Taylor & Francis
Taylor & Francis Group

AVIATION
ISSN 1648–7788 / eISSN 1822–4180
2016 Volume 20(3): 137–144
doi:10.3846/16487788.2016.1237787

SYNERGISTIC EFFECTS OF INFORMATION AND CYBERNETIC INTERACTION IN CIVIL AVIATION

Yuriy DANIK[1], Ruslan HRYSCHUK[2], Sergiy GNATYUK[3]

[1, 2]Zhytomyr Military Institute n.a. S.P. Korolyov, Miru Ave. 22, 10004 Zhytomyr, Ukraine
[3]National Aviation University, Kosmonavta Komarova Ave. 1, 03680 Kyiv, Ukraine
E-mails: [1]zvir@zvir.zt.ua; [2] dr.hry@i.ua; [3]s.gnatyuk@nau.edu.ua (corresponding author)

Received 30 July 2015; accepted 06 June 2016

Yuriy DANIK, *Prof. Dr Habil*
Date and place of birth: 1964, Kyiv, Ukraine.
Education: Zhytomyr Higher Military School of Radioelectronics, 1987; Kharkiv Military University, 2002; National Academy for Public Administration under the President of Ukraine, 2007; Institute of State Military Management, 2010.
Affiliation and functions: Head of Zhytomyr Military Institute n. a. S. P. Korolyov, since 2011.
Research interests: governance in state security and defence.
Publications: author of over 400 scientific publications including monographs, dictionaries, textbooks, papers and patents.

Ruslan HRYSCHUK, *Dr Sc, Senior Researcher*
Date and place of birth: 1981, Pischanytsya, Ukraine.
Education: Zhytomyr Military Institute of Radioelectronics n. a. S. P. Korolyov, 2003.
Affiliation and functions: Head of the Information & Cybernetic Security Department at the Scientific Centre of Zhytomyr Military Institute n. a. S. P. Korolyov, since 2015.
Research interests: information and cybernetic security of the state.
Publications: author of over 153 scientific publications including monographs, textbooks, papers & patents.

Sergiy GNATYUK, *PhD, Assoc Prof.*
Date and place of birth: 1985, Netishyn, Ukraine.
Education: National Aviation University, 2007.
Affiliation and functions: Associate Professor at the Academic Dept of IT-Security, since 2012.
Research interests: information and cybernetic security, cyberthreats in civil aviation, information security incidents management, quantum cryptography.
Publications: author of over 100 books and papers, and 5 patents.

Abstract. Scientific research on information and cybernetic influence on citizens, society and the whole state is a hot topic of many famous worldwide scientific publications. These studies have become particularly relevant in critical spheres from the viewpoint of security. Civil aviation is one of the most critical spheres. Information and cybernetic actions in civil aviation have been studied separately to date. Known approaches did not allow considering the synergistic effects of information and cybernetic interaction. This factor has adversely affected preventive and countermeasures for minimizing the effects of information and cybernetic threats to aviation subjects. Taking this into account, in the paper, the essence of synergistic effects of information and cybernetic interaction on civil aviation are presented. Also, the methodology for the early detection, assessment and prediction of these effects was developed. The analysis revealed that the study of synergistic effects in civil aviation is an effective controller of nonlinear processes, which can occur as the result of information and cybernetic interaction.

Keywords: synergy, synergistic effect, information action, cybernetic action, methodology, interaction, civil aviation, critical aviation information system, aviation subject, cyberthreat.

1. Introduction

The intensive and irreversible destruction of a world order system established during a decade inevitably causes global changes in the classical international security paradigm. Today we are the eyewitnesses of an international security strategy transformation in the cybernetic space (cyberspace) (Jardine 2015; Gnatyuk 2013b). Therefore, the leading role of international security in the cyberspace is given to the cybernetic security (cybersecurity) system (Korchenko *et al.* 2013). The formation of a new cybersecurity paradigm (Danik 2011) is essentially associated with the following issues: methodology formation, objectives and contents' correction, definition of the role and place in the international security system, and, also, new methods, techniques and means for its enhancement. Consequently, a new scientific paradigm must be based on the correlation of practical and theoretical cybersecurity provinces (achievements), including their strong interrelation. The most acute problems threaten the most vulnerable path of the cybersecurity of the state's critical infrastructure, such as gas transportation infrastructure, energy complex and transportation (Hryschuk, Danik 2013; Kharchenko *et al.* 2009). Obviously, an unauthorized interference in the above-listed objects can cause serious economic losses, death of people and national infrastructure destruction. With this in mind, it is necessary to define and secure the state infrastructure sectors which are critical from the viewpoint of its security, functionality, and economic and social stability. Also, it is necessary to provide the functionality of the crisis emergency system and the security of the infrastructure that is important in dealing with the crisis. In civil aviation, the criticality level is heavily amplified by an increased degree of connectivity and interaction between ground systems and aerial vehicles (aircraft). Modern information and communication technologies' investigation on one hand increases the efficiency of civil aviation, and on the other hand creates a set of new vulnerabilities and different potential threats (Hryschuk, Chernyshuk 2013). According to documentation regulating civil aviation (in particular: Annex 17 to the Chicago Convention on International Civil Aviation "Security. Safeguarding International Civil Aviation against Acts of Unlawful Interference", Doc 8973, "Guidance on Aviation Security", Doc 9985, "Guidance on the Security of Air Traffic Management System", and Doc 30, "ECAC Policy Statement in the Field of Civil Aviation Security") the key task is ensuring the security of *critical aviation information systems (CAIS – a* set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination or disposal of information involved in all safety-critical aspects of aviation operations) against cyberthreats (Gnatyuk 2013b; Korchenko *et al.* 2010). The security of passengers, aircrew members and also airline nonflying personnel depends on the efficiency of solving the problem mentioned above. The international character of civil aviation makes this solution compulsory for all states which want to be a part of the international aviation community.

There are many incidents of non-power struggle (confrontation) between different states in the cyberspace. A good up-to-date example of the struggle mentioned is the powerful cyberattack with intensive information actions support on Estonia in 2007 that shut down practically all of its critical cybernetic infrastructures. Also, another example of confrontation in the cyberspace is the information and cybernetic actions (ICAs) during the Russo-Georgian war in 2008 (Tikk *et al.* 2012; The Russo-Georgian War… 2012), etc. A typical act of a non-power struggle in the cyberspace is the attack focused on Iran's nuclear objects using a network warm «Stuxnet» in the frame of the "Olympic game" program (Milevski 2011; Gnatyuk 2013b). This cyberattack destroyed automated control systems of Iran's nuclear infrastructure. It is also worthwhile to mention the ICAs in the "Color Revolution" management and Near East disorders in 2010 during the "Arab Spring" (Welt, Schmemann 2010; Khondker 2011). Take into account the incident dynamics in the cyberspace, referred to as cyberincidents (Gnatyuk 2013a; Symantec 2014), we can predict an increase of them in the near future and this fact is not good for international security. Considering the effects on international security, it is fair to say there is a *synergistic effect* (Haken 1993) resulting from the information and cybernetic interaction in cyberincidents. In the context of this study, a synergistic effect is the phenomenon obtained as a result of information and cybernetic interaction achieved by means of integrated destructive actions in the cyberspace which are concurrent with objectives in time and space and also carried out by a single idea and plan. Priory detection, assessment and prediction of the synergistic effect of information and cybernetic interaction is an actual scientific problem that must be solved. From the viewpoint of international experience this problem has a special importance in critical spheres, like civil aviation. The ICAs with regard to civil aviation were researched separately.

The latest discoveries and developments (Toth 2007; Tikk *et al.* 2012; The Russo-Georgian War … 2012; Milevski 2011; Welt, Schmemann 2010; Khondker 2011; Symantec 2014; Kaspersky Lab 2013) show a high demand of the global scientific community for studying the ICAs influence on citizens, society and whole states. But the characteristic feature of up-to-date scientific investigations in this direction is the fact that it is a separated study. As a result, the interaction synergy of ICAs

is ignored and causes the impossibility of asymmetric counter measure development against the destructive effects. The actuality of this study also relies on the absence of any conventional methods, techniques and parameters for the synergistic effect (caused by the ICAs) assessment. This essentially influences the time objectives, forms of analysis, and method establishment.

2. Objectives of the study

As seen from the analysis of the latest publications on this subject, the existing methods and instruments do not have the ability to provide an "early regulation effect". It's possible to report that the interaction synergy of the ICAs still remains an open issue. The *main objective of this paper* is the methodology development to assess synergistic effects resulting from information and cybernetic interaction. This methodology could offer the possibility of a well-timed synergy detection and its prediction in the cyberspace to solve a wide variety of tasks in civil aviation cybersecurity, as an important part of international security.

It has been found that the main impediment in the attempt to carry out a complex study of information and cybernetic interaction is, primarily, definition uncertainty. Considering the latest investigations and the best practice (Hryschuk 2011; Danik 2011; Korchenko *et al.* 2013), we formulated the following definitions:

- *information actions* – actions directed towards the public and/or individual consciousness changes in order to influence subjects to actuate the type of behavior defined by them.
- *Cybernetic actions* – actions directed towards cyberspace objects and subjects (social medium, technical and socio-technical systems) in the likeness of destructive influences that cause its management processes to breakdown or take complete control.

Taking into account the definitions, the methodology development for the information and cybernetic interaction's synergistic effect assessment must be based on an adequate mathematical model. This model development requires the establishment of principles, meanings and ICAs features, as well as a study of their formulation mechanisms and technologies. The analysis shows that both information actions and cybernetic actions have individual features, as described in the following sections.

3. Information actions

Information actions have the following characteristic features:

a) information actions have a determined nature (in other words all information action channels are known);
b) information actions have a selective target direction (i.e., not only the target but also subjects are known);
c) information actions have a long preparatory period and this is characterized by a continuous latent phase;
d) information actions are a prognostication of the preparation and realization of other actions (including a power struggle);
e) the subject of information actions is public and/or individual consciousness;
f) the "chain reaction" effect is peculiar to information actions;
g) information actions are usually prepared and carried out by competent specialists (experts) in this sphere.

Based on the above, the main categories of information actions are: disinformation, discredit, intimidation, compromising, lobbying, convincement, warning, propaganda, motivation (stimulus), blackmail (faking), etc. The listed information actions can be realized using the following methods (Prybut'ko, Luk'janec' 2007; Cyberspace… 2010; Stephen 2011): demonstration, information dosing, information reloading, context conflict, information imposing, neurolinguistic programming, emotion reorientation, fact substitution, psychological inversion, psychological pressure, psycholinguistic programming, psychological contrast creation, stamp (symbol) creation, image-building, inverse effect forming, psychological affect forming and others. These methods, as a rule, are used in preparing and realizing different briefings, meetings, conferences and other events with a wide public mass attraction. They are also used in radio broadcasts and telecasts, video, audio and Internet content distribution, mass and personal SMS and MMS sending by cellular communication, agitprops, films, printed matters, exhibitions, expositions, theatrical performances, public lectures, webinars and others cultural activities among the masses (Propaganda… 2014; Mondal 2015; Maliukevičius 2006). Considering the fact that information technologies are accessible to all civil social strata, recently the most effective technology for information actions is the use of electronic mass-media communication (Pyukke 2004; Techniques… 2014).

4. Cybernetic actions

In contrast with information actions, *cybernetic actions* have the following characteristics:

a) cybernetic actions are performed in cyberspace;
b) cybernetic actions do not have any geographic or time frames;
c) cybernetic actions have an asymmetric character;
d) cybernetic actions are performed in quasi-real time;

e) cybernetic actions are hidden and characterized by a high level of anonymity and uncertainty of objectives, locale and period of the play;
f) cybernetic actions' consequences, whether directly or indirectly, focus on global processes;
g) cybernetic actions' objects and subjects are social, technical and socio-technical management systems of a different hierarchy level and intended functions;
h) cybernetic actions are based on a complex methodology of force and facility application (main and adjacent);
i) cybernetic actions can be performed by both specialists and unskilled subjects.

In terms of influence on objects and subjects, the main areas of cybernetic actions can be:

– social management systems – methods are similar to information actions;
– technical management systems based on a hardware-and-software complex of automatized management systems – cybernetic influence methods are oriented on Denial of Service (DOS); unauthorized access to control information from a remote machine, remote to local (R2L); unauthorized access to local super-user privileges, user to root (U2R); ports scanning for getting sensitive information (PROBE);
– socio-technical management systems – a combination of the two mentioned cybernetic action methods.

To realize the methods of the described cybernetic actions in technical management systems based on a hardware-and-software complex of automatized management systems the following methods can be used (KDD Cup 1999): *back, land, neptune, smurf, teardrop, pod, apache2, mailbomb, processtable, udpstorm,* etc. – for a DOS attack; *ftp_write, guess_passwd, imap, phf, multihop, spy, warezclient, warezmaster, httptunnel, worm, name, sendmail, xlock, xsnoop, snmpguess,* etc. – for an R2L attack; *bufferoverflow, perl, rootkit, loadmodule, Ps, sqlattack, xterm.* etc. – for a U2R attack; *ipsweep, nmap, satan, portsweep, Mscan, saint,* etc. – for a PROBE attack.

Cybernetic action methods can be realized through both malware (computer viruses, network worms, Trojan horses, etc) implementations in information and communication systems and, also, special destructive information implementation into social and peer networks (Tikhomirov *et al.* 2014). In contrast with information actions that are realized mostly by electronic mass-media, cybernetic actions in relation to social management systems are realized by social Internet services (SIS). The most popular SIS are social networks, blogs, micro blogs and others. The use of SIS as the main cybernetic action instrument causes a control chaos generation and is characterized by the absence of a salient single control center. In spite of all differences between information and cybernetic actions, they have the following similarity – its forms, such as actions, measures, operations, campaigns and games.

5. Synergistic effects

The generalization of up-to-date world experience on synergistic effect's (caused by information and cybernetic interaction) place and role yields a *typical technology of synergistic effect generation* (Fig. 1).

Figure 1 shows that a synergistic effect occurs when the ICAs have only a sigle concept and plan correlated by time and space. Practical knowledge displays that the synergistic effect in most cases is initiated by information actions (first level of interaction), and, later, it is supplemented by cybernetic actions (second level of interaction). Let us consider the singularity of typical technology of the synergistic effect generation caused by information and cybernetic interaction (Fig. 1). After the concept formation and decision making to realize the ICAs, the influence target must be selected. Therefore, a concrete subject (or subjects) is defined. It can be individuals (citizens) or social groups, and, also, states or

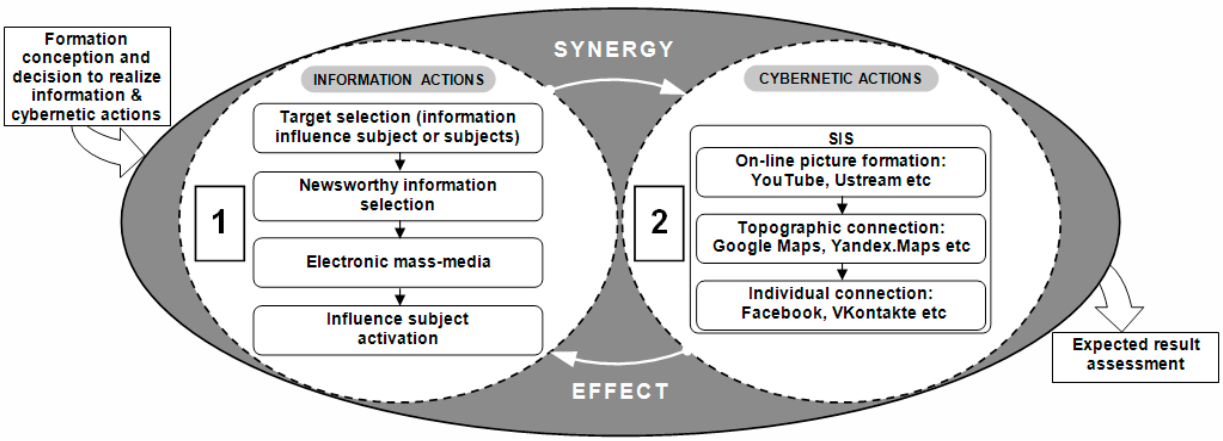


Fig. 1. Typical technology of a synergistic effect generation caused by information and cybernetic interaction

its coalitions. Next, for selected target, the most actual, newsworthy information must be selected, and it will be popularized through electronic mass-media to activate the influenced subject (subjects). The second level of interaction amounts to the target response assessment by using the SIS. In this case, the cybernetic action technology includes the following steps: 1) on-line picture formation using *YouTube*, *Ustream*, *Livestream*, *Smotri.com*, *Flickr*, *Bambuser,* etc; 2) topographic connection formation using SIS like *Google Maps, Yandex.Maps,* etc.; 3) individual connection formation by means of social networks (*Facebook*, *VKontakte,* etc.). The described sequence of operations builds a background for the formation of a directional synergistic effect. The nonlinearity effects from information and cybernetic interaction fade in as a result of the cyclical replication of the described steps. Therefore, early detection, assessment and prediction of the synergistic effect caused by information and cybernetic interaction will be an effective controller for the nonlinear effects which have a significant influence on the international security in the cyberspace.

Let us formalize the problem of the synergistic effect caused by information and cybernetic interaction assessment. Suppose that a same interaction matrix $E_{m\times n}$ has been formed as a result of information and cybernetic interaction:

$$E_{m\times n}=\begin{pmatrix} e_{11} & e_{12} & \cdots & e_{1j} & \cdots & e_{1n} \\ e_{21} & e_{22} & \cdots & e_{2j} & \cdots & e_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ e_{i1} & e_{i2} & \cdots & e_{ij} & \cdots & e_{in} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ e_{m1} & e_{m2} & \cdots & e_{mj} & \cdots & e_{mn} \end{pmatrix}, \quad (1)$$

where e_{ij} is the matrix element, $i=\overline{1,m}$, $j=\overline{1,n}$.

The value of matrix $E_{m\times n}$ (1) elements is defined as the result of information and cybernetic interaction. This interaction depends on the values of the matrix elements; it can have one of two possible effects – synergistic or system, and, also, information and cybernetic interaction can have no effects. In Figure 2, the principle of matrix (1) element formation as a result of information and cybernetic interaction by some k - th newsworthy information r_k, where $r_k \in R$, is presented.

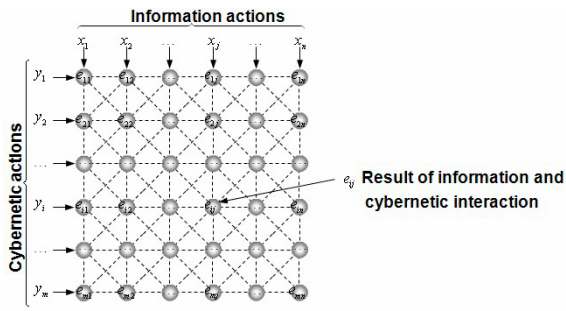


Fig. 2. Principle of interaction matrix element formation

Consequently, taking into account (1) and the principle of interaction matrix element formation shown in Figure 2, it is necessary to develop a methodology for the synergistic effect e_{ij} assessment, and, also, to find the trend accounting to which a well-timed detection and prediction of the synergistic effect in cyberspace would be possible.

6. Methodology for synergistic effect assessment

After analyzing the different nature of ICAs, it is sensible to assess the synergistic effect using a graphical analytical method. This method, in the process of defining the e_{ij} - th matrix element in (1), provides the following four steps for completion.

First step. Correlation coefficient $\tilde{N}_{ij}$ (between ICAs) is assessed using the following formula:

$$C_{ij}=\frac{\eta\cdot\sum_{z=1}^{\eta}x_{iz}y_{jz}-\sum_{z=1}^{\eta}x_{iz}\cdot\sum_{z=1}^{\eta}y_{jz}}{\sqrt{\left(\eta\cdot\sum_{z=1}^{\eta}x_{iz}^2-\left(\sum_{z=1}^{\eta}x_{iz}\right)^2\right)\cdot\left(\eta\cdot\sum_{z=1}^{\eta}y_{jz}^2-\left(\sum_{z=1}^{\eta}y_{jz}\right)^2\right)}}, \quad (2)$$

where η indicates the quantity of experimental observation over ICAs; x_{iz}, y_{jz} – the number of ICAs respectively; $z=\overline{1,\eta}$.

Second step. Metrics of self-similarity are assessed for ICAs. In this paper, as a means of self-similarity metric, the Hurst exponent (Nayman 2009) is used. This exponent, unlike most self-similarity metrics, not only provides trend detection in ICAs, but also allows defining its nature. The Hurst exponent calculation for information H_{Inf} and cybernetic H_{Cyb} actions is carried out separately with the following expression:

$$H=\frac{\lg\left(R/S\right)}{\lg\left(\eta*\pi/2\right)}, \quad (3)$$

where H indicates the Hurst exponent; S – the root-mean-square deviation of the observational series; R – the variation of accumulated deviation.

The value of the self-similarity metrics H_{Inf} and H_{Cyb}, respectively, according to Eq.(3) for ICAs depends on the quantity of experimental observation η and provides a possibility to not only detect the trend but also define its nature. For example, if the Hurst exponent (3) in place with information or cybernetic actions for observational series $\eta=30$ is in the interval $H\in\left[0,0.347\right]$, then the investigated actions are described by a non-persistent series, but in the interval $H\in\left[0.653,1\right]$ – by a persistent series. In the case of the Hurst exponent occurring in the interval $H\in\left[0.347,0.653\right]$ the ICAs with a probability of 99,73% have a random character and are described by a random series.

Third step. The definition of the e_{ij} -th element of the interaction matrix $E_{m\times n}$. With this object in mind,

the unit efficiency circle with its center at point O is built and the values of defined parameters (2) and (3) are intercepted on three axes OH_{Inf}, OC_{ij} and OH_{Cyb}, directed from the center of circle O at an angle of $\alpha=\beta=\gamma=120^0$ (Fig. 3).

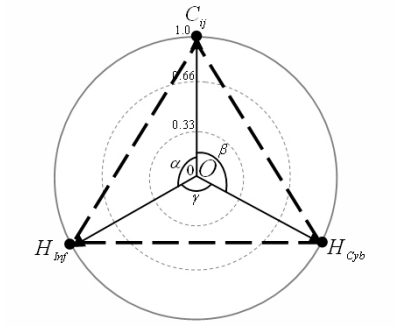


Fig. 3. Circular chart for synergistic effect assessment of the e_{ij} - th element of the interaction matrix $E_{m\times n}$

As seen in Figure 3, the parameters C_{ij}, H_{Inf} and H_{Cyb} are the vertexes of the triangle $\Delta C_{ij}H_{Inf}H_{Cyb}$. Consequently, the synergistic effect of information and cybernetic interaction e_{ij} can be assessed by the area of this triangle:

$$e_{ij}=\kappa^{-1}S_{\Delta C_{ij}H_{Inf}H_{Cyb}}, \tag{4}$$

where κ indicates the normalization coefficient, $\kappa=1.3$; $S_{\Delta C_{ij}H_{Inf}H_{Cyb}}$ – the area of the triangle $\Delta C_{ij}H_{Inf}H_{Cyb}$, $S_{\Delta C_{ij}H_{Inf}H_{Cyb}}=S_{\Delta C_{ij}H_{Inf}O}+S_{\Delta C_{ij}H_{Cyb}O}+S_{\Delta H_{Inf}H_{Cyb}O}$.

As Figure 3 shows:

$S_{\Delta C_{ij}H_{Inf}O}$ is the area of the triangle $\Delta C_{ij}H_{Inf}O$, $S_{\Delta C_{ij}H_{Inf}O}=\frac{1}{2}OH_{Inf}\ OC_{ij}\sin\alpha$; $S_{\Delta C_{ij}H_{Cyb}O}$ – the area of the triangle $\Delta C_{ij}H_{Cyb}O$, $S_{\Delta C_{ij}H_{Cyb}O}=\frac{1}{2}OH_{Cyb}OC_{ij}\sin\beta$; $S_{\Delta H_{Inf}H_{Cyb}O}$ – the area of the triangle $\Delta H_{Inf}H_{Cyb}O$, $S_{\Delta H_{Inf}H_{Cyb}O}=\frac{1}{2}OH_{Cyb}\,OH_{Inf}\sin\gamma$.

To correlate quantitative estimation results of the synergy of information and cybernetic interaction (4) and qualitative (linguistic) evaluation values, the proposed special normalized fundamental scale (Table 1) can be used.

Table 1. Normalized fundamental scale for synergistic effect assessment

Level	Parameter value, e_{ij}	
	Quantitative	Qualitative
Emergent	1–0.44	Synergistic effect
Boundary	0.43–0.12	System effect
Brownian	<0.11	Non-effect

As a result, if the synergistic effect is present $e_{ij}\in\left[0.44,1\right]$ (Table 1), the investigated system takes on the properties of an emergent. The described procedure is repeated for all interaction matrix $E_{m\times n}$ elements.

Fourth step. Synergy interaction trend finding. Let us assume that the synergistic effect of information and cybernetic interaction W by some k-th newsworthy information r_k consists of partial synergistic effects on any interaction steps:

$$W=\sum_{i=1}^{n}w_i, \tag{5}$$

where w_i – gain on any interaction steps, $w_i=e_{ij}$.

The set of step by step synergy controls $\left(e_{11},e_{12},\ldots,e_{mn}\right)$ is the control of the synergy interaction integrally:

$$e=\left(e_{11},e_{12},\ldots,e_{mn}\right). \tag{6}$$

Then a formalized trend of synergy interaction e^*, for which the total synergistic effect (5) is directed to the maximum, must be found:

$$W^*=\max_{e\in E}\left(W\left(e\right)\right). \tag{7}$$

7. Example of the use of the proposed methodology in civil aviation

It is assumed that a global economic crisis gives an opportunity to newsworthy information and that an N – th aviation subject is regularly the target of information and cybernetic influences from business rivals and other intruders. The information influences present actions directed against the aviation subject's *management, staff, customers* and *partners*. Cybernetic influences are realized by way of cyberattacks directed on such components of the CAIS as: information systems, communication systems and information and communication systems. Let us assess the synergistic effects from information and cybernetic interaction and also define the most vulnerable spots of this interaction.

The general interaction matrix $E_{m\times n}$ (1) is traced to the following form:

$$E_{3\times4}=\begin{pmatrix}e_{11}&e_{12}&e_{13}&e_{14}\\e_{21}&e_{22}&e_{23}&e_{24}\\e_{31}&e_{32}&e_{33}&e_{34}\end{pmatrix}, \tag{8}$$

And, in a graphical interpretation, it can be presented in the form illustrated in Figure 4:

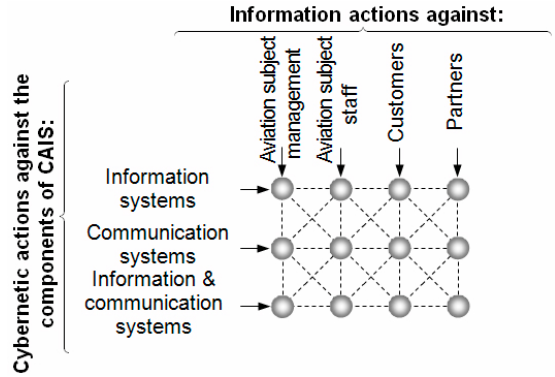
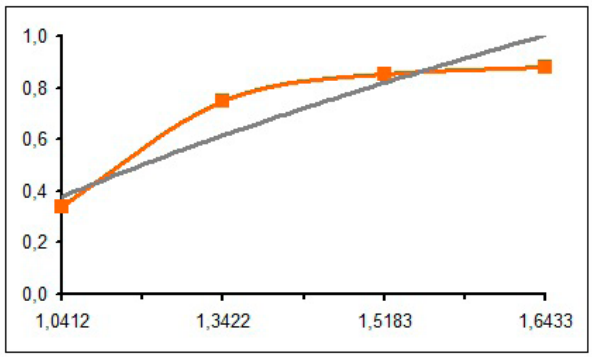


Fig. 4. Interaction matrix for the given example (CAIS)

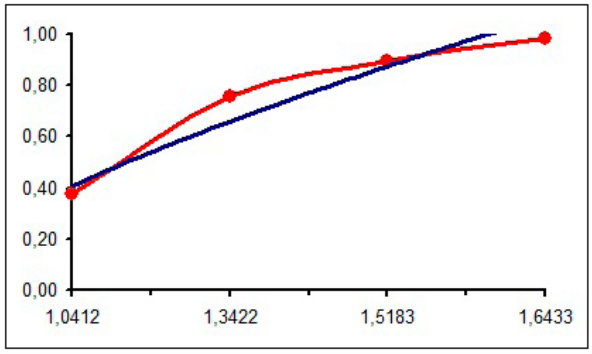
The interaction matrix $E_{3\times4}$ elements must be calculated from the first element e_{11}. The correlation coefficient C_{11} is defined using (2) and input data (Table 2) in relation to the defined subjects of information influence (in this case it is *aviation subject management)* and objects (component of the CAIS) of the cybernetic influence (in this case it is *information systems)*. The correlation analysis shows that coefficient $C_{11} = 0.56$, and this points to the fact of a positive correlation connection existence (caused by information and cybernetic interaction).

Table 2. The set of input data

Date	Number of actions		Date	Number of actions	
	Information	Cybernetic		Information	Cybernetic
08.03.2015	8	1	22.03.2015	13	2
09.03.2015	14	2	23.03.2015	18	3
10.03.2015	6	5	24.03.2015	19	1
11.03.2015	9	1	25.03.2015	15	1
12.03.2015	12	1	26.03.2015	8	1
13.03.2015	5	1	27.03.2015	8	1
14.03.2015	2	1	28.03.2015	12	2
15.03.2015	3	2	29.03.2015	15	2
16.03.2015	23	15	30.03.2015	2	3
17.03.2015	22	15	31.03.2015	12	1
18.03.2015	25	9	01.04.2015	17	1
19.03.2015	22	11	02.04.2015	9	1
20.03.2015	7	6	03.04.2015	19	1
21.03.2015	9	4	04.04.2015	15	2



a)



b)

Fig. 5. Results of the R/S – analysis: (a) – information actions; (b) – cybernetic actions N

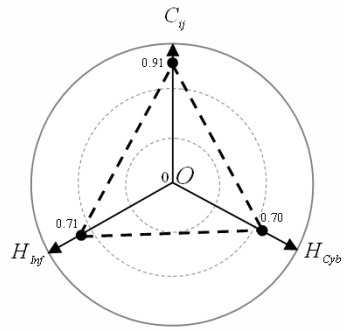


Fig. 6. Circular chart for the synergistic effect assessment of the e_{11} - th element for the interaction matrix $E_{3\times4}$

The calculation of the self-similarity metrics was carried out by a known method (Nayman 2009) and the complete results are shown in Figure 5.

The calculated parameters C_{ij}, H_{Inf} and H_{Cyb} (using Eq. (2) and (3)) were intercepted on a circular chart (Fig. 6) and in accordance with (4) the quantitative estimation value of the synergistic effect is obtained: $e_{11} = 0.77$. Given the quantitative value with regard to a normalized fundamental scale (Table 1), it may be declared that the information influence on the aviation subject's management and cybernetic influence on its information systems have caused a synergistic effect in the aviation subject (and as a consequence of this – a synergistic effect in civil aviation).

Afterwards, the procedures described are repeated for the calculation of other interaction matrix $E_{3\times4}$ elements and the matrix takes the following form:

$$E_{3\times4} = \begin{pmatrix} 0.77 & 0.55 & 0.67 & 0.32 \\ 0.32 & 0.48 & 0.78 & 0.53 \\ 0.61 & 0.14 & 0.45 & 0.59 \end{pmatrix}. \quad (9)$$

Taking into account the interaction matrix (9) and Figure 4, the trend of the synergy interaction can be defined by the synergistic effect parameters $e^* = (e_{11}, e_{12}, e_{23}, e_{34})$, which provide the maximum synergistic effect $W^* = 2.69$.

7. Conclusions

This paper shows that the ICAs with a single concept and plan in the cyberspace correlated by time and space results in the synergistic effect generation. The developed methodology is a theoretic basis for a prior detection, assessment and prediction of the synergistic effect of information and cybernetic interaction in information and communication systems (particularly in aviation subject CAIS). The obtained quantitative and qualitative results of the synergy assessment allow developing effective preventive and countermeasures against destructive information and/or cybernetic influences. Civil aviation, like other critical spheres, can use the proposed methodology as a tool to provide security against cyberthreats.

References

Cyberspace Operations Concept Capability Plan 2016–2028. 2010. Department of the Army Headquarters, United States Army Training and Doctrine Command (TRADOC Pamphlet 525–7-8) Fort Monroe, Virginia 23651–1047: 77.

Danik, J. G. 2011. Osnovni aspekty paradygmy kibernetychnoi' bezpeky [Basic aspects of cybernetic security paradigm], *Naukovyj visnyk Instytutu mizhnarodnyh vidnosyn NAU* [online], [cited 21 September 2016]. Available from Internet: http://jrnl.nau.edu.ua/index.php/IMV/article/view/3171 (in Ukrainian).

Gnatyuk, S. O. 2013b. Kiberteroryzm: istorija rozvytku, suchasni tendencii' ta kontrzahody [Cyberterrorism: development history, current trends and countermeasures], *Bezpeka informacii'* 19(2): 118–129 (in Ukrainian).

Gnatyuk, V. O. 2013a. Analiz definicij ponjattja "incident" ta jogo interpretacija u kiberprostori [Analysis of "incident" definitions and its interpretation in cyberspace], *Bezpeka informacii'* 19(3): 175–180. (in Ukrainian).

Haken, H. 1993. *Advanced synergetics: instability hierarchies of self-organizing systems and devices.* Springer-Verlag. 356 p.

Hryschuk, R. V. 2011. Ataky na informaciju v informacijno-komunikacijnyh systemah [Attacks on the information in information and communication systems], *Suchasna special'na tehnika* 1(24): 61–66 (in Ukrainian).

Hryschuk, R. V.; Chernyshuk, S. V. 2013. Metodyka ocinjuvannja rivnja nebezpeky kibernetychnyh zagroz [Method of security assessment for cyberthreats], *Suchasnyj zahyst informacii'* Specvypusk, 23–28 (in Ukrainian).

Hryschuk, R. V.; Danik, J. G. 2013. Osnovy zabezpe-chennja kibernetychnoi' bezpeky sudnoplavstva [Basis of cybersecurity ensuring in shipping industry], in *Mizhnarodna naukovo-praktychna konferencija "Informacijni upravljajuchi systemy ta tehnologii"*, 2013, Odesa, Ukraine, 172–174. (in Ukrainian).

Jardine, E. 2015. *Global cyberspace is safer than you think: real trends in cybercrime* [online], [cited 21 September 2016]. Available from Internet: https://www.cigionline.org/sites/default/files/no16_web_1.pdf

Kaspersky Lab. 2013. *Kaspersky security bulletin 2013*. [online], [cited 21 September 2016]. Available from Internet: http://media.kaspersky.com/pdf/KSB_2013_RU.pdf

KDD Cup. 1999 [online], [cited 21 September 2016]. Available from Internet: http://kdd.ics.uci.edu/databases/kddcup99

Kharchenko, V. P.; Korchenko, A. G.; Gnatyuk, S. O., *et al.* 2009. Kiberterrorizm na aviatsionnom transporte [Cyberterrorism in aviation], *Problemi informatizatsii ta upravlinnya* 4(28): 131–140 (in Russian).

Khondker, H. H. 2011. Role of the New Media in the Arab Spring, *Globalizations* 8(5): 675–679. http://dx.doi.org/10.1080/14747731.2011.621287

Korchenko, O. G.; Burjachok, V. L.; Gnatyuk, S. O. 2013. Kibernetychna bezpeka derzhavy: harakterni oznaky ta problemni aspekty [Cybernetic security of the state: characteristic features and problem aspects], *Bezpeka informacii'* 19(1): 40–45 (in Ukrainian).

Korchenko, O.; Vasiliu, Y.; Gnatyuk, S. 2010. Modern quantum technologies of information security against cyber-terrorist attacks, *Aviation* 14(2): 58–69. http://dx.doi.org/10.3846/aviation.2010.10

Maliukevičius, N. 2006. Geopolitics and information warfare: Russia's approach, in *Lithuanian Annual Strategic Review,* 121–147.

Milevski, L. 2011. *Stuxnet and strategy: a special operation in cyberspace?* [online], [cited 21 September 2016]. Available from Internet: http://www.academia.edu/872101/Stuxnet_and_Strategy_-_A_Special_Operation_in_Cyberspace

Mondal, D. 2015. Role of media in society – an analytical review, *International Journal of Research* 2(2): 107–123.

Nayman, E. 2009. Raschet pokazateley Khersta s tsel'yu vyyavleniya trendovosti (persistentnosti) finansovykh rynkov i makroekonomicheskikh indikatorov [Calculation of Hurst exponents to detect trends (persistence) of financial markets and makroeconomics indicators], *Ekonomist* 10: 18–28 (in Russian).

Propaganda, obman, dezinformatsiya – "Operatsiya po stabilizatsii" [Propaganda, deception, disinformation – "Stability operations"] [online] 2014. [cited 21 September 2016]. Available from Internet: http://www.tvernedra.ru/content/prousa.html (in Russian).

Prybut'ko, P. S.; Luk'janec' I. B. 2007. *Informacijni vplyvy: rol' u suspil'stvi ta suchasnyh vojennyh konfliktah* [Information influences: role in society and modern warfare conflicts]. K.: Palyvoda. 252 s. (in Ukrainian).

Pyukke, S. M. 2004. Metodologiya informatsionnogo vozdeystviya v sotsial'noy srede. Al'ternativnyy podkhod, Zashchita informatsii [Methodology of information influence in social environment. Alternative approach, information security], *Konfident* 1: 28–31 (in Russian).

Stephen, C. W. 2011. *Revealed: air force ordered software to manage army of fake virtual people* [online], [cited 21 September 2016]. Available from Internet: http://www.rawstory.com/rs/2011/02/18/revealed-air-force-ordered-software-to-manage-army-of-fake-virtual-people

Symantec. 2014. *Corporation Internet Security Threat Report 2014*, Vol. 19 [online], [cited 21 September 2016]. Available from Internet: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Techniques for visual information operations. 2014, *Army Techniques Publication.* No. 6–02.40. [online], [cited 21 September 2016]. Available from Internet: https://armypubs.us.army.mil/doctrine/index.html

The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict [online] 2012. [cited 21 September 2016]. Available from Internet: http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf

Tikhomirov, A.; Kinash, N.; Trufanov, A. *et al.* 2014. Network society: aggregate topological models, *Information Technologies and Mathematical Modelling* 487: 415–421. http://dx.doi.org/10.1007/978–3-319–13671–4_47

Tikk, E.; Kaska, K.; Rünnimeri, K., *et al.* 2012. *Cyber attacks against Georgia: legal lessons identified* [online], [cited 21 September 2016]. Available from Internet: http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

Toth, B. 2007. *Estonia under cyber attack* [online], [cited 21 September 2016]. Available from Internet: http://cert.hu/sites/default/files/Estonia_attack2.pdf

Welt, C.; Schmemann, A. 2010. *After the color revolutions: political change and democracy promotion in Eurasia* [online], [cited 21 September 2016]. Available from Internet: https://www.gwu.edu/~ieresgwu/assets/docs/PONARS_Eurasia_After_the_ Color_Revolutions.pdf