World Applied Sciences Journal 25 (3): 399-403, 2013
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2013.25.03.13316

Ensuring the Security of Critically Important Objects and Trends in the Development of Information Technology

Andrey Olegovich Kalashnikov, Yevgeniy Viktorovich Yermilov, Oleg Nikolayevich Choporov, Konstantin Aleksandrovich Razinkin and Nikolai Ilyich Barannikov

Voronezh State Technical University, Voronezh, Russia

Submitted: Aug 20, 2013; **Accepted:** Sep 29, 2013; **Published:** Oct 3, 2013

Abstract: This article examines specific vectors in the development of the IT sphere in the context of the security of the information-technological infrastructure of critically important objects. In the context of prospects for the development of the IT industry (inclusive of social networks and social development, staffing and creativity in youth, education and work activity, information weaponry and conflicts, legislation and the monitoring of effectiveness, measuring chance and risk, the growing level of complexity, the emergence of new threats and challenges), the author examines the attributes of information confrontation with an emphasis on critically important objects and elements of the country's critical information infrastructure. Given international and national statutes and regulations, the article examines the conceptual structure of the above objects, which are of primary importance to the security of the global community; note that these can be both military and civil or have a dual use. The article also examines international critically important objects and critical information infrastructures, which include the Internet domain name system, communication satellites, intercontinental cables and routers. In this regard, the article focuses upon an analysis of risks of disbenefit and chances of benefit in such systems.

Key words: Attack · Information weaponry · Information security · Critically important object · Damage · Risk

INTRODUCTION

The sweeping development of information technology (IT) is forming a global information space which creates new opportunities for economic growth, political modernization, cultural development, but at the same time paves the way to the emergence of new threats and risks, including new forms of conflict (information warfare, network confrontation, hacker attacks, etc.). As a result of these spreading around, the character of society changes and so, consequently, does the character of contradictions arising in it and forms of resolving those [1]. Developed countries get engaged in the creation of information weaponry, which comes to be employed by even terrorist and criminal forces.

The Information Security Doctrine construes the information security of the Russian Federation as a state of protectedness of its national interests within the information sphere, which are defined as an aggregate of balanced interests of individuals, society and the state [2]. Furthermore, information security (IS) comprises two major aspects: information-technical and information-psychological security. Ensuring information-technical security consists in the protection of, control over and adherence to legitimacy and order in the IT sphere (protection from unauthorized access, hacking into computer networks and websites, computer viruses and malicious programs, unauthorized use of frequencies, radio-electronic attacks, etc.). Whereas ensuring information-psychological security implies the protection of the psychological state of specific citizens, groups and collectives of citizens, society and the state from negative information impact [3].

Essentially, the vectors in the development of the sphere examined in the context of ensuring IS are seen as follows:

Corresponding Author: Andrey Olegovich Kalashnikov, Voronezh State Technical University, Moskovsky Prospect, 14, 394026, Voronezh, Russia.

- Society, the state and its regions will experience the growing significance of the humanitarian component of the issue of ensuring IS. Social networks will serve as catalysts for this process. Secret services will turn them into an arena for testing and employing not so much cybernetic but rather psychological weapons. Information-psychological confrontation in this theater of military operations will reach an unprecedented scale [4].

The hyper-popularity of social networks and "melting" of natural resources will provoke attempts of takeover of the information space with a view to gaining an economic advantage at the inter-state level.

Most social actions will be inconceivable without the "global web". Elections, protests and other public actions will increasingly actively employ the virtual space. The image and rating of politicians will, to a large degree, be formed on the Internet, which will become a basic playground for pre-election campaigns, including those of a regional scale, which, in turn, will require effective protection of the population against destructive information impacts. The information-psychological hygiene and protection of individuals, various social groups and society on the whole will become a norm in life and a sphere of activity for specialized institutions.

- Specialist staffing in the IS sphere will undergo radical changes. Outmoded educational models will disappear in this area. We'll have to shift from mass production to piecemeal production of IS specialists based on employers' target orders, including the preparation of higher qualification human resources. Note that special significance will be attached to the moral traits of IS engineers, who, as Charlie Chaplin put it, are "able to not only install the glass but break it too".

Creative and IT-savvy youth (oriented towards not routine but rather creative activity) will make up the core of "information SWAT teams". The quality of IS staffing will be decisive to the outcome of information confrontation.

- Just like education itself, work activity following it will have an increasingly at-a-distance nature. The workplace of most people will be fixed in the information not physical space. Wireless networks will ensure any employee's virtual presence at production meetings and other business events. However, guarding commercial and business secrets, as well as protecting any other confidential information, will in this case become a substantial problem, especially in conditions of innovative development of competitive products.
- The sophistication and destructive effect of information weaponry will reach such a level that it will be compared to other kinds of weapons of mass destruction, including non-lethal ones. Information-cybernetic and information-psychological means of attack will be used widely by terrorist institutions, which will make us radically reconsider our anti-terrorist agendas.

The information arms trade will become a part of the circle of criminal interests alongside drugs and regular weapons.

Subdivisions of cyber- and information-psychological security will be created on a mandatory basis not only for general staffs but troops (at least at the squad level), including the creation of a new line of troops – cybernetic.

- In the information sphere, substantial changes await legislation, especially in the area of protecting information and ensuring information security. Legislative acts will rely in their articles on the balance of public benefit chances and social disbenefit risks in the law-enforcement practice the monitoring whereof coupled with statistical assessment of benefit and damage will become a regular analytical practice.
- The multidimensionality, structural diversity and component heterogeneity of information technology and systems, the degree of sophistication and massiveness of malicious impacts on those will make us employ not determinate but probabilistic models; therefore, the methodology of risk analysis will become an indispensable attribute of assessing the real protectedness from computer and other information attacks. Through this prism, we'll have to view all cyber-crime threats, from piracy to hacking, keeping in mind that security is a state where risks do not go beyond an acceptable level [5, 6, 7].

Furthermore, the statistical monitoring of the damage size and attack perpetration frequency will become a norm in practices on ensuring IS, both for large corporations

and smaller and medium businesses across a range of sectors. Thus, the issue of risk control will become overriding not only in the mid-run but in the strategic run of things as well [5]. This aspect will be especially important for critically important objects and elements of the information infrastructure [8-18].

When it comes to information-technological components of information confrontation, especial risks will be brought about by impacts on critically important objects (CIO's) and elements of the country's critical information infrastructure (CII). Violation of the security of the information infrastructure of power, transport and armament systems can lead to a more devastating aftermath than if they were attacked with regular weapons. Therefore, in Russia, the US and the EU countries, the protection of CIO's and the CII will become one of the major areas of ensuring national security, since CIO's and the CII are crucial to maintaining public order, economic stability and integrity in any given country, especially developed countries [8].

Each country defines its CIO's and CII on its own, in consonance with its national traditions, social and political reasons, as well as geographical and historical attributes [9]. In this regard, the USA Patriot Act defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [10].

The 2009 SCO Accord on Information Security defines critically important infrastructures as "a country's objects, systems and institutions, impacts on which can have consequences that directly affect national security, including the security of individuals, society and the state" and information infrastructures as "an aggregate of technical means and systems for forming, creating, transforming, transmitting, using and storing information".

The main attribute of the critical infrastructure is its key significance to the security of society and the state. Note that CIO's and the CII can be military and civil objects and have a dual use as well [1]. Some works [12-18] juxtapose the Russian and American views on the critical infrastructure.

Apart from national, there are international critical information infrastructures, which include the Internet domain names system, communication satellites, intercontinental cables and routers and other information objects [1].

It's clear that information risks for all the above objects and structures will only be increasing.

- The lop-sidedness of assessing the effectiveness of functioning of IT systems will be overcome. Measuring chance in combination with risk analysis will open up real prospects of proper control of the general effectiveness of such systems and forecasting [19-23] within the revolutionally developing information space, which will be the case at the regional and municipal level as well. In this regard, there will be high demand for the creation and development of specialized mathematical and methodical support for decision-making by authorities and corporations, including the creation of situational centers capable of processing in real time large amounts of incoming socio-economic and personal data. Information-analytical assistance, many can presently only dream of, will become a regular service in network and "cloud" technology, which will also have to be dependably protected from computer attacks and computer reconnaissance and do so at the regional level as well [19-23].
- The increasingly growing level of complexity of IT used in all spheres of life will lead to the impossibility of detailed examination of products supplied by outside vendors of software-hardware complexes for conformity with security requirements. This will make us shift from the notion of "protectedness requirements" to the notions of "the level of real protectedness" and "the level of trust", which, in turn, will require corresponding changes to the statutory and regulatory space on the part of regulators.
- In conditions of the constantly changing dynamic of the internal and external environment and emergence of still newer threats in various spheres of activity in society and the state, there will be a gradual transition from the doctrine of "control with maximum effectiveness" to the doctrine of "control via expected chance and risk".

This is the way we picture the innovative trends in the development of the IT sphere in the context of ensuring its security, on the whole and the security of CIO's and the CII, in particular. It is the aspect of cyber-protection of critically important objects and infrastructures that is the most crucial in this context, since attacks on the them can have disastrous

consequences. Note that the key element of this protection is, no doubt, risk analysis and risk control for the above structures subjected to information attacks.

Major scientific publications in this area mainly address various types of threats, attacks and damage [18-23] with respect to computer and telecommunication systems in wide use.

Note that CIO risk analysis attempts mainly have an expert non-analytical nature, which hinders optimization and control. On the other hand, the probabilistic theory of extreme distributions, which offers a certain analytical apparatus, leaves out the size of damage, which is acceptable only in fatal risk assessments.

In this regard, the priority seems to be with the objective of developing the methodology of temporal risk analysis in application to the most crucial state variables of attacked automated systems of control of technological processes of CIO's.

REFERENCES

1. Fyodorov, A.V., 2008. Information Security in the Global Political Process. M.: MGIMO (U), pp: 73.
2. The Information Security Doctrine of the RF. Ratified by the President of the RF on 9.09.2000, # Pr-1895.
3. Korotkov, A.V. and Y.S. Zinovyeva, 2012. The Security of Critical Information Infrastructures in International Humanitarian Law / Political Science, pp: 154-161.
4. Gubanov, D.A., D.A. Novikov and A.O. Kalashnikov, 2010. Theoretical Game Models of Information Confrontation in Social Networks // Managing Large Systems, 31: 192-204.
5. Kalashnikov, A.O., 2011. Models and Methods for the Organizational Management of Corporations' Information Risks. // M.: Egves, pp: 312.
6. Zhukov, M.M., Y.V.O.N. Yermilov, Choporov and A.V. Baburin, 2012. Building a Risk Model for the Components of a Distributed System Based on a Given Damage Distribution Law // Information and Security, 15(4): 449-460.
7. Zhukov, M.M., Y.V. Yermilov, N.I. Barannikov and I.P. Nesterovsky, 2012. The Specifics of Building Multi-competent Systems with Given General Risk Parameters // Information and Security, 15(4): 567-570.
8. Major Areas of State Policy in the Area of Ensuring the Security of Automated Systems of Control of Production and Technological Processes of Critically Important Objects of the Infrastructure of the Russian Federation. Ratified by President D.A. Medvedev on 03.02.2012, # 803.
9. International Critical Information Infrastructure Protection Handbook 2008 / 2009. / Ed. by Wenger, A., Mauer, V. and Cavelty, M. Center for Security Studies, ETH Zurich., 2009.
10. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162.
11. Andreyev, O.O., 2008. Critically Important Objects and Cyber-terrorism. Part 1. A Comprehensive Countering Approach. / Andreyev, O.O. et al. Edited by Vasenina, V.A. M.: MTsNMO, pp: 37.
12. Executive Order 13010—Critical Infrastructure Protection. Federal Register, July 17, 1996. 61(138).
13. White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive, pp: 63.
14. Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, Federal Register, 66(196), (October 8, 2001)
15. U.S. Department of Homeland Security, The National Strategy for Homeland Security, July 16, 2002.
16. White House, Executive Office of the President, The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, (February, 2003).
17. Homeland Security Presidential Directive 7, HSPD-7, December, 2003.
18. Rauscher, K. and A. Korotkov, 2011. Working Towards Rules for Governing Cyber Confict. Rendering Geneva and Hague Conventions in Cyberspace. East-West Institute, URL:www.ewi.info/working-towards-rules-governing-cyber-confict.
19. Pakhomova, A.S., O.N. Choporov and K.A. Razinkin, 2013. Advanced Persistent Computer Espionage Threats: Symptoms, Principles and Implementation Methods // Information and Security, 16(2): 211-214.
20. Ryabkov, V.Y., A.P. Pakhomov and N.I. Barannikov, 2013. On the Application of Methods of Visual Analysis of Multivariate Data in the Area of Information Protection // Information and Security, 16(2): 259-260.

21. Ostapenko, A.G., 2010. The Possibility Function in Assessing Risks, Chances and System Effectiveness // Information and Security, 10(2): 185-194.
22. Yermilov, Y.V., Y.A. Popov, M.M. Zhukov and O.N. Choporov, 2013. Risk Analysis of Distributed Systems Based on Their Components' Risk Parameters // Information and Security, 16(1): 123-126.
23. Ostapenko, G.A., D.G. Plotnikov, N.Y. Shcherbakova and N.I. Barannikov, 2013. Models for the Survivability of an Attacked Distributed Information System: Risk-formalization Inclusive of Possible Damage // Information and Security, 16(1): 63-68.