Irada Y. Alakbarova
Institute of Information Technology, ANAS, Baku, Azerbaijan
airada.09@gmail.com
DOI: 10.25045/jpis.v06.i2.04

PROBLEMS CREATED BY CYBER-CONFLICTS AND METHODS TO SOLVE THEM

The article analyses the problems related to conflicts over information in cyberspace and the purposes behind cyber-attacks. The classification of the tools of information conflicts in cyberspace is studied. The methods to choose the most effective information security tools during cyber conflicts are proposed.

Keywords: *cyber-conflict, cyber-environment, information security, net-war, cyber-attack.*

Introduction

The rapid development of information and communication technology (ICT) makes it almost impossible to predict its exact consequences, and substantial funds, time and knowledge are required to overcome any negative outcome. New technologies, projects, and programs in the global network may seem benign and helpful at first glance, but experience shows that in many cases it is impossible to avoid problems completely. For example, social networks, open encyclopedias, blogs and other projects have become the main fields of activity of Internet users. However, information manipulation and disinformation are common for these projects.

The Internet is expanding in the sense that more servers are connected to the network, information availability is increasing, and the number of users is increasing. The expansion of computer networks enables the use of network technologies in cyber-conflicts and enhances the coordination, scalability and complexity of the activities of network users. This expansion also increases cyber-conflicts and causes more experienced and equipped users to initiate cyber-conflicts [1].

Organised crimes perpetrated by secret social networks operating in cyberspace have a devastating impact on the state and society and on the country's economy in particular. Today, new challenges such as dark webs, the underground economy and covert networks are emerging in cyberspace. Covert networks are the main coordinating tool in human trafficking, cybercrime and terrorism and are being used more often in cyber-conflicts.

The penetration of modern ICT in different areas has led to the emergence and expansion of unfavorable incidents such as network wars, cyber-attacks, cyber-crime, cyber-conflicts and cyber-terrorism. Since the above-mentioned information operations are influential, the problem of national information security support in cyberspace is the most pressing problem for governments. Currently, government agencies and various coalitions, large companies and political parties and groups (including terrorist groups) are participating in cyber-conflicts. The research shows that the targets of information attacks in cyberspace include critical infrastructure (energy systems, transport, government offices, banks and financial offices) of the government, citizens and various information resources [2, 3].

Basic cyber-conflict concepts and terms

The origin of the word "cyber" comes from the word "cybernetics", which stems from the ancient Greek term "kibernetes" and means "to manage". With the development of Internet technologies, new words emerged from the word cyber, which are related to the Internet and virtual reality [4].Cyberspace was first used by the Canadian science fiction writer William Gibson in 1982. In the following studies, the author defines the cyberspace as a "universal nightmare" [5].

The cyber ecosystem is global and dynamic, and covers hundreds of thousands of networks and millions of devices. The notion of cyberspace is defined by official bodies of several countries in different ways. For example, the documents related to the national strategy on

cybersecurity in the United States state that cyberspace consists of hundreds of thousands of interconnected computers, servers, cables, communication switches, which ensure the normal operation of the government's critical infrastructure. This means that cyberspace plays an important role in national security and the development of the economy. The documents also indicate that cyberspace is associated with real geography and is the key element of geopolitics. Thus, communications, servers and technical relations have a geographic localisation. Yet, cyberspace is also associated with nations in terms of its domain zones, language and state control. Cyberspace characterises the physical geography through various services, navigation devices, technical gadgets and mobile devices, sensors that create an interactive map of facilities, information flow and people [6].

Cyberspace is a medium through which cyber-operations are realised. In cyberspace, information operations include attacks, defence measures and investigations [1, 4].*The Economist* declared cyberspace as the fifth war medium after land, sea, air and space. Cyberspace differs from these media as it is created through ever-evolving ICT. The US and some developed European countries are training special cyber-soldiers to participate in cyberwars [7].The term cyberwar was first used in the article "Cyber War Is Coming!" by Arquilla and Ronfeldt in 1993 [8]. Using the notions of cyberwar and network warfare, the authors tried to prove that modern network wars are capable of creating more serious problems than we can imagine. Studies have claimed that "cyber-terrorism", "cyber-conflict", "network warfare" and "cyber-attack" are not synonymous terms. Nevertheless, each of them is closely linked to the Internet and computer networks, which means that they have much in common. Using computer networks, cyber-terrorism aims at undermining the critical infrastructure of the state or psychologically influencing citizens. The dependence of economic and governmental systems on networks has increased the risk of cyber-terrorism [2, 6, 9].

Causes and stages of emerging cyber-conflicts

Conflicts in cyberspace are part of information war, and cyber-conflicts are emerging in various forms from conflicts begun in social networks to hacker attacks and the capture of domain names that reflect national values. These conflicts area manifestation of the contradictions between the object and subject, and cyber-conflict is a stark in consistency in cyberspace [9]. Cyber-conflict can be covert, dangerous, passive, and insidious, and covers the operations as the destruction of financial systems, as well as neutralisation of network protection.

To analyse cyber-conflicts, the source of these conflicts and their expansion should be studied. They can be due to:

1. lack of mechanisms to monitor the global network;
2. an increasing number of network users;
3. users' anonymity, using the proxy server;
4. gaps in the network;
5. automation, eliminating time and space dependence on the network;
6. challenges regarding legal cooperation in cyberspace.

In terms of their scale, complexity and other properties, cyber-conflicts are growing as the Internet expands. Cyber-conflicts cover various organisations, societies, nations and states, and are becoming more global [10].Cyber-conflicts are complex, dynamic processes that incorporate the following phases:

- the objective situation or objective reasons for cyber-conflicts;
- the impact of the conflict in terms of the expansion of cyber-conflicts;
- solutions for cyber-conflicts (full or partial).

Cyber-conflicts have two sides: cyber-defence and cyber-attacks. Defensive operations and attacks are based on decision support systems and their security issues [11].Cyber-defence is a cyber-operation aimed at the detection, analysis and modification of information in cyberspace,

and notification about unauthorised interventions. The two types of cyber-defence are passive and active. Active cyber-defence includes the active detection and analysis of network attacks, the elimination of disturbances arising from the failure of network security in a short period of time, and countermeasures taken in real time. Passive cyber-defence includes the theft and control of confidential information using network intelligence tools and solving information security issues. As political and economic tensions increase in the community, the more cyber-conflicts will grow, and in most cases, passive cyber-defence will be replaced by active defence [9, 11].

Globalisation has caused challenges in cyber-defence operations. The interaction between information systems and networks causes many challenges related to information security, so that we cannot be completely sure of the absence of weak points in the network. In addition, modern technology used in cyber-conflicts obscures solutions to these challenges [10, 11].

Cyber-attacks use different ICT tools to perform the following operations: replacing and copying information transmitted through the network, limiting the requests of legal users, transmitting misinformation and damaging the functionality of information resources. Cyber-attacks use available ICT tools to extract necessary information from the targeted network, which damages information exchange. Cyber-attacks remotely control the applications in government and corporate information systems. Reducing the efficiency or destroying the functionality of structural elements of the network are the basic operations performed in cyber-attacks. Robot intervention, denial of service attacks (DoS) and malicious applications are the most commonly used methods to reduce the effectiveness of separate elements of the network. The cyber-attack was first accomplished by hackers using specific information software [12].

The scope of cyber-attacks covers military, economic, banking, social and other fields, and aims at:

- failure of control structures, traffic and communication;
- limiting or isolating the activity of enterprises, banks and various production areas by damaging multiple technological connections and mutual account operations, and implementing financial fraud;
- organizing large-scale industrial accidents within the territory of the opponent by abusing the control of technological processes and facilities related to high concentrations of dangerous industrial chemicals and materials;
- manipulating and proliferating ethical stereotypes, ideas and behaviours;
- causing confusion and dissatisfaction among the population, as well as destructive activities between different social groups.

Cyber-attacks are carried out through the following special structures [11, 12]:

- managing computer and communication systems of governmental organisations;
- military information infrastructures engaged in the management of the armed forces and military equipment, and the collection and processing of information for the interests of armed forces;
- information and management structures of banks, transportation and manufacturing facilities.

Cyber-attacks can be due to internal and external sources. Internal sources include errors caused by system failure, accidental errors caused by company employees and intentional errors caused by employees. External sources include cyber-attacks by hackers, transmission of viruses, criminal groups, activists with particular ideology, terrorists and foreign government agencies.

Efficiency in cyber-conflicts

Efficiency in cyber-conflicts can only be acquired under certain conditions including detecting unauthorised interference and preventing attacks against the information network [13].

Basic terms to be considered in cyber-conflicts are the subject of the conflict; the parties of the conflict; conditions for sustainable cyber-conflict; the scale of cyber-conflict (organisational, states, and so on);the strategic and tactical behaviour of the parties; and the consequences of cyber-conflict.

Negative consequences of cyber-conflicts may include:

- crash of production processes through changing or preventing the flow of information;
- crash of production processes through work delays and damage to installations, causing a threat to people's lives or a negative impact on the environment;
- encouraging the operators to take false steps by sending them deceptive information, and thus disrupting the performance of the organisation and causing economic losses;
- destruction of the software to prevent failure of the system;
- failure of the system through malicious applications and information theft;
- inflicting danger toward people through security system termination.

The following conditions must be provided to avoid cyber-conflict:

- the source of conflict should be defined;
- the software and hardware (conflict tools) used in the conflict should be analysed;
- the type of conflict should be defined;
- the causes of the conflict should be studied;
- the characteristics of the conflict should be identified.

Three aspects of the cyber-conflict should be considered to address cyber-conflicts:

1. detecting an unauthorised intrusion to the network promptly and taking appropriate measures;
2. preventing the network load.
3. organising counter-measures by controlling the network of the opponent(i.e., manipulating the information resources on the network, spreading misinformation, network failure).

The above-mentioned aspects of the conflicts that occur in computer networks define the main target of the cyber-conflict, and prove that traditional information security features are not sufficient to establish an information protection system. At the same time, a system should be developed that is capable of solving the problems regarding information security, unauthorised access and counterattacks.

Cyber-kinetic operations are widely used in cyber-conflicts. Cyber-kinetic operations ensure the network's resistance to external and internal unauthorised interference, which is the primary information security issue. System adaptation, quickly predicting potential cyber-enemies and the availability of self-organising features should be provided to resolve these issues.

Conclusion

The problems related to cyber-conflicts and cyber-crimes are newer than information warfare problems, having emerged with the expansion of the Internet. The problem covers almost all areas of human activity and requires taking adequate and advanced measures at the national and international levels. The consequences of cyber-conflict, such as controlling citizens' behaviour, damaging information resources or causing functional disorders, focus on causing significant economic crisis for opponents and increasing dissatisfaction among the population. This requires a solution for information security issues as one of the aspects of the state's economic and scientific-technical policy, before the country has joined the global open network.

State policy aimed at the legitimate interest in protecting the information and intellectual property of citizens and the government should be supported by the protection of the network across the country, and cyber-attacks must be prevented by all possible measures. The information security of the network requires a systematic and comprehensive approach including conceptual, organisational, scientific and methodological, legal, financial and technical aspects.

References

1. Alakbarova I.Y. Comparative analysis of information attacks in Internet // Information technologies and computer engineering, No.3 (19), 2010, pp. 81-87.
2. Imamverdiyev Y.N. Model of situational information security management of e-government // Information Technology. No 8, 2014, pp. 24, 33.
3. Alguliev R.M., Volodin A.V., Ustinov G.N. Some approaches to information security technology working on the Internet // Proc. rep. on the anniversary scientific and technical conference of the academic, scientific and engineering-technical staff MTUCI. M., 2001, pp. 265-266.
4. Imamverdiyev Y.N. New generation Information cybersecurity strategies // Society issues of national2013, №2 (8), 42-51.
5. GibsonW. Neuromancer, Ace Books, 1984, 271 p.
6. A. Klimburg, Ph Mirtl. Cyberspace and Governance. The Austrian Institute for International Affairs, 2012, 65 p.
7. http://www.economist.com/node/16478792
8. Arguilla J., D. Ronfeldt Cyberwar is coming! // Comparative Strategy, vol. 12, no 2, 1993, pp. 141-165.
9. Lewis JA Assessing the risks of cyber terrorism, cyber war and other cyber threats // Center for Strategic and International Studies, 2002, pp. 3-12.
10. P. Sawyer, Third World may start on the Internet // Computerworld Russia, Moscow, No 32, 2009, p. 29.
11. Ali IY Information warfare technologies, "Information Technologies" publishing house, Baku, 2012, 108 p.
12. Schmitt of cyber conflict MN // Conflict and Security Classification, 2012, vol. 17, no. 2, pp. 241-250.
13. Applegate SD, Stavrou A. Towards a cyber conflict Taxonomy / Proceedings of the 5th International Conference on Cyber Conflict, June 4-7, 2013, Tallinn, pp. 431-448.