Qeios

Protection of Complex Network Systems From Targeted Attacks and Non-Target Lesions

Olexandr Polishchuk

Laboratory of Modeling and Optimization of Complex Systems
Pidstryhach Institute for Applied Problems of Mechanics and Mathematics, National Academy of Sciences of Ukraine, Lviv, Ukraine
od_polishchuk@ukr.net

Abstract. A comparative analysis of structural and flow approaches to study the vulnerability of complex network systems (NS) from targeted attacks and non-target lesions of various types is carried out. Typical structural and functional scenarios of successive targeted attacks on the most important by certain criteria system elements are considered, and scenarios of simultaneous group attacks on the most important NS's components are proposed. The problem of system lesions scale from heterogeneous negative influences is investigated. It was confirmed that the flow approach allows us to obtain a much more realistic picture of such lesions consequences. It is shown that the scenarios of group targeted attacks built on the basis of on NC flow model are more optimal from the point of view of selecting attack targets than structural ones.

Keywords – complex network, network system, vulnerability, targeted attack, non-target lesion, core, centrality, influence, betweenness.

1. Introduction

Over the past 5 years, humanity has faced two global challenges – the Covid-19 pandemic and the Russian-Ukrainian war. These events and resulting comprehensive sanctions against the aggressor country are vivid examples of targeted attacks and non-target lesion of almost all spheres of human activity [1, 2]. Lesions of real systems can be local, group, and system-wide, and local can develop into group, and group – into system-wide [3]. They can be predictable and unexpected, centralized and decentralized, when the damaged element itself becomes a source of lesion, spread with different speed – from almost instantaneous (cascade phenomena) to those that last for decades (global warming, the spread of AIDS) [4, 5], etc. Despite the diversity of real systems and the variety of types of negative influences on them, targeted attacks and non-target lesions can have much common both in the methods of action and the consequences of such influences: the spread of dangerous infectious diseases (DID) and computer viruses, traffic jams and DDoS attacks, shelling of populated areas and earthquakes, and so on.

https://doi.org/10.32388/RH65Y6

Currently, the main attention of researchers in the theory of complex networks (TCN) is focused on the development of protection strategies against successive targeted attacks on the most structurally important nodes of network systems [6, 7]. Much less attention is paid to the creation of attack scenarios on the operation process of such systems. Undoubtedly, damage to the structure affects this process, but it is possible to destabilize or even stop of the system functioning even with an intact structure (during the Russian-Ukrainian war the air transport system of Ukraine completely stopped its activity only because the threat of downed planes). Another shortcoming of the structural approach to NS vulnerability analysis is the evaluation of lesion scale [8]. Directly damaged objects are actually destroyed elements that must be removed from the system structure. Only of the network system nodes adjacent to the directly damaged can reasonably be considered consequentially injured. This approach is quite acceptable for assortative networks [9]. However, for disassortative NSs, which include the majority of man-made systems and the elements of which are connected by paths, this approach does not fully reflect the entire set of victims as a result of targeted attack or non-target lesions of system elements. Only the objective comprehensive evaluation of real picture of negative influence consequences, which combines all directly damaged and consequentially injured system elements, will make it possible to more accurately classify the type of this influence and quantify the damage caused by it.

One of the ways to protect the system is neutralization the source of negative influence, in particular, a counterattack against it (sanctions against the aggressor country, destruction of agricultural pests, cessation of terrorist and hacker groups activities, vaccination [10, 11], etc.). The problem of optimizing the scenarios of such attacks, as well as the development of effective countermeasures against non-target lesions, is also paid a little attention so far, although the party that initiates and carries out such counterattack, for example, imposes sanctions against the aggressor country or quarantine measures during epidemics of DID, also bears considerable losses. In order to at least partially solve the problems listed above, the article proposes a flow approach to the vulnerability analysis of NS operation process and shows its advantages over the structural approach when evaluation the real losses caused by negative influence on the system, as well as optimizing the scenarios of targeted attacks on it.

2. Attacks on the structure of network system

The mathematical model of complex network (CN) G=(V,E), where V is the set of nodes of network G and E is the set of connections (edges) between them, is the adjacency matrix $\mathbf{A} = \{a_{ij}\}_{i,j=1}^{N}$. Here N is the number of elements of the set [12]. The value a_{ij} of matrix $\mathbf{A}$ is equal to 1 if there is connection between nodes n_i and n_j (such nodes are called adjacent), $i, j = \overline{1, N}$, and is equal to 0 if there is no such connection. It is also assumed that the nodes do not have loop connections, i.e. the diagonal elements of matrix **A** are zero.

No large-scale complex system can protect all its elements [13, 14]. Therefore, the problem arises of determining those NS nodes that must be protected first of all. To solve this problem, the concept of centrality is used as an importance indicator of node [15, 16]. The main local characteristics of a binary directed network node are its input and output degrees [12] or degree centrality. Here, by local we mean a characteristic that describes the properties of element itself or one or another aspect of its interaction with adjacent system elements. The input degree of node determines the number of edges that "enter" it, and the output degree – the number of edges that "leave" from a given node to adjacent NS nodes. Characteristics of element that describe one or another aspect of its interaction with all other elements of this system will be called global. Global centralities allow us to determine the importance of node in the network as a whole. However, the concept of "importance" can have different meanings, which has led to the appearance of many definitions of the term "centrality", namely betweenness, closeness, eigenvector, Freeman and many others [16, 17] (there are about 20 of them in total). At the same time, the value of one centrality may contradict another, and the centrality important for solving one problem may be insignificant for another [18], which introduces some ambiguity when they are used as importance indicator of element in the system structure.

Usually, an attack in TCN refers to actions aimed at intentionally removing from the system structure a certain number of the most important nodes based on the chosen centrality in order to change the structural network properties [19]. Since the system lesion is usually carried out by successive or simultaneous damage to its elements, the first step in formation of its protection methods consist in construction the so-called scenarios of targeted attacks on the network system [6, 16]. The most effective scenarios of such attacks are formed when their developer "puts himself" in the place of "attacker", who tries to cause maximum damage to the attacked system with minimal means. The development of each scenario should be preceded by the development of attack success criteria. From a structural point of view, such criteria can be the division of complex network into unconnected components, increase of average length of the shortest path [16], and so on.

The structural scenarios of NS lesions developed so far, which can be divided into two main groups, are based on the use of above-mentioned centralities of nodes in the system structure (generalized degree centrality, as the sum of input and output degrees of node in directed CN, centralities by betweenness, closeness, eigenvalue, and so on) [16, 20]. Each of scenarios of the first group begins with ordering a set of NS nodes according to decreasing values of their centrality of selected type and subsequent sequential removal of nodes from the structure according to this order until the attack success criterion is met. The scenarios of this group do not involve changing the centrality values of nodes that remained in the network. In the second group of scenarios, it is taken into account that with each removal of node, the structure of NS changes due to the establishment of new connections between the remaining nodes. This requires a new ordering of the sequence of NS nodes according to the changed values of their centrality of selected type. The next step in this scenarios group removes a node from the beginning of newly created list that takes these changes into account. It is obvious that the typical scenarios described above do not determine specific ways to protect a real system, which depend on its type and kind of negative influence, however, these scenarios make it possible to identify the elements that must be primarily protected from the point of view of their importance in the NS structure.

In general, three types of interrelated problems appear to protect network systems from various negative influences, namely: analysis of real and potential threats and the development of effective means of protection against them *before* lesion, provision of ways to counteract the spread of negative influences and minimize their consequences *during* lesion, and evaluation of consequences and restoration of the structure and operation process of the system *after* its lesion. After all, the better the system is protected, the weaker the effect of negative influence, and therefore the smaller its consequences. To solve the first of these problems, the considered above typical scenarios of targeted attacks can be used, and for the second and third, the structural model of network system can be applied. Obviously that all changes occurred in structure and operation process of the system should be immediately reflected in its structural and flow models. Then the difference between the rank of matrix **A** before lesion and the rank of this matrix during (after) lesion determines the number of nodes destroyed during (after) it in the source NS structure. The difference between the number of non-zero elements of structural model of network system before the lesion and the number of non-zero elements of matrix **A** during (after) damage determines the number of edges destroyed during (after) it in the source NS structure. Thus, the comparison of structural models of network system makes it possible to draw up a sufficiently objective quantitative picture of the level of damage to the system or its separate components as a result of targeted attack or action of non-target lesion. At the same time, along with the integral damage indicators (the total number of destroyed network nodes and edges), the structural model allows us to analyze the lesion of each NS's element. Thus, zeroing the element of matrix **A** indicates the removal (destruction, blocking) of corresponding edge from NS structure, zeroing of all elements of row and column of matrix **A** – the removal of corresponding node from this structure, reducing the generalized degree of node – decreasing the number of its interactions with other system elements. In general, the structural model allows us to reproduce the picture of all directly damaged and part of consequentially injured NS elements. The ratio of number of directly damaged to the number of attacked system elements is an objective indicator of its protection against the negative impact of a certain type. The main drawback of structural approach to evaluation the lesions consequences is that only elements adjacent to the directly damaged nodes of the network system can be considered consequentially injured (Fig. 1, directly damaged NS nodes are marked in black; gray – adjacent to directly damaged (consequentially injured) nodes; white – undamaged nodes of the network system; the continuous curve delimits the directly damaged NS domain; the dashed curve delimits domain of consequentially injured network system elements).

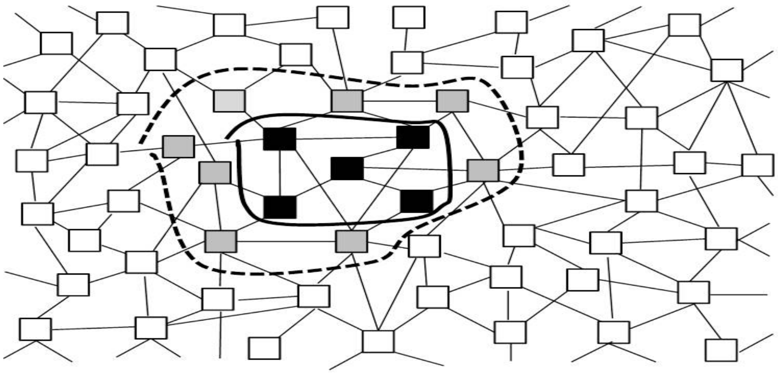


Fig. 1. Evaluation of the consequences of targeted attack based on the structural model of network system

It is obvious that simultaneous group attacks or non-target system lesions are much more difficult than successive attacks on most important NS elements, both from the point of view of its protection and overcoming the consequences. We divide simultaneous group negative influences into one-time (Al-Qaeda attack on the USA on September 11, 2001), repeated (18 missile strikes on Kyiv in May 2023) and successive (attacks on transformer stations of the Ukrainian power system in 2022-2024). Repeated group attacks are carried out regularly at certain time intervals on the same system objects. Consecutive group attacks differ from repeated attacks by changing the targets. A particular danger is that successful sequential group attacks can lead to system-wide NS lesions, for example, a prolonged blackout in the country. In the case of targeted attacks, this separation is often determined by the attacker's ability to launch subsequent massive attacks and the ability of attacked system to effectively defend and counter them. It is clear that each of above types of attack requires the development of specific type of scenarios for its most likely implementation. The simplest scenario of one-time group attack is obviously implemented by an attempt to simultaneously defeat a group of the most important NS elements according to determined centrality. The repeated attack scenario is realized by an attempt to damage a preselected and previously attacked, but not destroyed, group of network system elements. A sequential group attack scenario involves the consecutive execution of following steps:

1) compile a list of groups of NS nodes (subsystems) in order of decreasing indicators of their importance in the system, selected according to a certain feature;

2) delete the first group from the created list;

3) if the criterion of attack success is reached, then complete the execution of scenario, otherwise go to point 4;

4) since the structure and operation process of the system changes as a result of removal of a certain group of nodes (and their connections), compile a new list of groups in order of decreasing recalculated indicators of their importance in the NS and proceed to point 2.

If, during the implementation of last scenario, a certain group of nodes contains too many elements that the attacker is unable to hit at the same time, then such group is divided into the minimum number of connected subgroups available for such attacks (the Russian aggressor during the attacks on Ukraine launched not more 100-150 missiles each and UAVs at the same time, but not 500 each due to a lack of appropriate resources). In addition, the execution of scenario may terminate when the attacking party has exhausted the resources to continue the attack. It follows from the above scenarios that the main way to increase their effectiveness is to choose importance indicators of group in network system, the lesion of which will cause it the greatest damage [21]. The most obvious way of such choice is to form a list of NS nodes in order of decreasing the values of their centrality of selected type and form a group from the first nodes of this list, the number of which is determined by the ability of attacker to carry out a simultaneous attack on them. The second method is based on the principle of nested hierarchy of the network system [22]. The method proposed by us consists in applying the concept of k-core of CN, as the largest subnet of source network, the centrality of which, according to the generalized structural degree of nodes, is at least k >1 [23]. This method is based on the use of the most structurally important components of network and obviously fits into the above scenario of successive group attacks. In particular, groups are initially selected for the maximum value k for a given CN, which is then sequentially reduced until the attack success criterion is met.

3. Attacks on operation process of network system

To determine the functional importance indicators of separate NS components, we will use its flow model [3]. By a flow that passes through a network edge, we mean a certain positive function correlated to this edge. This function can reflect the flow density at each point of the edge or the volume of flow that is on the edge at the current moment of time $t \geq 0$, or the total volume of flow that has passed through the network edge up to the current moment for a certain period of time T>0, etc. Let us display the set of flows that pass through the NS edges in the form of flow adjacency matrix $\mathbf{V}(t)$, the elements of which are determined by the volumes of flows that have passed through the edges of complex network G for the period $[t-T, t]$ up to the current moment in time $t \geq T$:

$$\mathbf{V}(t) = \{V_{ij}(t)\}_{i,j=1}^{N}, \quad V_{ij}(t) = \widetilde{V}_{ij}(t) \Big/ \max_{l,m=\overline{1,N}} \widetilde{V}_{lm}(t), \quad i,j = \overline{1,N},$$

in which the values $\widetilde{V}_{ij}(t)$ are equal to the real volumes of flows that passed through the edge (n_i, n_j) , $i, j = \overline{1, N}$, of the complex network during the time interval $[t - T, t]$, $t \geq T$. It is obvious that the structure of matrix $\mathbf{V}(t)$ coincides with the structure of matrix $\mathbf{A}$. The elements of flow adjacency matrix of the network system are determined on the basis of empirical data about movement of flows through its edges. Currently, with the help of modern means of information extraction, such data can be easily obtained for many natural and the vast majority of man-made systems (transport, energy, financial, information, and so on) [24]. It is clear that the NS flow model described above is not its mathematical model in the usual sense of the word, but it gives a sufficiently clear quantitative picture about the operation process of network system, allows us to analyze the features and predict the behavior of this process, as well as evaluate its effectiveness and prevent existing or potential threats [25]. At the same time, the more extreme the situation in which the system is, the smaller the value T should be chosen.

Another, compared to the structural, and often much more effective and easier to implement method of attack consists in destabilizing or stopping the operation process of separate components or the system at a whole without directly destroying its elements – significantly reducing or stopping the movement of flows through the network, creating conditions for critical loading of the paths of movement of these flows, blocking of separate nodes – generators, transitors and/or final receivers of flows, desynchronization of flows movement through the network, etc. The construction of scenarios of successive targeted attacks on the most functionally important system elements is carried out according to the same principles as typical structural ones, with the difference that as importance indicators of NS nodes are used the characteristics that determine the role of NS elements in the process of its functioning as generators, final receivers and transitors of flows [3]. Structural and functional approaches to building scenarios of targeted attacks on the system can be combined. For example, if there are groups with the same values of a certain type of functional centrality in the sequence of NS nodes, they can be ordered by the values of selected type of structural centrality and vice versa.

The difference between the sum of elements of the matrix $\mathbf{V}(t)$ before lesion and the sum of elements of this matrix during (after) lesion can be used as an integral indicator of losses caused to the network system by a certain negative influence. This indicator determines the total decrease in the volume of flows in NS as a result of such influence. At the same time, along with integral indicators, the flow model makes it possible to analyze the damage of each network element. Thus, the zeroing of matrix $\mathbf{V}(t)$ element indicates the removal (destruction, blocking) of corresponding edge from the operation process of network system, the zeroing of all elements of the row and column of matrix $\mathbf{V}(t)$ that correspond to a certain node of NS – the removal of this node from the system operation process. It is obvious that these NS's elements are determined using the structural model of network system too. A decrease of the value of matrix $\mathbf{V}(t)$ element is a sign of decrease in the volume of flows that pass through the corresponding edge, and decrease in the value of the sum of elements in a row and column that correspond to a certain node of network system indicates a decrease in the volume of flows that are generated, received and transited through this NS's node. In general, the flow model makes it possible to reproduce the picture of not only destroyed, but also all consequentially injured nodes and edges of network system and to quantify the level of lesion, which is an additional advantage of this model. In fig. 2 shows the consequences of targeted attack on the network system, obtained on the basis of its flow model (in black are marked the directly damaged NS's nodes; in gray – nodes, the volume of flows from (to, through) which decreased as a result of attack (consequentially injured nodes); in white – undamaged nodes of network system; continuous curve delimits the directly damaged NS domain; the dashed curve is adjacent to the directly damaged domain of network system; the dotted curve is the consequentially injured NS's domain). As follows from fig. 2, the domain of consequentially injured NS elements determined on the basis of flow model can be much larger than domain of adjacent to directly damaged nodes of network system determined on the basis of its structural model. Thus, the comparison of NC flow models before, during, and after negative influence allows us to draw up a sufficiently objective quantitative picture of the level of lesion of network system or its separate components as a result of targeted attack or the action of non-target lesion. The ratio of number of directly damaged to the number of attacked elements of the system is an objective indicator of its protection against attacks or lesions of a certain type. The concept of system sensitivity to consequences of negative influence can be determined as the ratio of number of directly damaged to the number of indirectly affected elements. It is obvious that the closer the value of this indicator is to zero, the more sensitive the system is to negative influences, since a small number of directly damaged generates a large number of consequentially injured NS's elements.

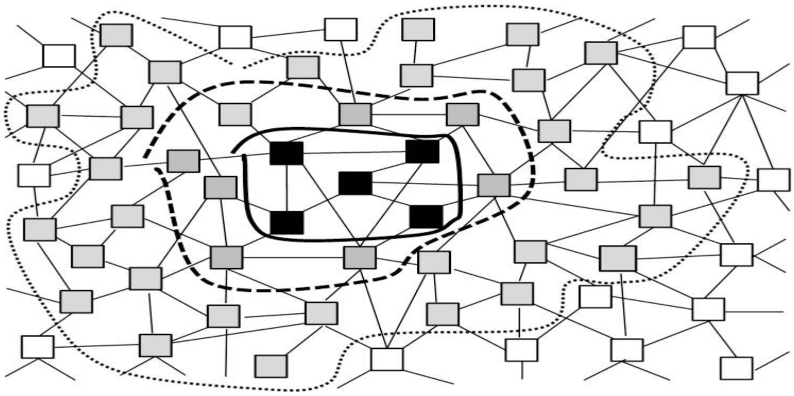


Fig. 2. Evaluation of a targeted attack consequences on the basis of NS flow model

On the basis of flow model, we can determine such global characteristics of NS nodes as input and output parameters of their influence on the system, as well as betweenness parameters [3]. Namely, the input (output) strength of influence of the node – final receiver (generator) of flows is considered to be the total volume of flows that were received (generated) in this node during the period $[t-T,t]$; the input (output) domain of influence of the node – final receiver (generator) of flows is considered to be the set of NS nodes, in which the flows directed to (from) it were generated (finally received) during the period $[t-T,t]$; the input (output) power of influence of the node – final receiver (generator) of flows is equal to the number of elements of input (output) domains of influence of this node, respectively. The measure of betweenness of the node is considered to be the total volume of flows that passed through it in transit during the time period $[t-T,t]$, $t \geq T$; the domain of betweenness of the node is the set of NS nodes that directed and received flows through this transit node, and the power of betweenness is the number of elements that make up the domain of betweenness. In general, after lesion of certain NS node, the combination of domains of its influence and betweenness fully determines the totality and number of all system elements indirectly affected as a result. In fig. 3 shows the consequences of targeted attack on the network system based on analysis of behavior of influence and betweenness parameters of network system elements (the directly damaged NS nodes are marked in black; the gray squares are the nodes adjacent to the directly damaged nodes; the gray diamonds, triangles and circles are the consequentially injured generators, final receivers and transitor nodes, respectively; the continuous curve delimits the directly damaged domain of network; the dotted curve represents the consequentially injured domain of network).

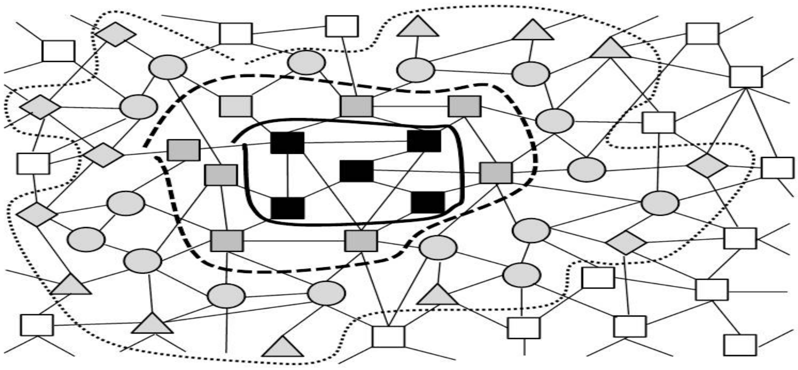


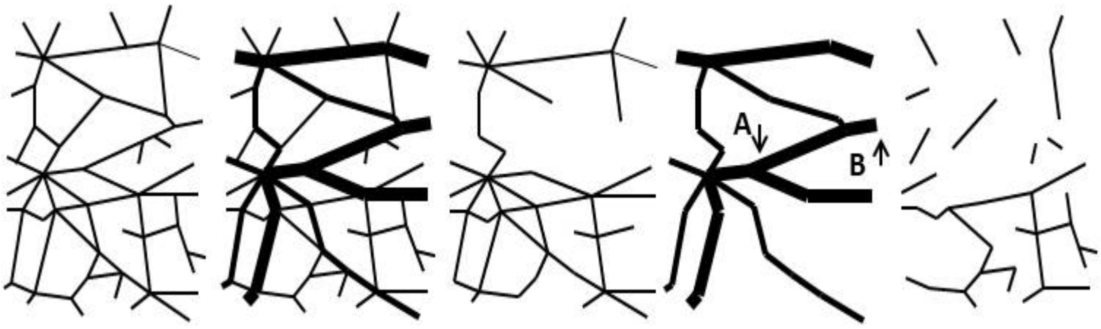
Fig. 3. Evaluation of consequences of targeted attack based on the analysis of influence and betweenness parameters of NS's nodes

Comparing fig. 1, 2, and 3, it can be reasonably concluded that the flow approach makes it possible to create a much more realistic picture of lesions consequences caused by a certain negative influence than the structural one. The importance of analysis of generator, final receivers, and flow transitor nodes lesions is explained by the fact that they require the search for new suppliers, consumers and alternative paths of flow movement, which is usually a rather difficult problem, especially in the case of mass NS lesions. During the development of scenarios of simultaneous group attacks, as a functionally most important component of the network system, the concept of its flow λ-core [21] can be used, as the largest subsystem of source system, elements of flow adjacency matrix of which have values not less than $\lambda \in [0, 1]$. It is obvious that the larger the value λ, the more important from a functional point of view NS's components are reflected by its λ-core. They can become one of the primary targets of simultaneous group attack, the scenario of which was given in the previous section. Similarly, as for NS elements, we can determine the parameters of influence and betweenness of its λ-core, which significantly deepens the analysis of lesions of network system.

4. Optimization of targeted attack scenarios

It was mentioned above that one of the ways to protect the system is to counterattack the attacker. In the case of Russian aggression against Ukraine, this means financial and economic sanctions, counterattacks to liberate the territories of country seized by the aggressor, the destruction of its combat units, logistics hubs and military command centers, etc. It is clear that the organizers of such counterattacks also suffer considerable losses. That is, the problem of optimizing attack scenarios arises, namely, how to destroy or block the operation of minimum number of nodes of attacked system, to cause it the greatest possible damage. A similar situation is observed during the development of scenarios for combating the spread of non-target lesions, for example, epidemics of dangerous infectious diseases (Covid-19). In particular, how to minimize the volume of movement of passenger flows through the network by blocking the smallest possible number of nodes that ensure the movement of these flows. Obviously that it is advisable to take into account not only the magnitude of direct negative influence, but also the magnitude of indirect lesion consequences. Above, for the construction of simultaneous group attacks scenarios, it was proposed to use the concepts of structural k- and flow λ-core of network system. We will show that the use of flow λ-cores compared to structural k-cores of NSs is significantly more effective when building scenarios of targeted attacks, both from the point of view of possible lesion to the most functionally important NS's elements, and for the purpose of optimizing these scenarios in terms of the number of attack objects. Let's consider the railway transport system (RTS) of the western region of Ukraine. In fig. 4a shows the structure of this system, and in fig. 4b – the same structure, but in the form of weighted network, which schematically displays the volumes of cargo flows that passed through its edges during 2021 (the thickness of lines is proportional to the volumes of flows). Note that this network contains 354 nodes in total, but in fig. 4a-b, only 29 nodes and 62 edges are displayed (transit nodes with a structural degree 2 are not shown, and an edge is considered to be a line that connects two nodes with a degree greater than 2). In fig. 4c contains the structural 4-core of RTS, which includes

12 nodes and 35 edges, and in fig. 4d is its flow *0.8*-core, which contains 4 nodes and 12 edges. One of the main disadvantages of k-cores compared to flow cores is the possibility of excluding functionally important components of the network system (path A-B in fig. 4d).



a) b) c) d) e)

Fig. 4. Examples of the structure (a), operation process (b), structural 4-core (c), flow *0.8*-core (d), and the addition to flow *0.8*-core in the source structure (e) of railway transport system of the Western region of Ukraine

It is obvious that the flow *0.8*-core reflects a functionally more important subsystem of RTS and the target of group attack on it is a much smaller number of nodes than 4-core of corresponding structure. Easy to see that in both cases, a successful attack on NS nodes selected with the help of k- and λ-cores will lead to actual termination of its operation process, as it divides RTS into unconnected components (fig. 4e), but in the second case, the goal of attack is achieved with significantly less efforts (three times in terms of number of nodes and edges). Thus, the flow approach makes it possible to build scenarios that are much more optimal from the point of view of attacking side's efforts than the structural one. By analyzing the parameters of influence and betweenness of *0.8*-core of given RTS fragment, it was established that all elements of this fragment will be indirectly damaged by a successful targeted attack on it.

In monograph [3], the scenario of combating non-target lesion (Covid-19 pandemic spreading) was considered, which consisted in granulation of network, that is, its successive division according to the principle of nesting [22] into subnets, the connections between elements of which become significantly weaker or completely blocked, than before the lesion. However, such scenario simultaneously is a very effective way of targeted attack. The main feature of network granulation, as a type of attack, is the destruction or blocking not nodes, but NS's edges. Such approach, which is practically not developed within TCN and consists in using not nodes, but edges of network systems as attack targets is a powerful resource for optimizing scenarios of targeted attacks, especially for the party that uses active protection. At the same time, it is obvious that much easier to block communication between NS nodes than to destroy one of them. Thus, in order to damage the defense-industrial complex of aggressor country, along with the direct destruction of facilities that manufacture high-precision weapons, it is enough to stop supplying these facilities with the modern equipment and components. That is, we can formulate the following optimization problem: how, by blocking the minimum number of edges between NS nodes, stop or at least significantly delimit the operation process of maximum number of network system elements. Solution of this problem requires development of models of multidimensional network systems operation process [26], because manufacture of any high-precision weapon requires supply of many heterogeneous components – from the simplest, for example, UAV propellers or fuselages, to sufficiently complex ones – microcircuits, thermal imagers, software with artificial intelligence elements, and so on. On the other hand, to strike the budgetary sphere of aggressor country in order to reduce its financial possibilities for continuation of the war, along with the freezing of international assets, an embargo on purchase of energy carriers and other minerals can be established. Then we can formulate formulate the following optimization problem: how, by blocking the minimum number of edges between NS nodes, to maximally reduce the volumes of flow movement in the system. To solve this problem, it is expedient to use the concept of flow λ-core of network system, choosing as the volume of flow the financial equivalent of its content. That is, for this case as well, the flow approach makes it possible to develop more optimal scenarios of targeted attacks on the functioning of complex network systems compared to the structural one.

5. Conclusions

In 2019-2024, humanity faced two global challenges, the first of which (the Covid-19 pandemic) is a vivid example of system-wide non-target lesion, and the second is a targeted attack (aggression of the Russian Federation on Ukraine) and the resulting threat of a global food, energy, and financial crisis and introduction comprehensive sanctions against aggressor, the negative consequences of which affected almost all countries of the world. Humanity proved to be unprepared for such challenges, but no less dangerous threats remain. Over the past half century, 67% of biological species known to man have disappeared [27], and over the past 20 years, the costs of combating climate disasters have increased 8 times [28]. Currently, scientists know more than 20 viruses of dangerous infectious diseases, the mutations of which can lead to the spread of pandemics, much more catastrophic than Covid-19 [29], the threat of global military conflicts increases, etc. This confirms the relevance of studying the features of lesions of complex network systems and developing methods of effective protection against them. Understanding the structural and functional importance of system components allows us to choose objects that require priority protection or as soon as possible blocking, because they contribute the most to the lesion spreading. In the paper, a comparative analysis of structural and flow approaches to analysis of the vulnerability of complex network systems to heterogeneous negative influences is carried out, typical scenarios of successive targeted attacks on the most important elements of the system based on certain characteristics are considered, and scenarios of simultaneous group attacks on the most important NS's components are proposed. The problem of scale of system lesions caused by heterogeneous negative influences has been studied and it has been confirmed that the flow approach makes it possible to obtain a much more realistic picture of such lesions consequences. It is shown that the scenarios of targeted group attacks built on the basis of NS flow model are more optimal from the point of view of selecting attack targets than structural ones.

References

1. Vitenu-Sackey PA, Barfi R (2021) The impact of Covid-19 pandemic on the global economy: Emphasis on poverty alleviation and economic growth. The Economics and Finance Letters 8(1): 32-43. doi: 10.18488/journal. 29.2021.81.32.43
2. Bluszcz J, Valente M (2022) The Economic Costs of Hybrid Wars: The Case of Ukraine. Defence and Peace Economics 33(1): 1-25. doi: 10.1080/10242694.2020.1791616
3. Polishchuk O, Yadzhak M (2023) Models and methods of comprehensive research of complex network systems and intersystem interactions. Pidstryhach Institute for Applied Problems of Mechanics and Mathematics, National Academy of Sciences of Ukraine: Lviv.
4. Sawada Y, Bhattacharyay M, Kotera T (2019) Aggregate impacts of natural and man-made disasters: A quantitative comparison. International Journal of Development and Conflict 9(1): 43-73.
5. Wandelt S (2018) A comparative analysis of approaches to network-dismantling. Scientific Reports 8(1): 13513. doi: 0.1038/s41598-018-31902-8
6. Nguyen Q et al (2019) Conditional attack strategy for real-world complex networks. Physica A: Statistical Mechanics and its Applications 530: 12156. doi: 10.1016/j.physa.2019.121561
7. Bellingeri M, Cassi D, Vincenzi S (2014) Efficiency of attack strategies on complex model and real-world networks. Physica A: Statistical Mechanics and its Applications 414: 174-180. doi: 10.1016/j.physa.2014.06.079
8. Hansberry RL et al (2021) How wide is a fault damage zone? Using network topology to examine how fault-damage zones overprint regional fracture networks. Journal of Structural Geology 146: 104327. doi: 10.1016/ j.jsg.2021.104327
9. Noldus R, Van Mieghem P (2015) Assortativity in complex networks. Journal of Complex Networks 3(4): 507-542. doi: 10.1093/comnet/cnv005
10. Brunst PW (2010) Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. In: A War on Terror?, Ed. by Wade M, Maljevic A. Springer: New York, pp. 51-78. doi: 10.1007/978-0-387-89291-7-3

11. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote /index.html
12. Boccaletti S et al (2006) Complex networks: Structure and dynamics. Physics reports 424(4): 175-308. doi: 10.1016/j.physrep.2005.10.009
13. Proletarsky A et al (2020) Decision support system to prevent crisis situations in the socio-political sphere. Cyber-Physical Systems: Industry 4.0 Challenges, pp. 301-314. doi: 10.1007/978-3-030-32648-7_24
14. Waltner-Toews D, Kay JJ, Lister N (2008) Ecosystem Approach: Complexity, Uncertainty, and Managing for Sustainability. Columbia University Press: New York. doi: 10.1590/S0102-311X2010000200023
15. Saxena A, Iyengar S (2020) Centrality measures in complex networks: A survey. arXiv: 2011. 07190. doi: 10.48550/arXiv.2011.07190
16. Mariyam J, Lekha DS (2022) Need for a realistic measure of attack severity in centrality based node attack strategies. In: Complex Networks and Their Application X, Ed. by Benito RM et al, pp. 857-866, Springer: Cham. doi: 10.1007/978-3-030-93409-5_70
17. Glenn L (2015) Understanding the influence of all nodes in a network. Science Reports 5: 8665. doi: 10.1038/srep08665
18. Krackhardt D (1990) Assessing the political landscape: Structure, cognition, and power in organizations. Administrative Science Quarterly 35(2): 342–369. doi: 10.2307/2393394
19. Albert R, Jeong H, Barab´asi A-L (2000) Error and attack tolerance of complex networks. Nature 406: 378–382. doi: 10.1038/35019019
20. Holovach Yu et al (2006) Complex networks. Journal of physical studies 10(4): 247–289. doi: 10.30970/jps.10.247
21. Polishchuk O, Yadzhak M (2018) Network structures and systems: II. Cores of networks and multiplexes. System research and informational technologies 3: 38-51. doi: 10.20535/SRIT.2308-8893.2018.3.04
22. Polishchuk O, Yadzhak M (2018) Network structures and systems: III. Hierarchies and networks. System research and informational technologies 4: 82-95. doi: 0.20535/SRIT. 2308-8893.2018.4.07
23. Dorogovtsev SN, Goltsev AV, Mendes JFF (2006) K-core organization of complex networks. Physical review letters 96(4): 040601. doi: 10.1103/PhysRevLett.96.040601
24. Barabasi A-L (2007) The architecture of complexity. IEEE Control Systems Magazine 27(4): 33-42. doi: 10.1109/MCS.2007.384127
25. Polishchuk D, Polishchuk O, Yadzhak M (2016) Complex evaluation of hierarchically-network systems. arXiv preprint arXiv:1602.07548.

26. Boccaletti S et al (2014) The structure and dynamics of multilayer networks. Physics Reports 544(1): 1-122. doi: 10.1016/j.physrep.2014.07.001

27. https://www.theguardian.com/environment/ 2022/oct/13/almost-70-of-animal-populations-wiped-out-since-1970-report-reveals-aoe

28. https://www.oxfam.org/en/press-releases/800-increase-un-appeal-needs-extreme-weather-related-emergencies-over-last-20-years

29. He W-T et al (2022) Virome characterization of game animals in China reveals a spectrum of emerging pathogens. Cell 185(7): 1117-1129. doi: 10.1016/j.cell.2022.02.014