J. Appl. Environ. Biol. Sci., 5(7S)8-13, 2015

© 2015, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental
and Biological Sciences
www.textroad.com

Study on the Way of Securing Space and Exchanging Information Electronically

Ali Rezaei Khou and Younes N. Andish

Department of Law, Yasouj Branch, Islamic Azad University, Yasouj, Iran

Received: March 19, 2015
Accepted: May 2, 2015

ABSTRACT

The dominance level of information and communication technology in Iran has increased dramatically in the late 2000, so that it has been became toan independent variable for expression of some political and social changes. This study investigated the effect of internet and cell phone, as two main symbols in the age of information technology, on national security of Republic Islamic of Iran in the decade of 2000. The mentioned investigation is performed by utilizing Chaos Theory of James Rozena in terms of three parameters including micro, macro and mixing (micro-macro). The basic hypothesis is that" although the impact of developments related to these technologies is not a serious threat, but it shows the vulnerability of country for a wave changes. In this regard, the disputes between government and a group of people, the increase of foreign actors and opposition groups' activities against government, threatening the religious values and undermining the national unity could be noted which it requires basic solutions and not periodical conflictions.
KEYWORDS: Information Technology; Internet; National Security; Information Exchange; Cyberspace.

1. INTRODUCTION

Nowadays, the information agent has changed the human life and created the dissociation pattern in the foundation of economic, society and culture so that it is viewed as an independent index to define a new period in the history of human transformations. Of course, the entering into new period does not mean the loss of past order, rather, the new world has overlap with old one in which the power dependency to the institutions based on geography continues to be valid (Rozena and Sing, 2012 p.389). This reflects the continuing importance of the territorial and political extreme attention to national security (Bozan, 2000 p. 99), as the national security returns to existence and survival of a country. Considering the significant of this issue, in here the main focus is on the impact of new technologies on Republic Islamic of Iran's national security, because our society, as a young society continually has been trying to experience and effort to achieve facilities for promotion of its development level and global communications. So, the better understanding of modern technologies to develop society is necessary to exploit opportunities and confront threats with clear vision and away from extreme pessimism. Among different technologies, the focus is on internet and cell phone. This is due to the high influence of these two technologies in Iran as well as their quality and special characteristics which make them distinct and symbol of information age.

The History of Cybercrime:

The history of cybercrime may be attributed to the time when Abacus was entered into the human's calculations. But this question is raised that "Do the unauthorized use of Abacus in that time or even the use of Pascal summing machineand Leibniz calculating machine in the times after that were criminalized or not?" As we know, according to the legality principle of crimes and punishments, any act or omission for which the punishment has been determined under law is crime and nothing else (Khaje Servi, 1999, p.23). To prevent and control, the computer-related crimes have been mentioned in the manual of U.N. Determining the real time of first cybercrime committing is something difficult. The computer which has been existed from Abacus time, meaning 3500 BC in Japan, China and India, somehow has been discussed. In 1801 the financial incentives led to one of the textile factories' owner in French named Joseph Jacquard design the first PC card.

What is cybercrime?

The internet and cyber crimes are new ones. The broad spectrum of criminal acts followed this concept and the nature of their variable caused by momentarily advancement of information technology and the ways of exploiting it, make a comprehensive definition and free of conflict something difficult or perhaps impossible; as far as there has been no definition of these crimes in newest and most comprehensive international document in this field (2001 Budapest Convention on Cybercrime). It seems that this is the most complete definition:" Any crime that legislator explicitly has announced the computer as the subject or crime device of material element's minor offense, or the computer has role in terms of subject, committing means, saving device, processing or transferring crime reasons (Abdullahi Azagami, 1997 p.56). "

* **Corresponding Author:** Ali Rezaei Khou, Department of law, Yasouj Branch, Islamic Azad University, Yasouj, Iran

Types of Cybercrimes

Hacking:

Hacking is penetration into a computer system without having authorization, ownership or necessary qualification. It means overcoming on security systems of a computer system for illegal access into data stored in it.

Phishing:

Phishing is defined as trying to obtain information like password, account password or credit cart details by placing himself/herself as a reliable source. Phishing is done through email services and false promises or encouraging some internet users to enter their information into the sites made by swindlers via making some attractions. These swindlers usually design sites giving a sense of trust and entering into a secure site and normally they would succeed, meaning that they have fallen into the trap and would enter their information (Ardabili, p.47 2004).

Phishing attack:

It is a special type of cybercrime in which the offender creates a copy of almost 100% similartoa website of a commercial firm. Then he/she tries to deceive the users for disclosing personal details, username, password, PIN etc. via a form in fake website, allowing the offender make money through these information.

Phishers or phishing offenders use various techniques to deceive users and access to fake website. For example, sending e-mails that apparently are from a bank. These emails use logos and good commercial styles and the letterheads are designed in such a way that appears to be from legal bank. In general, these letters inform receivers that the bank has changed its IT infrastructure and request all customers to re-verify their user information. When the receiver clicks on the link in email, he/she will be directed to a fake site in which he/she enter his/her personal information (Zeraat, 2004 p.63).

Cyber stalking

Cyber stalking is the use of communications technology, particularly internet, to annoy people. Defamation, sending destructive softwares and destruction of data and computer equipments are in this group. These offenders mostly hunt users by using of chat rooms, forums and online communities, gaining their information (for example, phone number, address, workplace etc.) and whereby annoy their victims, do threatening emails, telephone harassment etc. which this case is one the most dangerous cybercrimes that has heavy penalty in global level (Aaskariyan, 1994, p.68).

The various types of cybercrimes have one thing in common, and this is: "illegal exploitation of new computer and communications technology to do misconduct activities (Teyyeb, 2011 p.57)

The production and exchange of police information:

.FATA acronym is a specialized police unit of Republic Islamic of Iran, launched in 23 January, 2011 and its task is fighting against cybercrimes, fraud and forgery in cyberspace and protection of national secrets on the Internet. The forming of "FATA police" does not mean the restriction of people and intervention in their privacy, rather, it is to prediction of new crimes in the new areas of Internet and social prevention. This attempt can be considered as the reaction of police to Stux net computer worm propagation as well as the fighting against cyberspace controlling by Iran government's oppositions (after Iran's unrest caused by election in 2010). The activity scope of this police is dealing with cybercrimes such as ethical, economical issues and even terrorism.

People's role in preventing cybercrimes

The people themselves disclose their information in cyberspace. In other words, there are people who have not enough information and without notice would chat with unfamiliar individuals. These people make their personal information subject to availability. In such a way that, these people are hacked by specialists, and consequently they would give their personal information to them. In addition, sometimes the individuals give the password of their acceleration card to site operators for buying a product from a website and as a result they pick money from theirs card. To prevent misuse by others, the password must not be put on the system or deleted after online payments including tuition and bills (Khomeyni, 1981 p.652).

Law on the security of network information

Different aspects of information security:

The information has long been significant subject and protection of information security (particularly some important information) has always been of paramount importance, but actually the first and most important issue in correct technique is not maintaining security, rather, it roots in definition of security and security breach. Till there is no security fundamental or agreement on it is clear that by addressing such an issue and focusing on cyberspace in the best form of legislation no significant problem will be solved.

For this reason the focus on "posterior" issues of information security should be founded on firmer principles called "priori" earlier which the consensus of state and nation is in the nature of security goals. So, the first question is that "which information and based on what information should be protected and what is the enforcement guarantee of it?The comparative study on foreign works about cyber information security law in most cases ends to cybercrime and responsibility law. In fact, the law of information security has been discussed in the text of cybercrime rules, studying reason, civil rights and privacy (Miawald, 2004); because in foreign law, there is national unity and constitution and main parts of issues that should be protected by law and the security of its information should be kept are existed. To more explanation, firstly we will be familiar with priori and posteriori of information security.

Priori and posteriori aspects of information security

The priori aspects of information security are related to most fundamental definition which the government presents about security and different types of it, and more exactly, they are a reflection of political system of a country; for example, the article 25 of Iran constitution states: "Inspection and failure to deliver the mail, recording and disclosure of telephone conversations, the disclosure of telegraphic and telex, censorship or failure to communicate and send them, eavesdropping, and any investigation is prohibited, unless according to the law." In fact, this part of individuals' privacy is a subject that has been protected in constitution and statutory has been required to prepare principles, rules and how to implement them for protecting this bright recognized in constitution.

By emphasis on this point that the above-mentioned article is confined only to governmental institutions having personal information of individuals and quite limited evidences- and it is possible to consider it the very simple and initial version of "data protection" and "privacy" rules. When this information is received to administrative and governmental institutions and these institutions somehow interchange it, they should necessary safety precautions to protect its content. Thus the act rules the protection of this content and the technical specialist should use these technical rules to protect information. The governmental institutions and legal regime of government information management are also an important issue in terms of information security. State is the biggest source of information production and access management or denial of access to this information is a subject to use rules and techniques of security. In political closed system, a big part of government's information is subject to privacy rules and usually many financial and human resources are spent to protect the security this information. In this system, there is the act of practical unavailability and it should be approved certain rules for free access to any part of governmental information (Ansari, p.45, 1996).

As a result, the security approach in this part is detailed, comprehensive and extensive and because there is practical act of access to governmental information, the legal and technical system should use necessary precautions to protect that vast part of information and any cost to secure this big informational structure is justifiable and its economic justification is subordinating priori issues of security and it goals. This priori approach is unlike countries in which the Freedom of Information Act has been approved or there is library system to access state information having a perfectly limited and case security perspective. In this case only a small part of governmental information is subject to privacy rules. While there would be an extensive range of principles to maintain information security which guarantee the citizens' access to governmental information. According to this perspective, European countries consider the application of information security rules something worthless and impractical (ArticleV of Guidelines for the Security of Information Systems and Networks, OECD, 2002). Therefore, discussion about logical costs of information availability is the main concern of these systems (Green, Paper on Public Sector Information in the Society, 1998).

Although in two opened and closed systems the costs are spent undoubtedly, the only difference is that in an open system due to the Freedom to Governmental Information Act, the small part of information issubject to privacy, consequently keeping privacy is better, more effective and less costly.

Information security

Safety means security against potential or actual threats that threatening existence and survival of a living entity, individual or community, have been described (Yazdi, 1384, p. 263).

A definition of security in computer science is minimizing the risk of unauthorized disclosure of information (King & Osmanoghlu, 2001: 74).Information security is a set of tools to prevent theft, assault, murder, espionage and sabotage (Hashemian, 1379, p. 37) and is the science of studying methods keeping of data in computer systems and communication to unauthorized access and changes (Abdullahi, 1375, p. 73). In fact, it can be said in the case of compliance with information security basically three attributes of "confidential information" (ie information is only available to those authorized, and the level of privacy with respect to the degree of importance of the information will be specify), " information correctness "(ie protection of the accuracy of the information and prevent from unauthorized changes and eliminate the information and appropriate processing it) and" access to information "(ensure that whenever the authorized users need, will have access to data) are provided (5-3, (Electronic information security, 2008).From a purely legal view, information security is typically in terms of computer crime, electronic commerce, electronic signatures and digital signatures has been appeared (UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, 2001). OECD (Organization For Economic Cooperation & Development) in it definition is attend to security purpose and says that: the purpose of information systems security is protect the interests of those who have confidence against defects in information systems availability, confidentiality and integrity (Directive OECD, 1992 S11-12). International Telecommunication Union Summit in July 2005, after the defining of cyber, security and cyber security, is categorized the problem to four main categories:

1. Prohibition: focus and the use of multilateral legislation on cybercrime, etc.;
2. Prevention: Design and use of more secure systems, better security management and development of security mechanisms;

3-Discovery: The development mechanism of cooperation policies in order to warn about the attacks;
4-Reaction: designing more robust information infrastructure, crisis management programs and police and judicial actions, etc.([ITU] thematic meeting on cyber security, 2005)

On the protection of information security in cyberspace, three categories of actions should be separated: First, the rules that normally are emanated in regulations and is a part of the country law. In this regard, can be pointed to two of newest innovations of America federal state about privacy in cyberspace: "Financial Services Modernization Act," known as "Graham Leach Balil, " and " Portability and accountability act (1996)are examples of technical-legal regulations of Cyber Security Law in America that in the first law, the detailed technical rules to respect the observing the privacy of individuals and how to publish and make available the information are presented. In the margins of this law, some of the effective security techniques (such as the digital signature in communications agencies) are independently attended, in order to being a means for made more adequate the regulations (Michael A Benoit & Joseph D. Looney). On Portability and accountability act ", the relevant institutions were required to implementing the health information protective standards and an office that named "Department of Human Health Services" is established `to run the provisions. The ultimate purpose of these regulations is to ensure the confidentiality, integrity and availability of protected health information (Protected Health Information- PHI) that has been maintained.

Privacy

One of the main information security challenges, is the protection of private information in cyberspace. Indeed, today the efforts of countries to protect the privacy of private life because of the emergence of new information and communication technologies, has been threatened. For more explanation should be said that in the information technology era, privacy protection, in a new form as "data protection" takes on a new form and covers a new concept of the right to privacy. As a result, any information that has personal aspects such as physical data, image, sound, sex, philosophical, religious, and political beliefs, racial or ethnic origin and even some interests and tastes, upon acceptance of the electronic data should be backed by legislation (Qajar Qayonlar, 2001, p. 71)

Electronic processing of personal data that in the electronic communications privacy, some prohibitions and restrictions have been imposed, from the view of the European Directive in October 24, 1995 on "the protection of individuals against processing the data contain he personal information and the free flow these data ", is: " any operation or an operation set, regardless of the use or non-use of automatic way about the personal nature through collection, recording, organization, preservation, compilation, analysis, extraction consultation, use, exchange or any other form, from transmission, access, contact or contemporary communication ways and also remove or destruction, to be applied. "

Instruction No. CE / 58/2002 dated 12 July 2002 entitled "private life and electronic communications", on the one hand is the substitute of the instructions No.CE/ 66/97 Parliament and of the Council of Europe on "processing of personal data and the protection of privacy in the remote telecommunications sector "; and on the other hand, is complementary to the European Directive dated October 24, 1995.

The Federal Department of Commerce, United States of America (FTC) done online measures to increase the customer confidence and security sense in the area of business. FTC is currently the newest and most efficient mechanism security services and tools to providing the anonymity and Privacy has engendered, are known as PET technologies (privacy enhancing technologies), can be mentioned as LPWA (Lucent personalized web), Anonymizer GNUnet's anonymity, GAP, (privacy preferences project) P3P, (assistant protocol) and technologies; for example, anonymizers technology is considered the measures for users that to be remain unknown in cyber space, the disappearing the IP addresses, and finally, inaccessibility to User data. However, these technologies must be accompanied by guides that provide more security for the users and the ISP and ESP, along with knowledge of the legal regulations in this area to be used. (Pereira, 2007).

Conclusions:

Although the information technology has positive impacts on improvement of relationship between states and individuals, diplomatic relations promotion, people empowerment to more participate in internal and external policies etc., but this not all the story, because these technologies, particularly for importers, have had threats. The Republic Islamic of Iran is from these countries and this study is an unavoidable confrontation of a political society with a new wave of technologies which it almost have had no role in it.

The results showed that information technology decade of 1900 has not made serious threat for national security, but the vulnerability of country has been increased in some components. This vulnerability mostly has been in two aspects: first, citizens' empowerment caused to orientation of some people in apposition with government; second, vulnerability led by foreign actors' efforts, which the cyberspace has increased the severity of these kind activities more than before, whereas there has been no effective and powerful diplomacy from Iran to cope with these attempts. In addition, the other security challenge is the threatening of national values and weakening of national unity. Due to liberal values, this challenge is in opposition with religious values and religious dimension of political system's identity.

In relation to the government reaction against threats three main attempts can be observed:

□ Monitoring and tracking of opponents: the cyberspace has made easy the opponents tracking, identifying and punishment of them by government. In the events after tenth presidential election, the social media give the possibility of monitoring and tracking of protesters. Thus, the state could prove how the offenders have relationship with foreigners in country. The other case is also the possibility of conversations' hearing and tracking of people through monitoring equipments of cell phone.

□ 2. Controlling online activities and filtering of cyberspace: it can be said that till the year 2004, government had no systematic strategy to block or filter of internet content. But by increasing activities on Web and users' number, the limitations were mostly for websites with anti-Islamic, immoral contents and subjects which were politically threats for national security. The formation of Committee for Filtering Instances is in this regard. In the events after election of August 22, 2010, besides filtering some social media the SMS services were also were disrupted and with 16 days continuing, Iran had the highest record till that time.

□ 3. Political advertising on the web for the benefit of the State: from the very beginning of internet entering into Iran, the government tried to achieve its goals and promote its views, indicating that even traditionalists could not be indifferent toward it; for example, Mohammad H. Sadarharandi, former Ministerof Culture and Islamic Guidance has announced that the Vice Press Office should be changed into Vice Media to include internet and weblog. The priesthood using of cyberspace, particularly Qom Seminary can also be studied in this regard, so that many Ayatollahs have personal website.

Suggestions:

1. Soft security strengthening: Today to Soft Ware and soft power, soft security is said. Soft security refers to the safeguarding of the players against damage and risks so be soft and intangible. One of the secrets of the Islamic Revolution was also spreading the message of peace and justice, outside its boundaries; thus, in the 21 century the axial approach should be soft power and message. So, legal action with Internet content threats should be done. Other dimension of soft security is positive approach to national security. In this new approach to security, rather than "security for states", is speaking of "public security", i.e. a situation in which there is a balance between national aspirations and effectiveness of political system, so that it create satisfaction in citizens. This approach is the opposite of negative approach and state-centered to national security, in which always there is a concern in relation to external threats to internal injuries and there is not a concern about the attitude of the authorities in the country.

2. Balance creating in the identity dimension: This strategy is to preserve and strengthen the national solidarity. Although Iran is a country of ethnic, nonetheless the minorities that living in Iran basically is Iranian and should not be treated them as a minority. Most constructor way, is sharing the ethnic group in power. Another point is to strengthen national identity through the balance of religious and national identity; the former regime not pay enough attention to national values. While the lack of emphasis on the link between them, may lead to challenges to the political system since the in information age, people are more susceptible to alien cultures and patterns.

3. Public Diplomacy Strengthening: Frequency of information in the current era leads to a deficiency in focus on specific information, this factor is create a source of power for those who can tell where to focus our attention. Iran also needs new diplomacy to influence or change the media outside the borders, this action is inactive measures and is the antithesis of the dominant passively measures against the threats. The media diplomacy when have a real impact that applied by non-governmental.

4. Cultural flexibility: Although today the elements of Western culture by IT is entered to Iranian culture, but this is not necessarily relate to key elements of our culture, but a change occurs in layer of culture that is a diverse layer. So must be learned that creatively fit ourselves with it and have some kind of cultural flexibility; while new technologies can be a great area to defend the values in the cultural invasion. Using Iranian-Islamic culture as a source of soft power in the same direction is investigable.

REFERENCES

a) Persian references:

1. Ansari, Valiollah (1996); Rules Set on Information Rights (collection and regulation); Secretariat of theHigh Council of Iran's Informatics, Tehran, Bahman

2. The scientific department of " The Publishing Industry in Other Countries" journal, Iran Journal, seventh year, serial no. 1897, Tuesday 13 september, 1992, p. 11-12. Yazdi, Ebrahim, (2006); National Security Doctrine, first edition, Saraei publication

3. M. Mohammad Sadeghi, M. Hossein (2004); Specific Criminal (Crimes against Peace and security), Mizan publication, Tehran.

4. Validi, M. Saleh (specific criminal law in detailed rules for the destruction of properties and intentional destruction of properties, Dad publication.

5. Hashemiyan, Vahid, (1997); Coding Methods of Information; Tehran: Rayaney-eh Sharif.

6. Yousef Nejad, Sadegh, (2003), A systematic review of the relationship between growth and corporate profitsin Tehran Stock Exchange, Islami Azad University (Arak branch).

7. Bouzan, bari, (2000), People, Governments and Harass, translator: researchers of institute for strategic studies, Tehran: Institute of Strategic Studies, Beheshti..

8. Khomeyni, Ruhollah, (1981), Tahrir-ol Vasileh, Qom, Dar-ol Elm, Gh, second edition, vol. 2, p.625

9. Khajeh Servi, Gholamreza (2001), Pepers on National Security and Police's Role. Tehran NAJA

10. Secretariat of the Council of Informatics (software authors studied law), p. 43. Official Gazette, 24 January 79.

11. newspapers and Singh (1391), a global IT policies, Mnrjm: Ahmed Ahmed Sltanynzhad and humble, printing, Tehran University of Imam Sadiq (Zyrchap).

12. Tayeb, A., (1389) Proceedings of information technology, data collection and translation, printing, Tehran's ambassador.

13. Abdullahi of confusion, M. (1375), design and implementation services for secure computer networks (terminal MA), Tehran, Sharif University of Technology.

14. Shah Qyvnlv, Siamak (1379) "Legal aspects of computer use, privacy, data protection" newsletter Informatics, No. 74, Vol. XV, Tehran, May.

b)English references:

1. .ITU] WSIS Thematic Meeting on Cyber security Document: CYB/05 10" June 2005.
2. .David, Bainbridge, Introduction to computer law. Fourth Edition, Longman ed, 2002.
3. .Kent, Stephen and I. Millett Lynette, Who Goes There? Authentication through the Lens of Privacy, National Academy Press, 2004.
4. .King, C. M., Dalton, C. E., & Osmanoglu. Security. 2001
5. .Maiwald, Eric, "Legal Issues in Information Security" In Fundamentals of Network Security, chapter 5. 2004.
6. .Pereira, Mario Freire & Manuela, Encyclopedia of Internet Technologies and Applications. Hershey, New York: Information Science reference, 2007.
7. .Green Paper on Public Sector Information in the Information 8.Society, EUROPEAN COMMISSION COM, 585, 1998
8. .Nafisi. A. (2008). *Blogging Outside Iran: A Too! for Internal Democratic Change. Thesis advisor.* US: University of Washington's Department of Communication Honors Program.
9. ."OECD Guidelines for the Security of Information Systems," 1992.