MATHEMATICAL MODELS OF NETWORK TERRORISM: FORMALIZING THE DESCRIPTION FOR WEIGHTED NETWORKS

Denis G. Plotnikov\textsuperscript{1}, Grigory A. Ostapenko\textsuperscript{2}, Vasily I. Borisov\textsuperscript{3}, Larisa V. Parinova\textsuperscript{4}, Nikolay M. Tikhomirov\textsuperscript{5}

\textsuperscript{1}Voronezh State Technical University, 14, Moscowskyprospekt, Voronezh, Russia
\textsuperscript{2}Voronezh State Technical University, 14, Moscowskyprospekt, Voronezh, Russia
\textsuperscript{3}Voronezh State Technical University, 14, Moscowskyprospekt, Voronezh, Russia
\textsuperscript{4}Voronezh State Technical University, 14, Moscowskyprospekt, Voronezh, Russia
\textsuperscript{5}Voronezh State Technical University, 14, Moscowskyprospekt, Voronezh, Russia


\texttt{plotnikovdenis@yandex.ru}, \texttt{ostg@mail.ru}, \texttt{borisov_v_i_2017@mail.ru}, \texttt{lv_parinova@mail.ru}, \texttt{n.tikhomirov@bk.ru}

Corresponding author: Denis G. Plotnikov

https://doi.org/10.26782/jmcms.spl.8/2020.04.00005

Abstract

Terrorist attacks and their probable consequences in networks are explored with the account of the network character of the modern terrorism. By using the network resources, the structure of a network conflict of terrorist character is formalized including the metrics of its depth. Probability and entropy models of a network conflict of terrorist character are proposed, taking into account the analytical estimations and regulation of risks of conflict situations occurrence. Viewing such characteristics as the value of a filler volume unit and the network bandwidth, the authors propose analytical expressions for risk, damage, chance and durability of the critical infrastructure elements.

Key words: Information network, network terrorism, network conflict model, risk analysis, critical infrastructure.

I. Introduction

Today, information is a means of ensuring success in business, an object of the most serious protection, one of the most important assets of an enterprise, but also one of the most significant elements of risk. In this context, it is information networks
that are becoming increasingly vulnerable and require serious multilevel protection. At the same time, the price to be paid by the owner of valuable information is substantially growing, if the owner does not make an effort to protect the resources. The root of many destructive processes in information networks nowadays (Newman, 2001, 2003a, 2003b, 2003c, 2005, e-resource) is often information conflicts (Antsupov & Shilov, 2007; Byrd, 2009; Korovin, 2009; Miroshnikov, 2002; Panarin & Panarin, 2003). Modern destructive (including terrorist) impacts are largely carried out in information networks, and their effects (damage) are significant both for the networks and for their users (Bachilo & Belov, 1992; Bachilo, 2001; Bachilo et al., 2001; Lisichkin & Shelepin, 1999; Nikitov, 2000). Therefore, it is very important to understand the cause of information conflicts, their development mechanisms, and the scenarios (Pastor–Satorras & Vespignani, 2001a, 2001b, 2002, 2003, 2004). In this regard, risks are evidently growing. It is not only the extent of the possible damage, but also the probability of its occurrence that is increasing. In this context, the relevance of network risk analysis and risk management becomes one of the most important issues that can significantly improve the security of weighted networks.

II. Network analysis of terrorist activities

Below we consider the network interaction of terrorist structures with the society and state through the application of system analysis techniques, in particular the conceptual and mathematical apparatus of the networks theories and conflicts. Let there be a terrorist network $Net_T$ that attacks a network $Net_A$ which is a part of a multinet $Net$ suprasystem (the state and/or their unions). The networks interact in accordance with their local goals $W, W_A, W_T$. Notation $Net$ means that there is no network $Net_T$ in the environment $Net_A$. This approach is useful for dealing with terrorist conflicts, because it uses radical assessment for exclusion (destruction, elimination) of the conflicting component $Net_T$ of network $Net_A$. At that, $Net_A \cap Net_T \neq \emptyset$, i.e., the intersection of attacking and being attacked networks is not an empty set.

Let us assume that network efficiencies and resources are measurable on a set $Net_A$ and there are real functions (efficiency functions) $E^W(Net_A), E^W(Net_T), E^W(Net)$ such that if $Net_A > Net_T$ ($>_W$ is better in the sense of $W$), then $E^W(Net_A) > E^W(Net_T)$. Accordingly, $Net_T >^W Net_A$, if $Res(Net_T) >^W Res(Net_A)$, and $Net_T >^W Net$ if $E^W(Net_T) > E^W(Net)$.

Evaluation of the effectiveness $E^W$ of a network $Net$ in terms of achieving goal $W$ is related to the essence of that goal. For example, if the network $Net$ is preparing to survive a crisis period (perhaps even a war), it is evident that the challenge of stockpiling has come to the fore, i.e., the strategic resource $Res(X) \uparrow$ should be increased. This requires the concentration of the filler $F_i$ in the vertices of network $X$. If $W$ requires the maximum interoperability of the network with the external environment and between its clusters, a full increase of the dynamic resource $Res(A) \uparrow$ in the arcs of network $A$ will be required. Analytically these options of the goal can be expressed as follows:

Copyright reserved © J. Mech. Cont. & Math. Sci.
Denis G. Plotnikov et al
\[ E^w = \frac{\text{Res}(X, t_2)}{\text{Res}(X, t_1)} > 1; \]
\[ E^w = \frac{\text{Res}(A, t_2)}{\text{Res}(A, t_1)} > 1, \]

where the time parameter \( t_2 > t_1 \) and \( \text{Net}(X, A, F_{\text{II}}) \).

Such a gradation of goals may be even more diversified. However, for simplicity, we will further operate with resource \( \text{Res}(\text{Net}) \), \( \text{Res}(\text{Net}_A) \) and \( \text{Res}(\text{Net}_T) \) without differentiating by type, because it can easily be done in each case of analysis (increase of the state “airbag”- reserves/assets; increase in the turnover of the network trade etc.). At the same time, network terrorist attacks will be in any case aimed at a certain type of resource of the affected network, i.e.

\[ W_T \Rightarrow \text{Res}(X) \downarrow \lor \text{Res}(A) \downarrow, \]

with a view to its significant reduction and inflicting maximum damage to the object by using the strategies of depleting or depreciating the resources (chapter four).

If \( \text{Net}_T \) is better without \( \text{Net}_A \), there is a need to eliminate the dominance of \( \text{Net}_A \) over \( \text{Net}_T \), which with disparate \( \text{Res}(\text{Net}_A) \gg \text{Res}(\text{Net}_T) \) resources of \( \text{Net}_A \) and \( \text{Net}_T \) may motivate \( \text{Net}_T \) to illegal confrontation (terrorist acts) against \( \text{Net}_A \).

The network \( \text{Net}_T \) is in conflict with the network \( \text{Net}_A \) in terms of achieving the goal \( W(\text{Net}_T \text{conf}^w \text{Net}_A) \) if

\[ \text{Res}(\text{Net}_A) < \text{Res}(\text{Net}_A | \text{Net}_T) \]

This means that the presence of a network \( \text{Net}_T \) in the network \( \text{Net}_A \) reduces the shared resource. In this case, one can assume that there are other relations providing for the fulfillment of the conditions for \( \text{Net}_T \) and \( \text{Net}_A \):

\[
\begin{align*}
\text{Res}(\text{Net}_A) &> \text{Res}(\text{Net}_A | \text{Net}_T); \\
\text{Res}(\text{Net}_A) &= \text{Res}(\text{Net}_A | \text{Net}_T). 
\end{align*}
\]

Under the first condition, the presence of \( \text{Net}_T \) increases the resource, and \( \text{Net}_T \) cooperates with \( \text{Net}_A \). If the presence of \( \text{Net}_T \) does not affect the overall utility (the second condition), then \( \text{Net}_T \) and \( \text{Net}_A \) are independent.

As this work deals with counter-terrorism issues, the further description will cover the conflict network relations only.

The network \( \text{Net}_A \) is in conflict with the network \( \text{Net}_T \) in terms of achieving the goal \( W_T(\text{Net}_T \text{conf}^w \text{Net}_T) \), if \( \text{Res}(\text{Net}_T) < \text{Res}(\text{Net}_T | \text{Net}_A) \). On the other hand (Figure 1), the network \( \text{Net}_A \) conflicts with the network \( \text{Net} \) in terms of achieving the goal \( W_A(\text{Net}_A \text{conf}^w \text{Net}_A) \), if \( \text{Res}(\text{Net}_A) < \text{Res}(\text{Net}_A | \text{Net}_0) \). In other words, the conflict is external if interaction with multinet-suprasystem \( \text{Net} \) is considered.

In general, let us assume that \( \text{Net}_T \text{conf}^w \text{Net}_A \) and the corresponding efficiency functions are reduced to dimensionless values (normalized) so that they can be compared. Consider the conflict metrics:

Copyright reserved © J. Mech. Cont. & Math. Sci.
Denis G. Plotnikov et al
\[
\rho(E^W) = \text{Res}(\text{Net}\_T | \text{Net}_A) - \text{Res}(\text{Net}\_T | \text{Net}\_A), \\
\rho(E^\text{\textbar}) = \text{Res}(\text{Net}\_T | \text{Net}_A) - \text{Res}(\text{Net}\_T | \text{Net}_A).
\]

These metrics can serve as assessments of the measure, which characterizes the degree of conflict in terms of achieving the goal \(W_A\). Indeed, if \(\rho(E^W) > 0\) and the higher the value, the stronger the conflict \(\text{Net}_T \text{ conf Net}_A\).

Similarly, differences can be considered:

\[
\rho(E^W) = \text{Res}(\text{Net}\_T | \text{Net}_A) - \text{Res}(\text{Net}\_T | \text{Net}_A), \\
\rho(E^\text{\textbar}) = \text{Res}(\text{Net}\_T | \text{Net}_A) - \text{Res}(\text{Net}\_T | \text{Net}_A)
\]

(3)

Metrics \(\rho(E^W)\) and \(\rho(E^\text{\textbar})\) can serve as an estimate of the measure which characterizes the degree of conflict. The higher the module of value \(\rho(E^W)\), the greater the degree of conflict.

The depth (intensity) of a mutual conflict can be measured as the sum \(\rho(E^W) + \rho(E^\text{\textbar})\). The intensity of the mutual conflict increases in descending order of this sum, which can provoke serious terrorist acts.

The relations of conflict in terms of goals \(W_A\) and \(W_T\) are formed on many efficiency functions \(\text{Res}(\text{Net}_A)\) and \(\text{Res}(\text{Net}_T)\). They may have different dimensions and may occur not in the interest of their local goals, but also the goals of other subnets. However, it is desirable for terrorists first to drastically adjust the goal \(W_A\) by significantly reducing the resources of the network \(\text{Net}_A\), which is susceptible to terrorist attacks from \(\text{Net}_T\).

The motives of committing the terrorist acts can be expressed through the following relations. Let \(W_A\) be a partially measurable goal, and a set of functions \(Q = \{\text{Res}(\text{Net}_1), \ldots, \text{Res}(\text{Net}_m)\}\) is defined on attacked networks \(\text{Net}_A\) to be such \(\text{Net}_i >^W \text{Net}_T\) that at least for one \(i = 1(1)m\) there is \(\text{Res}_m(\text{Net}_i) > \text{Res}_m(\text{Net}_T)\). The network \(\text{Net}_T\) conflicts with attacked networks \(\text{Net}_A = \text{UNet}_i\), i.e. \(\text{Net}_T \text{ conf Net}_A\), by vector \(Q\) in terms of achieving the goal \(W_A\). For each \(i = 1(1)m\)
There are two ways to assess the degree of conflict in a vector case. The first method is to postulate some scalar convolution of vector assessment of vector Q on a set Net, for example, in a form $\sum k_i \text{Res}(\text{Net}_i)$, where $k_i$ is some weighting quotient of the importance of a sectoral assessment $\text{Res}(\text{Net}_i)$. The second method is to directly introduce the distance between vectors $Q(\text{Net}_i \uparrow | \uparrow \text{Net}_\tau)$ and $Q(\text{Net}_i \uparrow | \uparrow \bar{\text{Net}}_\tau)$ separately for the case $\text{Net}_\tau \text{ conf } \text{Net}_A$, for example, in the form of a root mean square estimation

$$\rho(E^W) = \sqrt{\sum [\text{Res}(\text{Net}_i | \text{Net}_\tau) - \text{Res}(\text{Net}_i | \bar{\text{Net}}_\tau)]^2}. \quad (4)$$

The network $\text{Net}_\tau$ is in conflict with the network $\text{Net}_A$ ($\text{Net}_\tau \text{ conf } \text{Net}_A$) by vector Q in terms of achieving the goal $W_A$, if at least for one i

$$\text{Res}(\text{Net}_i | \text{Net}_\tau) - \text{Res}(\text{Net}_i | \bar{\text{Net}}_\tau) < 0. \quad (5)$$

In the case when the above inequality is not true for all i, the conflict is partial. The conflict is total, if \forall i

$$\text{Res}(\text{Net}_i | \text{Net}_\tau) < \text{Res}(\text{Net}_i | \bar{\text{Net}}_\tau), \quad (6)$$

and antagonistic, if

$$\text{Res}(\text{Net}_i | \text{Net}_\tau) << \text{Res}(\text{Net}_i | \bar{\text{Net}}_\tau), \quad (7)$$

for i with the largest weight quotients $k_i$.

It is these conflicts that should be dealt with in the subject area of countering terrorism. In this case, the relation $\text{conf}_\tau$ is often non-symmetrical and conflict resolution involves either changes in the environment of $\text{Net}_A$ (until the elimination of $\text{Net}_\tau$), or structural, functional, parametric and other transformations that actually lead to a radical change of goals $W_\tau$ and $W_A$.

In the context of this work, a terrorist act is primarily a detonator for the whole spectrum of informational and psychological consequences, destabilizing and disrupting the attacked STN in terms of increasing its entropy. Terrorist organizations, as a subject of the use of weapons, carry out a terrorist act against a selected site at the intersection of the technical and social subnets of the attacked STN. But the immediate object of the attack is the information and psychological space (IPS), more precisely its entropy – the static indicator of the STN sustainability. Let us consider the processes intensified by a terrorist act in IPS of the STN.

1. Chain reaction of the chain impulse dissemination based on two effects:
   - primary, i.e., the success of direct impact on a person from the information source;

Copyright reserved © J. Mech. Cont. & Math. Sci.
Denis G. Plotnikov et al
– secondary and higher order, i.e., by transferring the information impulse from one person to another.

Here, the success of the elemental destructive informative controlling impact (DICl) is intimidation of an individual, which leads to disorganization of the society and state.

2. At the threshold of establishing the global information society, mankind has developed a vast transnational information and communication environment, whose electronic media automatically disseminate the DICl almost without restrictions.

Let us consider the informational aspect of terrorist activity.

Let $T_R$ be an operator describing the process of preparing and implementing a terrorist operation, $T_{RA}$ be an operator describing the aftermath process, i.e. the network reaction to the attack. The resources and specificity of terrorist organizations (TO) do not allow them to fight openly, therefore their tactics is brought to unexpected short-term attacks at the “problem spots”. The need to confront the superior resource of the attacked network forces TO to “spare power” under conspiracy conditions. This tactical technique is most characteristic of the periods of preparation and aftermath of the attack ($t < t_R$ and $t > t_R$). It is noteworthy that TO is particularly careful in choosing the time of implementation of a terrorist act $t_{T_R}$. These are often landmark dates — anniversaries and commemorations of politically significant events. There is even an international terrorist calendar. At the same time, today’s terrorist attacks are less associated with commemorative events. It becomes more important for TO to determine the moment of maximum insecurity and to achieve the greatest damage to the attacked STN.

The period of aftermath continues from the moment of the attack $t_{T_R}$ to the moment of stabilization $t_{S}$ and its duration is determined by the extent of the damage to the information space of the attacked network. Thus, the purpose of a terrorist attack is to implement a short-term attack with a large-scale resonance in the information space with as long period of aftermath (or the period of eliminating its aftermath) as possible.

The choice of targets $Net_I$ of a terrorist attack for $Net_T$ is often limited to the following inequality:

$$E(Net_A|Net_{II}) \gg E(Net_A|Net_{I}).$$ (8)

The implementation of the operator $T_R$ involves a radical attack on the information space of the network $Net_A$ to significantly reduce its efficiency:

$$E(Net_A|Net_{II}) \downarrow\downarrow.$$ (9)

The demoralizing fear and chaos, which paralyze the information and psychological space of the network $Net_A$, constitute the most important expected results of the operation. In terms of sensitivity theory, this criterion $(\kappa - 1)$ can be written as follows:

Copyright reserved © J. Mech. Cont.& Math. Sci.
Denis G. Plotnikov et al
where \( S_{\Phi}^E \) is the quotient of relative sensitivity of the effectiveness of the attacked STN in relation to changing the effectiveness of its subnet – the attack target; \( S_{\Phi}^E \) is the quotient of relative sensitivity of the effectiveness of the attacked STN in relation to changing the efficiencies of its other subnets.

However, (10) is not the only criterion in this case. The degree of the object security in relation to the resource \( \text{Res}(\text{Net}_T) \) used to implement the operation, is also essential for the TO. Terrorist organizations are trying to maximize the effectiveness of overcoming the protection mechanisms M, or, at least, \( \text{Res}(\text{Net}_T) \), should be sufficient to overcome M:

\[
\text{Res}(T_R \cdot M) \ll \text{Res}(\text{Net}_T). \tag{11}
\]

The combination of criteria (10) and (11) motivates the object selection for TO. The latest large-scale terrorist acts combined a huge social impact with almost total insecurity of the object.

At the dawn of its development, terrorism was aimed, as a rule, at the physical destruction of political figures (the goal is to destroy the object \( \text{Net}_I \)). However, modern terrorism tends to pursue the goal of political blackmail through intercepting control over a critical object. Control over the situation allows terrorists to set up rigid demands and to steer the course of events in the necessary direction, maximally using the available information space to whip up fear through the interception of control over the terror object \( \text{Net}_I \).

Large-scale modern terrorist attacks also use a hybrid option when \( \text{Net}_I \) is partially destroyed to terrorize the society. In this case, the goal is composite:

\[
W_{TR} = \bar{\text{Net}}_{I0} \& \text{Net}_I. \tag{12}
\]

The aftereffect processes are perhaps the most significant in a terrorist attack. It is at this stage of development that TOs expect to achieve political destabilization of the attacked network. The information waves caused by the terrorist act contribute to this. The global character of information space offers unprecedented prospects. It is appropriate to compare a terrorist operation with an “information bomb”; where the actual act of terrorism is only a detonator.

Then, the attacked and other information networks (without any costs to the TO) disseminate the details of the terrorist act broadly and in detail (tactics of using the opponent’s networks for their own benefit). In this case the TO gains advantage. This can be easily shown.

The source of the terrorist threat \( \text{Net}_T \) carries out an operation \( T_R \) with regard to \( \text{Net}_A \) by means of an attack aimed at a critically important object \( \text{Net}_{II} \).

Implementation of the attack induces \( (T_{RA}) \) relevant waves \( T_m \) in the information space, by which the secondary sources \( \text{Net}_{i,i} = 1(0) \text{mare involved. They, with the totality of their views (in relation to the implemented attack), have an impact } T_B \) on...
the control center $Net_Y$ of the affected network $Net_A$. Much more damage occurs when the media is involved $Net_{CMH}$. In this case, television and the Internet (transmission opportunities $T_n$ of which are enormous $n \gg m$) can play the role of $Net_{CMH}$. As a result, the extent of impact (control) on $Net_Y$ is disproportionately increased. If terrorists are also able to influence the content of terrorist information by using a trusted source of information $Net_D$ connected to $Net_{CMH}$, the role of which special websites can perform, then the information damage from the terrorist operation increases significantly.

The results have proved the primarily information and control orientation of terrorist attacks.

Consider the synergistic aspect of conflict interaction of a terrorist nature. If anti-terrorism efforts (ATE) increase, the risk level is reduced and the curve shifts to the origin of coordinates along the axis of probable damage $U$, which is considered in a rationed form.

If the destructive information and control impact (DICI) grows, the risk level for TO increases and the curve shifts to the catastrophic boundary of probable damage.

The aim of TO is to shift the network to the bifurcation point by means of destructive information and control impact (DICI). The bifurcation point in the risk assessment is reached when $u_0 = 1$, i.e., the maximum risk is at the maximum allowable damage and $\text{Risk}'(1) = 0$.

In this situation, the network will have to change into a qualitatively different state (regenerate or perish). These states are called attractors, and they attract networks that fall into the bifurcation zone.

This situation is preceded by a crisis period when the upper limit of the high-risk zone $u_2$ comes at the maximum allowable damage ($u_2 = 1$), i.e., $\text{Risk}'(1) = 0$. This is a warning signal that the network is in a high-risk zone and ATE should be activated.

In this case, stability reserve can be roughly estimated as

$$S_{it} = \frac{u_2 - u_0}{u_2} = 1 - \frac{u_0}{u_2} = 1 - u_0.$$  \hspace{1cm} (13)

Thus, the dynamics of conflict in the terrorist space can be viewed as TO strive to increase the risk by shifting the attacked system to disaster and an attempt by the ATE agents to return it to stability.

### III. Probability and entropy models of terrorist attacks at networks

The attacked socio-technical networks and terrorist structures are presented as conflicting stochastic networks.

Let the socio-technical network $Net_A$ be subjected to terrorist attacks by TO network $Net_T$ (Ostapenko, 2006). At that, the range of terrorist acts is characterized by a set $Net(W_T) = \{\text{Res}(Net_{T_1}), \ldots, \text{Res}(Net_{T_L})\}$ which is stochastic and has the
corresponding sets of probabilities of “success” and “failure” in carrying out the attack:

\[ P(\text{Net}_T) = \{P[\text{Res}(\text{Net}_{T_1})], \ldots, P[\text{Res}(\text{Net}_{T_m})]\} \]

and

\[ P(\overline{\text{Net}}_T) = \{P[\text{Res}(\overline{\text{Net}}_{T_1})], \ldots, P[\text{Res}(\overline{\text{Net}}_{T_m})]\}. \]

Accordingly, the object of a terrorist attack \( \text{Net}_A \) is characterized by many possible states (vectors of state variables)

\[ \text{Net}_A = \{\text{Res}(\text{Net}_{A_1}), \ldots, \text{Res}(\text{Net}_{A_n})\}, \]

which are also of a probabilistic nature:

\[ P(\text{Net}_A) = \{P[\text{Res}(\text{Net}_{A_1})], \ldots, P[\text{Res}(\text{Net}_{A_n})]\}. \]

Let us consider the stochastic process of interaction between \( \text{Net}_A \) and \( \text{Net}_T \), using probability and entropy as utility functions.

This can be described as a conflict (Ostapenko, Linets, Guzev, & Chapurin, 2015) of random events, which are about achieving some of the target states. Then, if \( \text{Res}(\text{Net}_A) \) and \( \text{Res}(\text{Net}_T) \) are compatible dependent random events, aimed at the achievement of the target states by stochastic networks \( \text{Net}_A \) and \( \text{Net}_T \), then, accordingly, the following inequalities for conditional probabilities can be recorded in accordance with the definitions of the terrorist conflict:

\[
\begin{align*}
P[\text{Res}(\text{Net}_A|\text{Net}_T)] &\ll P[\text{Res}(\text{Net}_A|\overline{\text{Net}}_T)]; \\
P[\text{Res}(\text{Net}_A|\overline{\text{Net}}_T)] &\ll P[\text{Res}(\text{Net}_A)]; \\
P[\text{Res}(\text{Net}_A|\text{Net}_T)] &\ll P[\text{Res}(\text{Net}_A|\overline{\text{Net}}_T)]; \\
P[\text{Res}(\text{Net}_A|\overline{\text{Net}}_T)] &\ll P[\text{Res}(\text{Net}_A)].
\end{align*}
\]

The degree of interaction between the dependent events \( \text{Net}_A \) and \( \text{Net}_T \) is proposed to be evaluated in the form of a rationed quotient \( R_{WT} \), whose properties are similar to those of the pair correlation quotient for random values:

\[
R_{WT} = \frac{P[\text{Res}(\text{Net}_A|\text{Net}_T)] - P[\text{Res}(\text{Net}_A)]P[\text{Res}(\text{Net}_T)]}{\sqrt{(P[\text{Res}(\text{Net}_A)][1 - P[\text{Res}(\text{Net}_A)])][P[\text{Res}(\text{Net}_T)][1 - P[\text{Res}(\text{Net}_T)])}}. \quad (14)
\]

This quotient is called the events correlation quotient.

Convert numerator to (14):

\[
P[\text{Res}(\text{Net}_A|\text{Net}_T)] - P[\text{Res}(\text{Net}_A)]P[\text{Res}(\text{Net}_T)] = \]

\[
= P[\text{Res}(\text{Net}_T)]P[\text{Res}(\text{Net}_A|\text{Net}_T)] - P[\text{Res}(\text{Net}_A)]P[\text{Res}(\text{Net}_T)].
\]
The above ratios accurately describe the probability of conflict between the attacked socio-technical network $Net_A$ and the attacking terrorist network $Net_T$.

Eliminating the conflict involves changing the environment, creating functional, parametric, and other conversions. Resolving the conflict relates to changing the elements of the environment $Net_A$ by the network $Net_T$ in a way that allows the conditions of the conflict to be eliminated. One could also speak of resolving a conflict by choosing and building different schemes of compromise and optimization. However, compromises with the terrorists are unproductive.

Consider two random values $Net_A$ and $Net_T$ that characterize the behavior of a stochastic network $Net_A$. It has been proved above that there is a conflict between random values $Net_A$ and $Net_T$ if and only if the value of the sample correlation coefficient is less than zero. This value is significantly less than zero for a terrorist conflict.

Let us suppose that two networks $Net_A$ and $Net_T$, in the process of achieving their goals $Net_A$ and $Net_T$, are interacting in a certain environment $Net_{world} (world \ community)$ with a common goal. Each network is characterized by a combination of possible target states:

$$\{Res(Net_A), i = 1(1), s; Res(Net_T), j = 1(1), s.\}$$

The simple intersection of these network states $Net_A$ does not fully describe its behavior, because it is determined not only by the need to implement specific states, but also by the ability to implement these states, defined by the network operating environment, which includes network $Net_A$, with its own interests.

It is also clear that the degree of implementation of individual network states $Net_A$ can be described by some utility function $P$. For stochastic networks, it is natural that function $P$ is the probability of implementation of the network states $Net_A$, i.e.

$$0 < P[Res(Net_A)] < 1, i = 1(1), s,$$

$$\sum_i P[Res(Net_A)] = 1.$$
a numeric set that has the streamlining property \( P \). In other words, we can formally record all sets of possible states

\[
\begin{align*}
\text{Res}(\text{Net}_{A_1}|\text{Net}_{T_1}) & \quad \cdots \quad \text{Res}(\text{Net}_{A_i}|\text{Net}_{T_i}) \\
\text{Res}(\text{Net}_{A_2}|\text{Net}_{T_2}) & \quad \cdots \quad \text{Res}(\text{Net}_{A_j}|\text{Net}_{T_j}) \\
\vdots & \quad \vdots \quad \vdots \\
\text{Res}(\text{Net}_{A_S}|\text{Net}_{T_s}) & \quad \cdots \quad \text{Res}(\text{Net}_{A_l}|\text{Net}_{T_l})
\end{align*}
\]

for which \( \sum \text{Res}(\text{Net}_{A_j}|\text{Net}_{T_j}) = 1, j = 1, l \). Then dependence of network \( \text{Net}_A \) on network \( \text{Net}_T \) means that there is at least one state \( \text{Res}(\text{Net}_{A_j}|\text{Net}_{T_j}) \), such that

\[
P[\text{Res}(\text{Net}_{A_k})] \neq P[\text{Res}(\text{Net}_{A_k})|\text{Res}(\text{Net}_{T_j})].
\]

As the dependency (15) can be expressed in terms of more or less, we make the following conclusions.

A quantitative measure is needed to analyze the conflict of functioning stochastic networks. Since the conflict determines the degree of a contradiction development resulting from organization or disorganization, recognizability or non-recognizability of network states, then, it is appropriate to use the network entropy as such measure.

The entropy of the network \( H(\text{Net}_A) \) has the following properties:

1. \( H(\text{Net}_A) = 0 \), when one of the states \( a^* \) is true and others are not possible.
2. \( H(\text{Net}_A) \) ata specified number of states \( n \) reaches the maximum when these states are equiprobable: \( P[\text{Res}(\text{Net}_{A_1})] = P[\text{Res}(\text{Net}_{A_2})] = \ldots = P[\text{Res}(\text{Net}_{A_S})] \), and \( H(\text{Net}_A) \) rises when the \( s \)-parameter is increased.
3. \( H(\text{Net}_A) \) has the property of additivity

The entropy measure of a network \( \text{Net}_A \) is defined as follows: \( H(\text{Net}_A) = \sum_i P[\text{Res}(\text{Net}_{A_i})] \log_2 P[\text{Res}(\text{Net}_{A_i})] \).

The entropy of a network \( \text{Net}_A \) during the attack \( S_T \) is defined as

\[
H(\text{Net}_A|\text{Net}_{T}) = \sum_i \sum_k P[\text{Res}(\text{Net}_{T_i})] P[\text{Res}(\text{Net}_{A_i}|\text{Net}_{T_k})].
\]

Note that according to the well-known Bayes' formula:

\[
P[\text{Res}(\text{Net}_{T_k}|\text{Net}_{A_i})] = \frac{P[\text{Res}(\text{Net}_{T_k})|\text{Res}(\text{Net}_{A_i}|\text{Net}_{T_k})]}{\sum_i P[\text{Res}(\text{Net}_{T_i})] P[\text{Res}(\text{Net}_{A_i}|\text{Net}_{T_k})]}.
\]

entropy can only be calculated through previously introduced probabilities.

On the basis of the above, to assess terrorist activity as a measure of dependency between networks \( \text{Net}_A \) and \( \text{Net}_T \), we can use the parameter

\[\text{Para}\]
\[ J(\text{Net}_A, \text{Net}_T) = H(\text{Net}_A) - H(\text{Net}_A| \text{Net}_T) \] (16)

or

\[ J(\text{Net}_A, \text{Net}_T) = H(\text{Net}_A| \text{Net}_T) - H(\text{Net}_A), \]

which shows how much the uncertainty associated with \( \text{Net}_A \) changes from the prior execution of an attack on \( \text{Net}_T \).

In the information theory, the following relations are known to link different types of entropy:

\[ H(\text{Net}_A, \text{Net}_T) = H(\text{Net}_A) + H(\text{Net}_T| \text{Net}_A) = H(\text{Net}_T) + H(\text{Net}_T| \text{Net}_A)H(\text{Net}_A) + H(\text{Net}_T), \]

\[ J(\text{Net}_A, \text{Net}_T) = H(\text{Net}_A) + H(\text{Net}_T) - H(\text{Net}_A, \text{Net}_T) = H(\text{Net}_A) - H(\text{Net}_A| \text{Net}_T) = H(\text{Net}_T) - H(\text{Net}_T| \text{Net}_A). \]

In addition to an absolute measure of dependence (16), it is possible to introduce a normalized measure of dependency between \( \text{Net}_A \) and \( \text{Net}_T \):

\[ N(\text{Net}_A, \text{Net}_T) = \frac{J(\text{Net}_A, \text{Net}_T)}{H(\text{Net}_A)}. \] (17)

Measure (17) has the following properties:

1. \( N(\text{Net}_A, \text{Net}_T) = 0 \), if the networks \( \text{Net}_A \) and \( \text{Net}_T \) are independent, i.e., the ratio (17) is not executed for any of the states \( \text{Res}(\text{Net}_{A_k}) \) and \( \text{Res}(\text{Net}_{T_j}). \)
2. \( N(\text{Net}_A, \text{Net}_T) = 1 \), when any state \( \text{Res}(\text{Net}_{A_k}) \) of networks \( \text{Net}_A \) is determined by the network \( \text{Net}_T \) behavior, i.e., by the implementation of one of the states \( \text{Res}(\text{Net}_{T_j}). \)
3. Alongside with that, \( N(\text{Net}_A, \text{Net}_T) \) takes values that characterize the degree of the networks dependency.
4. In general, \( N(\text{Net}_A, \text{Net}_T) \neq N(\text{Net}_T, \text{Net}_A). \)

A conflict can be managed by changing the set of probable target states for each network by adding or removing individual states.

In this case, during the attack, there is an injection of entropy into network \( \text{Net}_A \) from network \( \text{Net}_T \). Here, the discharge depends on the sensitivity of the attacked object in the networks. The TO goal is to achieve a significant excess of \( N \) (entropy measure) compared to the background level. In turn, the ATE agents’ tasks is to decrease entropy as much as possible and to reduce the aftereffect period.

Obviously, risk is the most complete characteristic of state for networks exposed to threats. Let us suppose that the socio-technical network attacked by terrorists includes vulnerable objects \( \{O_i\}, i = 1(1)m, \) where \( O_i \in \text{Net}_A \). They are the targets of terrorists, whose weapons are a set of \( \{\text{Res}(\text{Net}_{T_j})\}, j = 1(1)l \). The probability of hitting the above objects by these weapons can be assessed in the form of a probability matrix.
The goal of the terrorist’s weapon is clearly the entropy of the attacked network. The terrorists increase it many times causing fear and chaos. As a characteristic of damage (Ostapenko, 2005), it is appropriate to use the growth in entropy of networks $Net_T$ as a result of the successful terrorist attack $T_j$ on the object $O_i$, which is normalized by the maximum allowable value of entropy of the networks $H_{\text{max}}$:

$$\overline{U}_A(O_i|T_j) = \frac{H_A(O_i|T_j) - H_A(O_i|\overline{T_j})}{H_{\text{max}}}.$$ (18)

The latter expression is a relative assessment of damage. Based on the expression, a corresponding matrix can be built:

$$T_1 \begin{pmatrix} O_1 & \ldots & O_1 & \ldots & O_m \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ O_1 & \ldots & O_1 & \ldots & O_m \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \overline{U}_A(O_1|T_1) & \ldots & \overline{U}_A(O_1|T_1) & \ldots & \overline{U}_A(O_m|T_1) \end{pmatrix}.$$ (19)

Matrices (18) and (19) can be bases for creating the matrix of elementary risks

$$T_1 \begin{pmatrix} \tilde{r}_{\text{isk}}(O_1|T_1) & \ldots & \tilde{r}_{\text{isk}}(O_1|T_1) & \ldots & \tilde{r}_{\text{isk}}(O_m|T_1) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \tilde{r}_{\text{isk}}(O_1|T_j) & \ldots & \tilde{r}_{\text{isk}}(O_1|T_j) & \ldots & \tilde{r}_{\text{isk}}(O_m|T_j) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \tilde{r}_{\text{isk}}(O_1|T_1) & \ldots & \tilde{r}_{\text{isk}}(O_1|T_1) & \ldots & \tilde{r}_{\text{isk}}(O_1|T_1) \end{pmatrix},$$

where $\tilde{r}_{\text{isk}}(O_i|T_j) = \frac{P(O_i|T_j)\overline{U}_A(O_i|T_j)}{\overline{U}_A(O_i|T_1)}$.

In other words, each pair “target object – typeof weapon” is assigned a risk. The network security is characterized by the difference

---

*Copyright reserved © J. Mech. Cont.& Math. Sci.*

*Denis G. Plotnikov et al*
At the same time, both opposing parties (attacking and attacked) attempt to implement risk management. The former tries to increase it and the latter – to reduce. Terrorists choose the critical objects with high \( u_A \), which increases the likelihood of success of their attacks. Contrary to this, NetA seek to reduce \( P(O|T) \) for their critical objects, since the control of \( u_A \) is difficult. Denote 

\[
H(O|T) = \frac{H_A(O|T)}{H_{\text{max}}}
\]

and 

\[
\overline{H}(O|T) = \frac{H_A(O|\overline{T})}{H_{\text{max}}}
\]

We define them as rationed entropies that characterize the criticality of an object \( O \) by entropy to attacks \( T \). Then, through the mathematical expectation \( M(O|T) \), we can make a mean assessment of the risk as follows:

\[
\overline{r}_{\text{risk}}(O|T) = M(O|T)\overline{H}(O|T) - M(O|\overline{T})H_A(O|\overline{T})
\]

The value of mathematical expectation is determined by the situation. Depending on the degree of confrontation, the anti-terrorist structures can establish the level of terrorist threat. Combined with the effectiveness of the mechanisms for objects protection \( Z \), this level determines the above mathematical expectations:

\[
M(O|T) = [Z(O|T)P(O|T)]
\]

If a simultaneous terrorist attack on multiple objects takes place, the risk will be

\[
R_{\text{risk}} = \sum_{i,j} M(O|T) \Delta H_A(O|T)
\]

where \( \Delta H_A(O|T) = H_A(O|T) - H_A(O|\overline{T}) \) is the rationed increment of entropy as a result of an attack at the object by TO. In the expression (6.20), the summation and multiplying operations are implemented for all \( i \) involved in the attack.

The obtained analytical expressions filled with numerical parameters of stochastic processes of terrorism (expert estimates are also relevant) can serve as a basis for scientific and methodological risk-analysis of terrorist attacks. By changing the set of probable target states of each network, the conflict can be controlled by decreasing the entropy outburst and reducing the period of aftereffect.
IV. Terrorist attacks on the critical infrastructure elements

The most desirable goal of any terrorist is a critical object (CO) or critical infrastructure element (CIE) (Kalashnikov, Yermilov, Choropov, Razinkin, & Barannikov, 2013), which are generally large nodes of a multi-network structure functioning at the country level. Incapacitating of CO or CIE causes catastrophic consequences (suffice to recall the Chernobyl disaster) and serious shocks to the attacked society, so the analytical risk assessment of such situations is very relevant.

Assume that \( a \) is a node of CIE in terms of its total failure as a result of a critical attack in a moment \( t \). This can be described by the distribution of probability \( F(t) \) and its density \( f(t) \), i.e.

\[
\text{Attacke} T(a, \bar{t}) \Rightarrow F(\bar{t}), f(\bar{t}),
\]

where \( \bar{t} \) is the time normalized by the average life expectancy \( T_{ср} \) of such nodes \( a \), i.e.,

\[
\bar{t} = \frac{t}{T_{ср}}.
\]

Then, the dynamic resource of node \( a \) will be equal to:

\[
\text{Res}(a) = \langle C_+ \rangle V'_+ + \langle C_- \rangle V'_-,
\]

where \( C_+ \) is the value of an объем unit of filler traffic coming into \( a \); \( C_- \) is a value of the объем unit of filler traffic coming out of \( a \); \( V'_+ \) is a capacity of arcs coming into \( a \); \( V'_- \) is a capacity of arcs coming out of \( a \); \( \mu(t_0) \Delta t \) is the probability that CIE, successfully functioning until the moment \( t_0 \), will be destroyed by a terrorist attack during a time interval \( (t_0 + \Delta t) \); \( f(t_0) \Delta t \) is the probability that the CIE element, created \( t_0 \) time ago, will be destroyed in the interval \( (t_0 + \Delta t) \); \( [1 - F(t_0)] \) is the probability that CIE will not be destroyed before time \( t_0 \).

For the total failure of the attacked CIE, the following probability ratio can be recorded

\[
\mu(t_0) dt = \frac{f(t_0) dt}{1 - F(t_0)} \geq f(t_0) dt,
\]

where \( f(t_0) \) is the probability density of its failure in a moment \( t_0 \); \( F(t_0) \) is the probability of failure within the interval \( (0, t_0) \);

At the same time, the risk (Ostapenko, Yermilov, & Kalashnikov, 2013a; Ostapenko, Yermilov, & Kalashnikov, 2013b; Ostapenko, Linets, Guzev, & Choropov, 2015; Ostapenko, Karpeev, Plotnikov, Batisheev, Goncharov, Maslikhov, et al., 2010) for CIE in case the attack is successful (21) can be estimated as follows:

\[
\text{Risk}(t_0) = f(t_0)(\Delta t)(1 - t_0) \frac{\langle C \rangle}{\langle V' \rangle},
\]

where the damage equals:

\[
\bar{u}(t_0) = (1 - t_0) \frac{\langle C \rangle}{\langle V' \rangle}.
\]
In turn, the chance can be expressed as follows:

\[
\text{Chance}(t_{0}) = \left[1 - F(t_{0})\right] \left(\frac{c}{v}\right),
\]

where the benefit equals \( u(t_{0}) = t_{0} \frac{c}{v} \).

From expressions (24) and (25), the resilience of CIE can be found:

\[
L(t_{0}) = \frac{\text{Chance}(t_{0})}{\text{Risk}(t_{0})} = \left[1 - F(t_{0})\right] \left(\frac{t_{0}}{f(t_{0})(\Delta t)}\right) \left(\frac{1}{1 - t_{0}}\right),
\]

if the attack is successful at the time \( t_{0} \).

For a set of the attacked CIEs \( r = 1 \) from (6.26), an integrated assessment could be proposed

\[
L^{(R)}(t_{0}) = \frac{\sum_{r=1}^{R} \text{Chance}(a_{r}, t_{0})}{\sum_{r=1}^{R} \text{Risk}(a_{r}, t_{0})}.
\]

Amendments \( D_{wc}(a_{r}) \) are also appropriate, which take into account the centrality (weighted) of the analyzed node in the network.

\[
L^{(R)}(t_{0}) = \frac{\sum_{r=1}^{R} D_{wc}(a_{r})(Z) \text{Chance}(a_{r}, t_{0})}{\sum_{r=1}^{R} D_{wc}(a_{r})(Z) \text{Risk}(a_{r}, t_{0})}.
\]

It should be noted that it is the nodes with the most centrality \( D_{wc}(a_{r}) \) that are the most likely to be chosen by terrorists as targets for their attacks.

**V Conclusion**

Thus, the dynamics of the struggle within the terrorism space can be represented as a TO strive to increase the risk by shifting the attacked system to disaster, and the attempts of the ATE agents to return it to a stable state; by changing a set of probable target states of each of the networks, the conflict can be controlled by decreasing the entropy outburst and reducing the period of the attack aftereffect.

The application of the obtained results will provide a scientific and methodological basis for the efficient existence and functioning of weighted networks, as well as a significant reduction in the risks of attacks (Ostapenko, Plotnikov, Makarov, Tikhomirov, & Yurasov, 2013; Ostapenko, Parinova, Belonozhkin, Bataronov, & Simonov, 2013; Ermakov, Zavorykin, Kolenbet, Ostapenko, & Kalashnikov, 2014; Radko, Ostapenko, Mashin, Ostapenko, & Gusev, 2014; Radko, Ostapenko, Mashin, Ostapenko, & Avdeev, 2014; Ostapenko, Bursa, Ostapenko, & Butrik, 2014; Islamgulova, Ostapenko, Radko, Babadzhanov, & Ostapenko, 2016) resulting from inter-network confrontation, and in terrorist attacks at weighted networks.
References

I. Antsupov, A.Ya., & Shilov, A.I. (2007). Conflictology: textbook for higher educational institutions. Saint Petersburg: Sankt Peterburg.

II. Bachilo, I.L. (2001). Informational law: fundamentals of practical information science: tutorial. Moscow: M.Yu. Tikhomirov Publishers.

III. Bachilo, I.L., & Belov, G.V. (1992). On the concept of legal support of informatization in Russia. Legislative problems of society informatization. Moscow: Mir.

IV. Bachilo, I.L., Lopatin, V.N., Fedotov, M.A., et. al. (2001). Informational law: tutorial. Saint Petersburg: Law Center.

V. Byrd, K. (2009). War with many unknowns. Computerra, 20, 5.

VI. Ermakov, S.A., Zavorykin, A.S., Kolenbet, N.S., Ostapenko, A.G., & Kalashnikov, A.O. (2014). Optimization of expert methods used to analyze information security risk in modern wireless networks. Life Science Journal, 11(10s), 511-514.

VII. Grinyaev, S. Russia in the global information society: threats, risks and possible ways of their neutralization. Retrieved from: http://www.noravank.am/upload/pdf/419_ru.pdf.

VIII. Islamgulova, V.V., Ostapenko, A.G., Radko, N.M., Babadzhanov, R.K., & Ostapenko, O.A. (2016). Discreet risk-models of the process of the development of virus epidemics in non-uniform networks. Journal of Theoretical and Applied Information Technology, 306-315.

IX. Kalashnikov, A.O., Yermilov, E.V., Choporov, ON., Razinkin, K. A., & Barannikov, N.I. (2013). Attacks at crucial objects of informational and technological infrastructure: risks assessment and regulation: monograph. Voronezh: Scientific Book.

X. Korovin, V. (2009). Main military secret of the USA. Network wars. Moscow: EKSMO.

XI. Lisichkin, V., & Shelepin, L., (1999). Third world information war of nerves. Moscow.

XII. Miroshnikov, B. N. (2002). Fighting against crimes in the sphere of information technologies. Security systems, 5(47), 10-11.

XIII. Newman, M.E.J. (2001). The structure of scientific collaboration networks. Proc. Natl. Acad. Sci. USA 98, 404–409.

XIV. Newman, M.E.J. (2003a). Ego-centered networks and the ripple effect. Soc. Networks, 25, 83–95.
XV. Newman, M.E.J. (2003b). Mixing patterns in networks. *Phys. Rev. E* 67.

XVI. Newman, M.E.J. (2003c). The structure and function of complex networks. *SIAM Rev.* 45, 167–256.

XVII. Newman, M.E.J. (2005). A measure of betweenness centrality based on random walks. *Soc. Networks*, 27, 39–54.

XVIII. Newman, M.E.J. Power laws, Pareto distributions and Zipf’s law. Retrieved from: [https://vk.com/dev/openapi_api](https://vk.com/dev/openapi_api).

XIX. Newman, M.E.J., & Girvan, M. (2004). Finding and evaluating community structure in networks. *Phys. Rev. E* 69, 72–93.

XX. Nikitov, V.A. (2000). *Information support of public administration*. Moscow: Slavonic dialogue.

XXI. Ostapenko, A.G., Bursa, M.V., Ostapenko, G.A., & Butrik, D.O. (2014). Flood-attacks within the hypertext information transfer protocol: damage assessment and management. *Biosciences Biotechnology Research Asia*, 11, 173-176.

XXII. Ostapenko, A.G., Yermilov, E.V., & Kalashnikov, A.O. (2013a). Risks of lameness, chances of usefulness and component resilience of automated systems under conditions of information threats impact on them. *Information and safety*, 16(2), 215-218.

XXIII. Ostapenko, A.G., Yermilov, E.V., & Kalashnikov, A.O. (2013b). Innovative trends and information risks of development of the IT sphere in the context of providing crucial objects. *Information and safety*, 16(3), 323-334.

XXIV. Ostapenko, G.A. (2006). Stochastic Models and the Secondary Effects Analysis of the Informational-Derivative Action in the Sociotechnical Systems. *CSIT* 2, 32-34.

XXV. Ostapenko, G.A., Karpeev, D.O., Plotnikov, D.G., Batishchev, R.V., Goncharov, I.V., Maslikhov, P.A., et al. (2010). Risks of the distributed systems: techniques and algorithms of assessment and management. *Information and safety*, 13(4), 485-530.

XXVI. Ostapenko, G.A., Linets, A.L., Guzev, Yu.N., & Chapurin, E.Yu. (2015). Characteristics of the network conflict and capacities of networks. *Management of information risks and safety of infocommunication systems*, 4, 72-92.

XXVII. Ostapenko, G.A., Parinova, L.V., Belonozhkin, V.I., Bataronov, I.L., & Simonov, K.V. (2013). Analytical models of information-psychological impact of social information networks on users. *World Applied Sciences Journal*, 25 (3), 410-415.

*Copyright reserved © J. Mech. Cont.& Math. Sci.
Denis G. Plotnikov et al*
XXVIII. Ostapenko, G.A., Plotnikov, D.G., Makarov, O.Y., Tikhomirov, N.M., &Yurasov, V.G. (2013). Analytical estimation of the component viability of distribution automated information data system. World Applied Sciences Journal, 25 (3), 416-420.

XXIX. Ostapenko, O.A. (2005). Methodology of a risk assessment and securities of systems. Information and safety, 8(8), 28.

XXX. Panarin, I.N., &Panarin, L.G. (2003). Information war and peace. Moscow: OLMA-PRESS.

XXXI. Pastor–Satorras, R., &Vespignani, A. (2001a). Epidemic dynamics, endemic states in complex networks. Phys. Rev. E., 101 – 104.

XXXII. Pastor–Satorras, R., &Vespignani, A. (2001b). Epidemic Spreading in Scale–Free Networks. Phys. Rev. Lett. 86, 45 – 56.

XXXIII. Pastor–Satorras, R., &Vespignani, A. (2002). Absence of epidemic threshold in scale–free networks with connectivity correlations. Phys. Rev. Lett. Pub.: American Physical Society,90(2), 1 – 4.

XXXIV. Pastor–Satorras, R., &Vespignani, A. (2003). Epidemic spreading in complex networks with degree correlations. Contribution to the Proceedings of the 28thSitges Conference ‘Statistical Mechanics of Complex Networks’. Berlin, 165 – 170.

XXXV. Pastor–Satorras, R., &Vespignani, A. (2004). Topology, Hierarchy, Correlations in Internet Graphs. Lecture Notes in Physics. Springer, 425 – 440.

XXXVI. Radko, N.M., Ostapenko, A.G., Mashin, S.V., Ostapenko, O.A., &Avdeev, A.S. (2014). Peak risk assessing the process of information epidemics expansion. Biosciences Biotechnology Research Asia, 11, 251-255.

XXXVII. Radko, N.M., Ostapenko, A.G., Mashin, S.V., Ostapenko, O.A., &Gusev, D.V. (2014). Assessment of the system’s EPI-resistance under conditions of information epidemic expansion. Biosciences Biotechnology Research Asia, 11 (3), 1781-1784.