(0)=15$, $z(0)=19$, и $A=1.8$, $\tau=5$, $\beta=1.5$, $\gamma=200.5$, $I_1=155$, $I_2=150$, $I_3=600$.

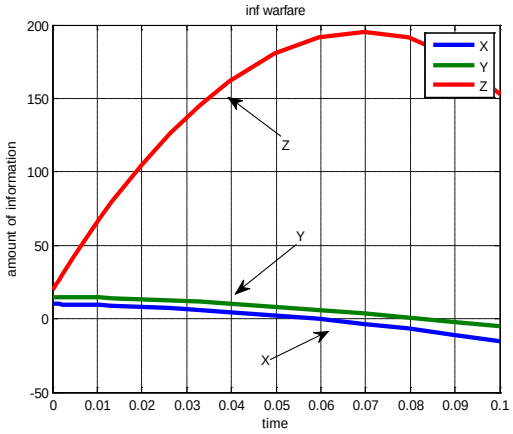

Fig. 4 High peacekeeping activity in Non-Preventive Information Warfare with Mutual Sharp Aggravation.

It should be noted that, as a computer experiment shows, in a mutual aggravation mode, with high rates of aggressiveness, peacekeeping efforts must be made from the very beginning to achieve an end to the Information Warfare, as this becomes impossible if the antagonistic parties have powerful Information Attacks – $x(t)$ and $y(t)$, similar respectively to the level of Information Technologies of the parties.

3.2.2 Non Preventive Information Warfare with One-sided Aggravation

Our interest is a Non-Preventive Information Warfare, when one of the parties after reaching time point τ gradually reduces the volume of Information Attacks, I.e. its activity fades. The other side, on the contrary, after reaching time point τ increases the Information Attacks, I.e. aggravates the Information Warfare. We will separately consider the case when the first side aggravates the Information Attacks and the second side selects fading mode, and vice versa. Of course, we could consider one of these cases and then generalize the results obtained to another case, but we would be interested in the possibility of selecting various aggressiveness indexes of the antagonistic sides for these cases. This approach is justified, since in paragraph 3.2.1 it has been established that in the event of a sharp mutual aggravation, the peacekeeping side needs to make incredible efforts to achieve an end to the Information Warfare.

Specifically, as an index of aggressiveness, you can choose, for example, functions for which $\alpha(t)=A\left((t-\tau)^3+\tau^3\right)$ is an infinitely large higher order and functions slowly changing at infinity. Such functions can be $\ln(t)$, $\ln(\ln(t))$, $\arctan(t)$ and others that are similar. Let's assume that in system (1) $\alpha_1(t)=A_1\ln(1+\ln(1+t+\varepsilon))$, $\alpha_2(t)=A_2\sin\left(\frac{\pi}{2\tau}t\right)+\varepsilon$, $\beta_1(t)=\beta_2(t)=\beta=const$, $\gamma_1(t)=\gamma_2(t)=\gamma=const$. then system (1) can be written in the following way:

$$\begin{cases}\frac{dx(t)}{dt}=A_1\ln(1+\ln(1+t+\varepsilon))x(t)\left(1-\frac{x(t)}{I_1}\right)-\beta z(t),\\ \frac{dy(t)}{dt}=\left(A_2\sin\left(\frac{\pi}{2\tau}t\right)+\varepsilon\right)y(t)\left(1-\frac{y(t)}{I_2}\right)-\beta z(t),\\ \frac{dz(t)}{dt}=\gamma\left(x(t)+y_2(t)\right)\left(1-\frac{z(t)}{I_3}\right).\end{cases} \quad (5)$$

The Cauchy task (5), (2) was investigated using a computational experiment. The computer experiment showed that the Non-Preventive Information Warfare given by model (5), (2) is controllable, i.e. there are such γ, I_3 values, for which the Information Warfare system from state (2) enters state (3). For example, with values: $x(0)=10$, $y(0)=15$, $z(0)=20$, and $A_1=0.5$, $A_2=1.2$, $\tau=5$, $\beta=0.05$, $\gamma=5.5$, , $I_1=155$, $I_2=150$, $I_3=250$ the first party stops the Information Attack at time point $t^*=2.3562$, the second side – at time point $t^{**}=3.1086$. See Fig. 5.

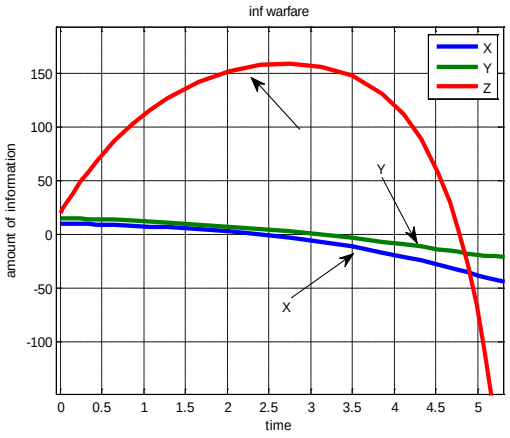

Fig. 5 Non-Preventive Information Warfare with first side Aggravation and second side fading.

Now let's consider the case when the second side fades its activity, and the first aggravates. Let's say $\alpha_1(t)=A_1\sin\left(\frac{\pi}{2\tau}t\right)+\varepsilon$, and for the second side we have $\alpha_2(t)=A_2 arctg(t+\varepsilon)$. Then system (5) will have the form:

$$\begin{cases}\frac{dx(t)}{dt}=\left(A_1\sin\left(\frac{\pi}{2\tau}t\right)+\varepsilon\right)x(t)\left(1-\frac{x(t)}{I_1}\right)-\beta z(t),\\ \frac{dy(t)}{dt}=A_2 arctg(t+\varepsilon)y(t)\left(1-\frac{y(t)}{I_2}\right)-\beta z(t),\\ \frac{dz(t)}{dt}=\gamma\left(x(t)+y_2(t)\right)\left(1-\frac{z(t)}{I_3}\right).\end{cases} \quad (6)$$

The Cauchy task (6), (2) research showed that the Non-Preventive Information Warfare is controllable, i.e. there are such γ, I_3 values, for which the Information Warfare system from state (2) enters state (3). However, for the controllability of the system (6), (2), the peacekeeping side needs to make considerable efforts; the value of peacekeeping activity γ must be increased by folds, in comparison to what it was for controllability in the previous case. For example, with $x(0)=10$, $y(0)=15$, $z(0)=20$, and $A_1=0.5$, $A_2=1.2$, $\tau=12$, $\beta=0.05$, $\gamma=31.5$, , $I_1=155$, $I_2=150$, $I_3=350$ the first side stops the Information Attack at time point $t^*=0.9836$ and the second side – at time point $t^{**}=2.4049$. See Fig. 6.

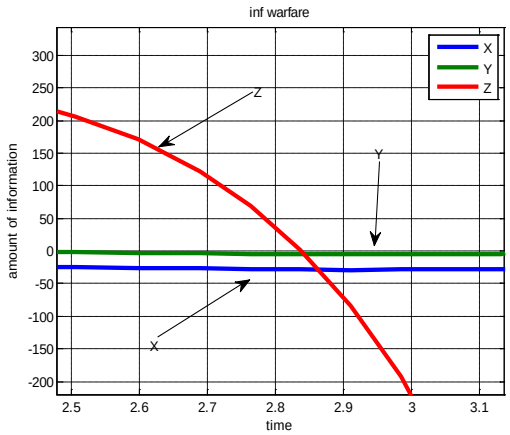

Fig. 6 Non-Preventive Information Warfare with second side Aggravation and first side Fading.

As we see from these data, besides increasing the value of peacekeeping activity, it has become

necessary to increase the level of third-party Information Technologies by 100 units.

4 Conclusion

The paper defines the concept of Non-Preventive Information Warfare and builds its mathematical model. Model problems of the Non-Preventive Information Warfare have been investigated by computer and mathematical methods and recommendations have been made for the peacemaking side to end this war. The cases of mutual fading and aggravation of the antagonistic party activity is considered in different modes. For the Non-Preventive Information Warfare with mutual fading, system controllability has been established; it has been revealed that to end the information warfare, much effort from the peacemaking side is not needed, except the situation during which the confrontation must end by the planned time.

For a Non-Preventive Information Warfare, with aggravation in different modes, the controllability of the system was established, and taking into account the time point τ , the tactics of the peacekeeping side were developed to end the Information Warfare.

References:

[1] Mikhailov A.P., Petrov A.P., Proncheva O.G., Marevtseva N.A. Mathematical Modeling of Information Warfare in a Society, *Mediterranean Journal of Social Sciences*, Rome-Italy, Vol. 6. No. 5 S2, 2015, pp. 27–35.

[2] Samarskiy A.A, Mikhailov A.P., *Mathematical modelling: Ideas. Methods. Examples*. 2nd ed. Correction. - M. FIZMATLIT. 2005.

[3] Chilachava T., Kereselidze N. *Continuous Linear Mathematical Model of Preventive Information Warfare*. Sokhumi State University Proceedings, Mathematics and Computer Sciences vol. 7. 2009, № 7. p. 113 – 141.

[4] Chilachava T., Kereselidze N. Non-preventive Continuous Linear Mathematical Model of Information Warfare. *Sokhumi State University Proceedings, Mathematics and Computer Sciences* vol. 7. 2009, № 7. p. 91 – 112..

[5] Chilachava T., Chakhvadze A. Continuous Nonlinear mathematical and computer model of information warfare with participation of interstate authoritative institutes. *Georgian Electronic Scientific Journal: Computer Science and Telecommunications* 2014| No. 4(44), p. 53 – 74.

[6] Mishra, B.K., Prajapati, A., Modelling and Simulation: Cyber war. Procedia Technology, vol. 10, 2013, Elsevier, Amsterdam, pp. 987-997.

[7] Kereselidze N. Mathematical model of information warfare taking into account the capabilities of the information technologies of the opposing sides. (In Russian). *Transactions II The International Technical Conference dedicated to the 90th anniversary of the Georgian Technical University "Basic Paradigms in Science and Technology", 21st Century*, Tbilisi, Georgia, September 19-21, 2012. Publishing House "Technical University", Tbilisi, 2012, p. 188-190.

[8] Kereselidze N. Mathematical model of information confrontation taking into account the possibilities of Information Technologies of the parties. (In Russian). *Proceedings of the XX International Conference Problems of Security Management of Complex Systems*. Moscow, December 2012, pp. 175-178.

[9] Kereselidze N. Combined continuous nonlinear mathematical and computer models of the Information Warfare. *International journal of circuits, systems and signal processing*, Volume 12, 2018, pp. 220-228.

[10] Kereselidze N. The Generalized Discrete Model of The Information Warfare with Restriction and The Problem of its Controllability. (In Russia). *Proceedings of the XXVI International Conference Problems of Security Management of Complex Systems*. Moscow, December 2018, pp. 33-39

[11] Kereselidze N. Discrete Systems of Information Warfare and Optimal Control Problem. *BULLETIN of TICMI*. Vol. 23, No 23, 2019, In The Press.

[12] Kereselidze N. An Optimal Control Problem in Mathematical and Computer Models of the Information Warfare. *Differential and Difference Equations with Applications : ICDDEA, Amadora, Portugal, May 2015, Selected Contributions. /Editors: Pinelas, S., Došlý, Z., Došlə, O., Kloeden, P.E. (Eds.), Springer Proceedings in Mathematics & Statistics*, 164, 2016, pp. 303-311.

[13] Kereselidze N. Chilker-type Mathematical and Computer Models in The Information Warfare. (in Russia). *Journal Information warfare's*. №2 (38). 2016, pp 18-25.

[14] Kereselidze N. Chilker type task for mathematical and computer model of information warfare of ignoring the enemy. *Proceedings of the XXIV International Conference Problems of Security Management of Complex Systems.* Moscow, December 2016, pp. 147-150.