Introduction to Methods of Modelling Information Wars as a 21st Century Threat*

Tomasz, Zawadzki[1], Tomasz Wałęcki[2], Halina Świeboda[3],
Ryszard Szpyra[4], M.Kuczabski[5], P.Stobiecki[6]

Abstract:

Purpose: Using System Dynamics approach together with Lanchester and SIR models for modeling information war. Theoretical considerations.
Approach: Due to the theoretical form of conducted research the main research methodso were a literature review and simulations based on developed model.
Conclusions: The result of the research is the model of information war based on System Dynamics approach. The model focuses on how socjety wealth and counterdisinformation campaings affect on war efficiency. One of the key conclusion from the simulations results is that one of the main goals of attacking side should be elimination or taking control over public media of attacked one.
Practical implications: The model of information war which was developed during the researche, gives a possibility to get new knowledge about war information procesess. It allows to predict causes and effects of disinformation campaings and helps to make proper decisions connected with countermeasuers that are taken. Presented article appoints directions which needs to be explored in connection with information wars.
Orginality: Presented researches are pioneerign and in such form on this field was not conducted so far. Using Lanchester equations, connected with epidemic spread model and System Dynamics approach they provide new knowledge about the phenomenon of information war.

Keywords: Information war, system dynamics, modelling, simulation.

JEL: C53, C63.

Paper type: Research article.

[1]Assistant profesor, Faculty of National Security, War Studies University, gen. Chruściela "Montera", Poland, e-mail: t.zawadzki@akademia.mil.pl;
[2]Phd student at the National Security Department, War Studies University,
e-mail: tom.walecki@gmail.com;
[3]Associate profesor, Faculty of National Security, War Studies University, gen. Chruściela "Montera", Poland, e-mail: h.swieboda@akademia.mil.pl;
[4]Professor, Faculty of National Security, War Studies University, gen. Chruściela "Montera", Poland, e-mail: r.szpyra@akademia.mil.pl;
[5]Assistant profesor, Faculty of National Security, War Studies University, gen. Chruściela "Montera", Poland, e-mail: m.kuczabski@akademia.mil.pl;
[6]Assistant profesor, Faculty of National Security, War Studies University, gen. Chruściela "Montera", Poland, e-mail: p.stobiecki@akademia.mil.pl;

1. Introduction

Information is playing an increasingly important role in the modern world. Its value increases proportionally to its level of strategic importance for companies and organizations as well as for governments, countries, and alliances. Moreover, in societies and economies based on knowledge, information becomes the basis of their functioning. As Krzysztof Liderman claims, "The basis for the operation of almost all modern companies and organizations, including organizations responsible for the functioning of the state itself, is the appropriate circulation of information. Interrupting this circulation or falsifying information causes losses: for companies this process may end in bankruptcy, and for the state - social unrest, disturbances in the national economy, and a decline in its reputation in the international forum" (Liderman, 2017).

The intensive development of technologies not only brings about essentially unlimited possibilities for information exchange but it also facilitates the emergence of new threats, including information and economic wars, which may bring about the massive destabilization of countries.

It was noted at the end of the previous century that modern society may be thought of as an information society. However, when this term was coined it was somewhat related to quick access to business information which presented certain organizations an advantage over their competitors. Through an observation of our present, it may be concluded that the term *information society* should be far more widely applied than it was in the recent past. The word *information* is for the most part associated with the worldwide web, especially social portals, television channels, and other kinds of electronic media.

The report published by the *We are social agency* and the *Hootsuite* platform shows the massive development of digital technologies, in particular social media (Table 1). The number of internet users around the world has increased by 400 million people compared to this time last year, this figure represents an annual growth of 10 percent which gives us an average rate of more than 1 million new users each day. A similar trend may be seen in social media, especially in the context of the users of mobile devices (Table 2).

Table 1. *Use of digital technologies around the world*

Total population	Uniqe mobile users	Internet users	Active social media users	Mobile social media users
7.734 bilion	5.155 bilion	4.479 bilion	3.725 bilion	3.660 bilion

Source: *https://wearesocial.com/blog/2019/10/the-global-state-of-digital-in-October-2019.*

The numbers presented in Table 1 and Table 2 clearly show that the Internet can be an attractive space for anyone who wishes to influence people to change their behaviour or thinking.

Table 2. *Annual digital growth*

Total population	Uniqe mobile users	Internet users	Active social media users	Mobile social media users
+1.0%	+2.4%	+10%	+9.6%	+15%
+79 milion	+123 milion	+416 milion	+328 milion	+476 milion

Source: *https://wearesocial.com/blog/2019/10/the-global-state-of-digital-in-October-2019.*

Although information cannot cause direct physical harm to either human or non-human beings or any other material things, during the last decade it has become a real weapon which has given rise to a wide range of possibilities. It has also turned out that the Internet is an excellent environment in which the conditions for the rapid dissemination of crafted content (their broadcasting around the world, duplication, editing out undesirable content, imposing one's own interpretation) have been created (Darczewska and Żochowski, 2017). It is important to note that by implementing the process above, one can remain anonymous and reach recipients directly, in real-time, bypassing all communication and information barriers and intermediaries in the transmission of content. This situation has been acknowledged by many countries that have recognized cyberspace as the fifth dimension of warfare.

2. Examples of Contemporary Information Wars

Offensive disinformation activities have long been one of the most important tools in the arsenal of active measures used by the Russian Federation, and even earlier by the Soviet Union (Szpyra, 2020). The main goal of these activities is to direct a particular opponent to implement the activities desired by Moscow. Given Russia's experiences outlined above, it may be assumed that their authorities are experts in the art of spreading disinformation in the online environment.

It is noteworthy that the Russians have formed military units with the sole purpose of conducting 'information operations', this was reported in February 2017 by the Minister of Defense of the Russian Federation - Sergei Szojgu. "Forces for information operations have been created, which are far more useful than what we previously designed and developed, and what was called counter-propaganda - said the minister, referring to the Soviet era. Propaganda should be intelligent, competent and effective - he added" (Wprost, 2020).

As J. Darczewska claims "[…] most Russian authors understand "information warfare" as the process of influencing the consciousness of the masses as a part of the rivalry between the different civilizational systems adopted by different countries in the information arena through the use of special means to control information resources as "information weapons" (Darczewska, 2014). Information war is a long-term and multidirectional process that uses many different attack vectors and impact areas. As Professor Igor Panarin notes (Panarin, 2012), the typical methods of information warfare include:

- Social control – influencing society.
- Social manoeuvring – the intentional control of the public aimed at gaining certain benefits.
- Information manipulation – using authentic information in a way that gives rise to false implications.
- Disinformation – spreading manipulated or fabricated information or a combination thereof.
- Fabrication of information – creating false information.
- Lobbying – influence by spokespersons in the interest of various political or economic groups
- Blackmail – the threat of revealing or publicizing either substantially true or false information about a person or people unless certain demands are met.
- Extortion of desired information - forcing entities to distribute specific information.

Russia runs disinformation campaigns using both the Internet (e.g. social media) and traditional media. These campaigns typically gain momentum especially during critical events such as elections, referendums or social conflicts. The presidential elections of the United States (Stobiecki and Kuczabski, 2020) or the protests of the 'yellow vests' in France may serve as examples of these activities (Wałęcki, 2020). Moreover, many of these campaigns are carried out by the citizens of the countries concerned, who are often unaware that the information they share comes from Russian sources. 'If the "toxic meme" is addressed to the appropriate recipient, they might disseminate it freely. These memes particularly appeal to Internet users who already feel marginalized and disempowered' (Cepa, 2019). It should be noted that Russian information war is based on three essential elements: traditional media, social media and the Internet, and also on supportive action, i.e. intensive cooperation with radical organizations or with fringe left-wing and right-wing political parties which share the Russian point of view. By using local actors as disseminators, Moscow considers that the content is more likely to be understood and shared. The phenomenon known as echo chambers is used here, these can amplify and reinforce disinformation and moreover, they make the Kremlin's activities more difficult to track down.

Another example of using prepared information campaigns to influence the public was observed during the Ukrainian crisis especially after the annexation of Crimea in 2014 by Russia or the events at Independence Square in Kyiv from November 2013 to February 2014. Although the Ukraine crisis first drew Western attention to the significance of Russia's information campaign, the Kremlin's use of disinformation long predates that crisis. Russian techniques have been growing in sophistication, intensity, reach and impact. Russian efforts are carefully orchestrated, thoughtfully targeted, generously funded and professionally produced (Cepa, 2014). Russians use fake social media accounts that simulate genuine ones to spread chaos by trolling the intended messages of other users by making fun of them or directing

insults at them and also bots are used which have the function of emulating human behaviour automatically. At the NATO summit in Wales in August 2014, General Philip Breedlove, the Supreme Allied Commander for NATO in Europe said that Russia was waging 'the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare' (Theatlantic, 2014).

A characteristic feature of Russian disinformation campaigns directed against Ukraine is their ability to adapt their message depending on the audience. One message will be directed at Western Europe (people in the east of Ukraine fighting for their independence) and another at Ukrainian citizens (encouraging anti-US and anti-EU sentiment) and still another at Russian citizens (connecting Ukrainian nationalism and German fascism). In order to make this content appealing, Russia is prepared to fabricate stories entirely, using photos and video footage to suit Russia's needs. A full range of media, from cinema to news, talk shows, print and social media are engaged in promoting official Russian narratives (Cepa, 2014). Hence, RT television broadcasts information about the celebration of holidays, organizes cultural events, or even presents recordings from the first marriage concluded in Novorossia.

On the other hand, the events in Kiev's Maidan were presented as a 'revolt against the authorities', 'coup', or the 'actions of a radical group' (Lakomy, 2014). As the authors of the study "Active measures. A Russian export commodity" (Darczewska and Żochowski, 2017) claims: "The effectiveness of the impact of the operations depends on the diagnosis of the balance of power, the political situation, but also on the prevailing political culture and the state of the social needs of the population. Such a diagnosis is based on the social engineering techniques used by the Russian services to oppose the elites and the wider society of the target country".

There is no doubt that the Internet has become a battlefield for the human perception of reality. We should build models to research in a more profound way how disinformation can be used to penetrate different echo chambers, how to identify bogus accounts in social media or measure the impact of bots and trolls on the opinions of the general public (Świeboda, 2019).

3. Basic Concepts of Information War Modelling

Modelling information warfare and predicting its behaviour will always be a challenging task due to the high degree of dynamics in such operations and the dozens of parameters that should be considered, this applies not only to field commanders but also to modellers. The main characteristic feature of war operations is that at least two opposing sides are engaged in them and each one significantly impacts the decisions and behaviour of the other side. In modelling, such a mutual influence is called *feedback*. This means that changing the state of object A has an influence on the state of object B, which is somehow connected with A, and in turn

the state of B can cause further changes to occur in the state of object A. Such an example of mutual influence is presented in Figure 1.

Figure 1. *Mutual influence of objects A and B. A affects B and B affects A.*
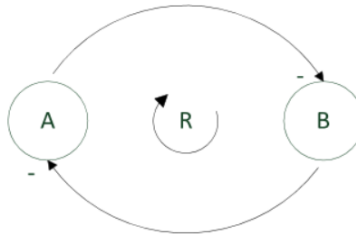
Source: *Own study.*

The theory of feedback loops has also been widely considered in control theory, which was developed over the decades by such great scientists as Euler, Lagrange, Laplace or Lyapunov. Each of them also made a significant contribution to the development of mathematical methods designed for dynamic systems modelling, called *calculus.*

Over the centuries, *calculus* methods have been widely used in mechanics because such systems stand out with their high degree of dynamics and many sources of feedback. That is one of the reasons why the first models of warfare were developed in 1916 by English car engineer Frederick Lanchester. He defined battle in the form of ordinary differential equations in two ways (Lanchester, 1916):

1. The first one, also known as the aimed fire model, assumes that each unit destroys enemy units in one unit time.
2. The second one assumes that both sides fire directly into the operating area (like artillery fire or bombardment) which is more appropriate to modern operations.

To date, the Lanchester models have been the subject of many research efforts, therefore the overall concept is a solid base for building information war models which are described later in the article. In contrast to traditional military operations which were carried out and then studied by researchers over centuries, information operations differ in many aspects. First of all, such a means of combat as information is characterized by:

1. It is abstract, unlike traditional weapons it has no physical effect.
2. Information does not have a direct physical impact on the enemy and cannot cause physical injuries.
3. Information may be used as many times as necessary.
4. It may have a delayed trigger.
5. In recent years, a situation has developed where all sorts of information may

be produced and published at a very low cost.
6. It has a very wide, even in the geographical sense, impact factor.
7. Information changes people's way of thinking and in the aftermath it changes their behaviour.

Due to the description listed above, it may be concluded without too much further consideration that for modelling information operations, the traditional Lanchester model is not sufficient. The main reasons for this are described in the following points above: 2, 4, 7 which generally state that information does not behave like traditional ammunition but rather, it has more of an influence on people's minds than on their physicality (e.g. injuries). An individual who is 'hit' by a piece of information will begin to process it (even unconsciously) depending on some external factors such as:

- Level of education
- Financial security
- Other information surrounding them

Then the person will take the final decision as to whether or not to believe the information. To put it in basic terms, the person is changing their state of mind from *undecided* – at the moment when they were "hit" by the information, to *aware* – the moment of consciously taking the decision. Such a transition from one way of thinking to another is well known and frequently used in the modelling of marketing campaigns.

Quite similar changes in the mindsets of people were defined by Kermack and McKendrick (1927) in their epidemic spread models. It is also worth emphasizing that the first concepts of mathematical modelling of infectious diseases were initiated by Bernoulli (1760). Kermack and McKendrick defined two models which are still used:

- SI from: *Susceptible – Infected;*
- SIR from: *Susceptible – Infected – Recovered;*
where:
- *Susceptible individuals* are uninfected but susceptible to the disease;
- *Infected individuals* can infect other susceptible individuals;
- *Recovered individuals* have recovered from the infection and are immune to reinfection.

Both of these models track the number of susceptible and infected individuals during the epidemic with the help of ordinary differential equations (ODE), while the SIR model additionally tracks the number of recovered ones.

While analysing changes to the individual's health status in the SIR model – from susceptible, through to infected to recovered – similarities to changes in decisions

states could be observed. A susceptible state corresponds to *undecided*, infected to *influenced* by the relevant piece of information, and recovered to taking a *conscious* decision about the information received. Due to the similarities observed, for information warfare modelling, the authors of the article combined two concepts:

- Lanchester war model;
- SIR epidemic spread model.

Because each of them, due to representing a highly dynamic system, is written in the form of ODE, such a combination would require considerable mathematical effort. To avoid complex mathematical calculations, the authors propose the use of System Dynamics which was introduced by Jay Forrester in the 1960s (Forrester, 1961). The key concepts of System Dynamics are:

- Finding relationships between key elements of the modelled dynamics system and discovering *feedback* loops.
- Representing the modelled system in the form of *stock and flow* diagrams instead of mathematical formulas.
- Machine transformation of *stocks and flows* diagrams into ODE and solving them through the use of numerical procedures.

An example of a feedback loop is presented in Figure 4, and the basic *stock and flow* diagram with its corresponding mathematical formula is presented in Figure 2.

**Figure 2.** *Stock and flow diagram with its corresponding mathematical formulas.*
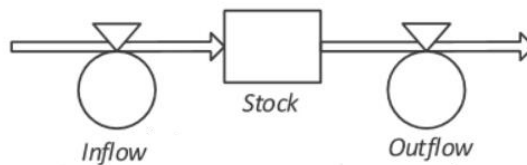
$$stock(t) = \int_{t_0}^{t} \left[inflow(s) - outflow(s) \right] ds + stock(t_0)$$

$$\frac{d(stock(t))}{dt} = inflow(t) - outflow(t).$$
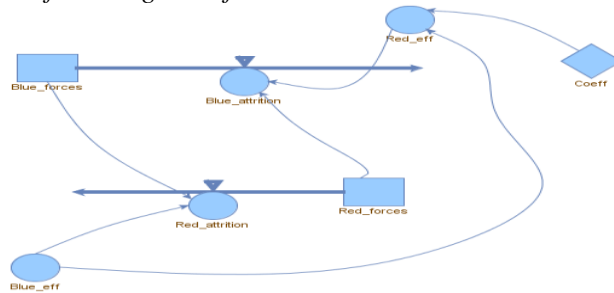
Source: *Own study.*

The System Dynamics approach which, due to its graphical representation, is much more straightforward to understand for modellers than raw mathematical formulas has become very popular in recent decades especially for modeling economic, environmental, social or other non-deterministic systems including war operations. Using the System Dynamics approach, feedback loops of Lanchester linear law are presented in Figure 3 and in the stock and flow diagram in Figure 4.

Figure 3. *Causal loop diagram of the Lanchester linear law.*
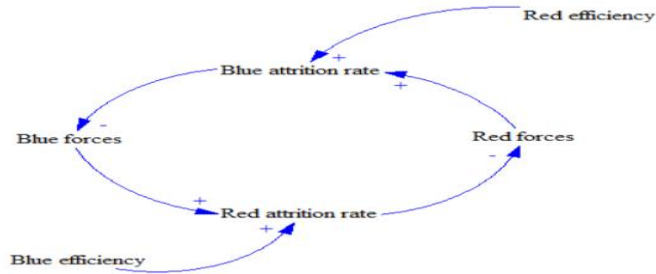
Source: Own study.

Figure 4. *Stock and flow diagram of the Lanchester linear law.*
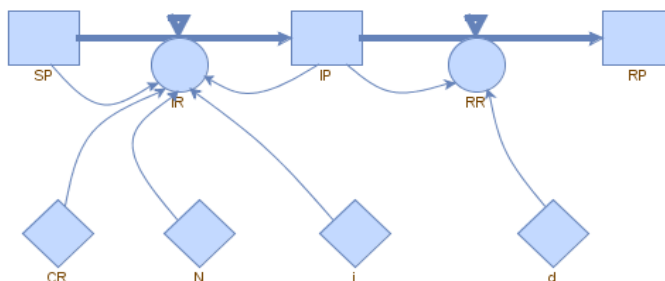

Source: Own study.

A simplified causal loop and a stock and flow diagram of a SIR model are presented in Figures 5 and 6 respectively.

Figure 5. *Simplified causal loop diagram of a SIR model.*

Source: Own study.

**Figure 6.** *Stock and flow diagram of a SIR epidemic model.*

Source: Own study.

4. Information War Basic Model

Having chosen the basic concepts and methodology for information war, the modelling authors of the article have identified the key elements of information war and have proposed its causal loop diagram which is presented in Figure 7.

Figure 7. *Causal loop diagram of an information war model.*
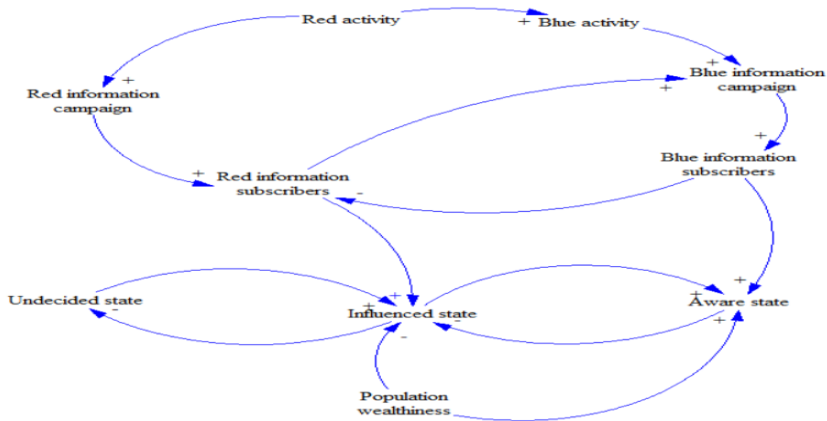
Source: Own study.

The authors assumed that information operations are carried out by two opposing sides with one referred to as *Red,* which is the attacking side and *Blue,* which defends its citizens from the influence of *Reds*.

The triggering element of the information war is a disinformation campaign started by the *Red* side. They start to publish in the available medias different kinds of information which are read and subscribed to by *Blue* society. If *Red's* information campaign is attractive enough the number of subscribers will increase and finally, more individuals will become affected and influenced by the *Red side*.

When the *Blue side's* administration discovers the *Red* disinformation campaign, they commence anti-disinformation operations. Such operations to encourage new subscribers must be at least as attractive as those carried out by the Red side.

Because *Blue's* administration dismisses information published by *Reds* or shows an alternative point of view of reality, individuals who were firstly influenced by *Red* propaganda start to think the matter over and depending on their material, educational and general wealth status, they become more aware of their surrounding reality and change their decisions. They also become more critical of *Red's* information and more trusting of the *Blue* point of view.

A stocks and flow diagram of the model described above is presented in Figure 8. It includes 10 stocks which means that 10 sets of ODEs are described.

Figure 8. *Stock and flow diagram of an information war model.*
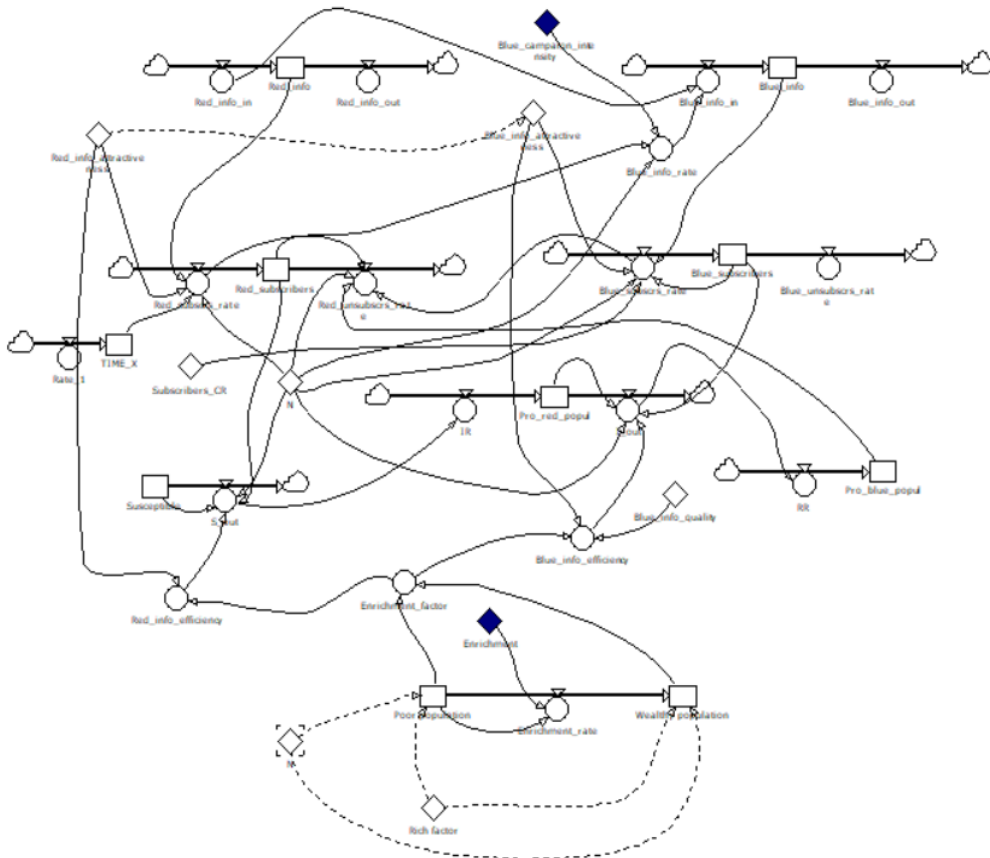
5. Simulation Results

Having created the model presented in Figure 8, the authors were able to run simulation experiments and go through different scenarios of information wars. As a numerical procedure, due to its speed and simplicity, the 4th-order Runge-Kutta was chosen. The authors made four experiments with different values of two variables:

- "Wealth factor" – which represents the status of individuals and is an average of their educational and wealth level, political, social and cultural maturity. The higher the "Wealth factor" is, the higher the average status of citizens in general and also the more developed the society
- "Blue campaign intensity" – shows the intensity of the information campaign carried out by the *Blue* (defending) side. A low value for this factor means that the *Blue* side has low resources and possibilities to counteract *Red's* propaganda. If the value of this factor is '0', it means that *Blue's* mass media are excluded from the information war (e.g. destroyed) or are totally in *Red's* hands.

In the first scenario, the authors assumed that the "Wealth factor" and 'Blue campaign intensity' are '0'. This means that the society is poor (Figure 9) with a low education level and low social and cultural awareness. There is also no anti-propaganda actions taken by the *Blue* side. As a consequence, individuals only receive information sent by the *Red* side and they do not have a broader perspective concerning the surrounding world. As a consequence, after some period of time all individuals become influenced by *Reds,* this is presented in Figure 10.
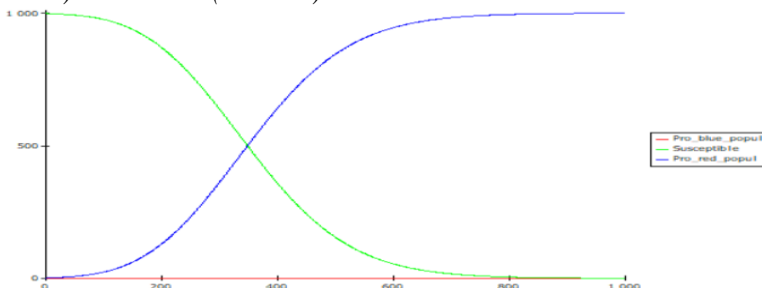
Figure 9. *The number of poor (green line) and wealthy individuals (red line). Source: own study.*
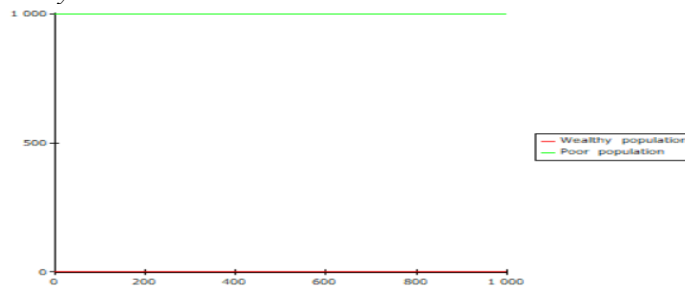
Source: Own study.

Figure 10. *The number of undecided individuals (green line), those influenced by Reds (blue line) and aware (red line).*
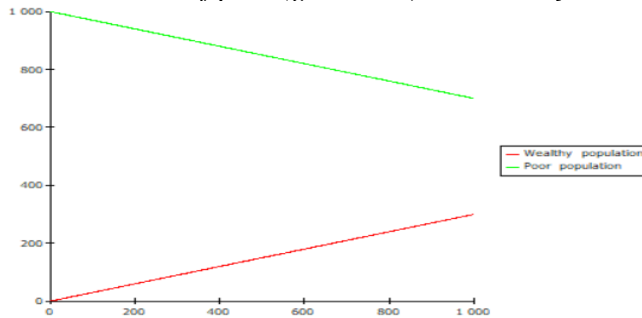

Source: Own study.

In the second scenario, the "Wealth factor" was increased to 0.3 and the "Blue campaign intensity" was held at level "0". As a consequence, the number of wealthy individuals started to grow linearly but because of a lack of anti-propaganda information society became influenced by *Reds* which is – with minor differences – similar to the first experiment. The results of this scenario are presented in Figures 11 and 12.

During the third, and last experiment, the authors left the value of the 'Wealth factor' at a level of 0.3 but in contrast to the previous simulation the value of the 'Blue campaign intensity' was increased to 10. This means that society is slowly developing and that the *Blues* have sufficient resources to counteract *Red's* propaganda. The results of this experiment are presented in Figures 13 and 14. The

last diagram shows that after some period of time the numbers influenced by *Red's* information begins to decrease and the number of aware individuals who agree with the *Blue* side starts to grow. In a practical sense, this means that the people who were given an alternative source of information received a broader perspective of reality and considered the information received with some degree of criticism which makes their decision more informed.

Figure 11. *The number of poor (green line) and wealthy individuals (red line).*
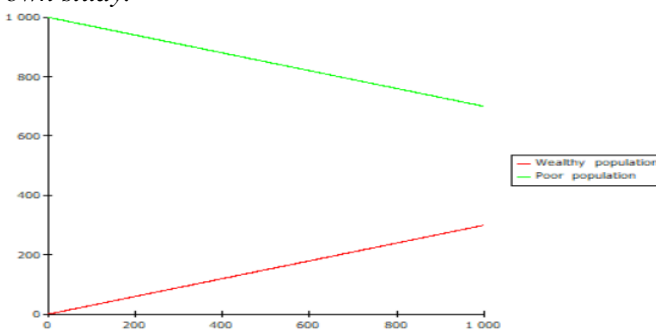

Source: Own study.

Figure 12. *The number of undecided individuals ((green line), those influenced by Reds (blue line) and aware (red line).*
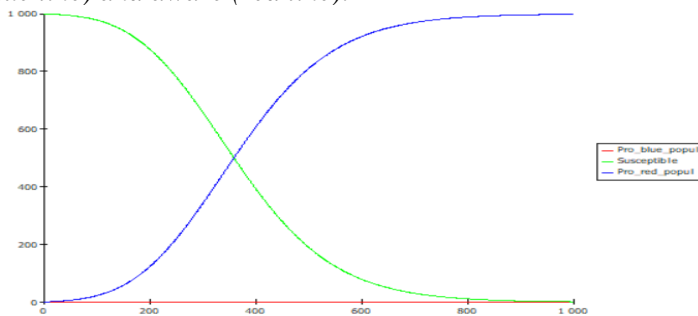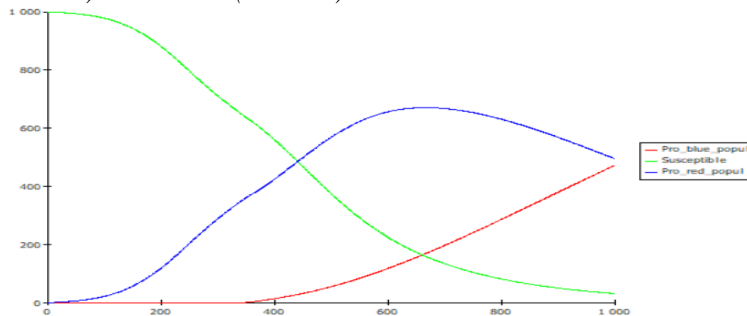

Source: Own study.

Figure 13. *The number of poor (green line) and wealthy individuals (red line). Source: own study.*

Source: Own study.

Figure 14. *The number of undecided individuals (green line), those influenced by Reds (blue line) and aware (red line).*

Source: *Own study.*

6. Conclusions

Generally speaking, war is a complicated subject to model in a formal sense due to the large number of parameters that are described, and by the dynamic changes of these parameters. Both now and in the past, many techniques have been used to model war operations, for example, probability theory, expert appraisal theory, Markov chains (Novikov, 2013) but the most famous and widespread one is the Lanchester model, which employs ODE used to model dynamical systems. With the development of computing technology the simulation methods approach based on differential equations became popular due to its increasing efficiency.

Information operations are a special kind of war operation because information is abstract and has no real identity. Because information affects the individual's mind rather than their body, it is difficult to model their impact. During their research, the authors discovered similarities between the spread of an epidemic and changes to the state of mind of individuals affected by the information campaign, they tried to adapt the epidemic model to the information war model. In order to avoid the deep mathematical analysis related to differential equations, which are the foundations of both the war and epidemic spread models, System Dynamics techniques were employed. Three different approaches were connected:

- Lanchester's model.
- Epidemic spread model.
- System Dynamics methodology.

The authors successfully built a basic model of information war and obtained satisfactory results, which revealed two key factors affecting information war efficiency: the wealth of the general society and anti-propaganda campaigns. In cases where the society is relatively poor, which means that in general the people are probably poorly educated and have a low level of political awareness, the resources for counteracting disinformation are not sufficient and as a result, propaganda activities become very efficient.

Based on the simulation results, it may be concluded that from the point of view of the attacking side, in order to eliminate anti-propaganda campaigns, it is well worth making an effort to seize control over the mass media of the target country. The destabilization of the economy could also be a worthwhile objective because relatively poor individuals may be influenced more easily.

References:

Bull, O.M. 2010. System Dynamics Applied to Combat Models. Proceedings of the 28th International Conference of the System Dynamics Society, Seoul.

Choucri, N., Goldsmith, D., Madnick, S.E., Mistree, D., Morrison, J.B., Siegel, M.D. 2016. Using System Dynamics to Model and Better Understand State Stability. Warszawa.

Darczewska, J. 2014. The anatomy of Russian information warfare, The Crimean Operation, case study. Warszawa.

Darczewska, J., Żochowski, P. 2017. Active measures. Russian export goods, Center for Eastern Studies. Warsaw.

Forrester, J. 1961. Industrial dynamics, Cambridge, MIT Press.

Forrester, J. 1969. Urban dynamics, Cambridge, MIT Press.

Forrester, J. 1971. World dynamics, Wright-Allen Press.

https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/.

https://www.wprost.pl/swiat/10043936/rosja-przyznaje-sie-do-prowadzenia-wojny-informacyjnej-propaganda-musi-byc-skuteczna.html (access: 10.01.2020r).

Lakomy, M. 2015. Cyberspace as a new dimension of competition and cooperation between member states. Wydawnictwo Uniwersytetu Śląskiego. Katowice.

Lanchester, F.W. 1956. Mathematics in Warfare. The World of Mathematics, Vol. 4, Eds. Newman, J.R., Simon, S., Schuster, S., 2138-2157.

Liderman, K. 2017. Information security. New Challenges, PWN, Warszawa.

Lucas, E., Pomerantsev P. 2015. Winning the Information War Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. https://cepa.ecms.pl/files/?id_plik=2706.

Meadows, D., Randers, J. 2005. Limits to Growth: The 30-Year Update. Warsaw.

Novikov, D.A. 2013. Hierarchical Models of Warfare. Automation and Remote Control, Vol. 74, No. 10, 1733-1752.

Panarin, I. 2012. World War II information war - war against Russia. Warsaw.

Pytlak, R., Tarnawski, T., Fajdek, B., Stachura, M. 2014. Interactive dynamic optimization server–connecting one modelling language with many solvers. Optimization Methods & Software, 29, 1118-1138.

Pytlak, R., Zawadzki, T. 2009. Dynamic modeling and supply chain process control. Economy and efficiency, Politechnika Poznańska.

Pytlak, R., Zawadzki ,T. 2014. On solving optimal control problems with higher index DAEs. Optimization Methods & Software, 29, 1139-1162.

Pytlak, R., Zawadzki, T. 2010. Application of dynamic modeling to supply chain research. Economy and efficiency, Politechnika Poznańska.

Skribans V. 2012. European Union Economy System Dynamic Model Development. Proceedings of the 30th International Conference of the System Dynamics Society, St. Gallen.

Sterman, J.D. 2000. Business dynamics, systems thinking and modeling for a complex world. The McGraw-Hill Companies, Inc.

Stobiecki, P., Kuczabski, M. 2021 in press. Analysis of threats during the election campaign and parliamentary elections in 2019. In: Social control rooms in the era of information war, ed. Świeboda, H., ASzWoj, Warsaw.

Szpyra, R. 2020. Russian information offensive in the internaltional relations. Security and Defence Quarterly, vol. 30, no. 3.

Świeboda, H. 2019. Actions in the information war against the state and the possibilities of defense. In: Between knowledge and power, (ed.) P. Bajor, A. Gruszczak, Księgarnia Akademicka, Kraków.

Wałęcki, T. 2021 in press. The influence of the Russian disinformation machine on the "yellow vest" movement. In: Social control rooms in the era of information war, ASzWoj, Warsaw.

Yamashita, T. 2011. A System Dynamics Approach to the Regional Macro-economic Model. Proceedings of the 29th International Conference of the System Dynamics Society, Washington D.C.

Zawadzki, T., Pytlak, R. 2011. Extending System Dynamics approach to higher index DAE's. Conference proceedings, System Dynamics Society, Washington.