Journal, Advances in Mathematical & Computational Sciences
Vol. 8 No. 1, March 2020
www.mathematics-computationaljournal.info

Article Citation Format
Akinwumi, D.A. Alese, B.K., Akingbesote, A.O. & Oluwadare, S.A. (2020): Towards a Theoretical Framework on Cyber Security Risk Management on the Computer Language Interpretation to Yoruba Language Project. Journal of Advances in Mathematical & Computational Sc. Vol. 8, No. 1. Pp 77-88

Article Progression Time Stamps
Article Type: Research Article
Manuscript Received 13th April, 2020
Final Acceptance: 21st May, 2020

Towards a Theoretical Framework on Cyber Security Risk Management on the Computer Language Interpretation to Yoruba Language Project

[1]Akinwumi, D.A. [2]Alese, B.K., [1]Akingbesote, A.O. & [2]Oluwadare, S.A.
[1]Department of Computer Science, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria.
[2]Department of Computer Science, The Federal University of Technology, Akure, Ondo State, Nigeria
E-mails: david.akinwumi@aaua.edu.ng, kaalfad@yahoo.com, oluwamodimu2012@gmail.com, samoluwadare2013@ gmail.com

ABSTRACT

One major issue that has not allowed ICT to thrive in Africa which Nigeria is part is the Language barrier that is used in writing computer programs. This is because these languages are written in English or other languages that are not basically understood to the Africans. To tackle this challenge, Adekunle Ajasin University, Akungba Akoko through the Software Development Unit is embarking on how computer languages could be interpreted to African indigenous languages. Currently, the interpretation to Yoruba is on-going. While other groups are in the area of Natural Language Processing and others, our contribution to this research is in the area Cyber security. This is among the most complex and rapidly evolving issues in which the society must contend. This paper proposes a Theoretical Framework on Cyber Security Risk Management on the Computer Language Interpretation to Yoruba Language Project. We studied Cyber Security Risk Management as defense- attack problem. Experiments were conducted and the risk and treatment results were obtained. From our results on risk, some were under the medium category. That is, the risk was medium, and implies that the threat-source was very strong but security controls were in place and good enough to prevent successful exercise of the vulnerabilities. Under the treatment, we observed that the number of risk handled by the administrator was almost linear between January 2018 and February 2018. However, between mid- January 2018 and March 2018 the number of risk treated by the administrator was almost constant. One contribution of this work is the formulation of a theoretical framework that determines the risk involved. Another is that of the proposed risk treatment in the context of Yoruba language interpretation.

Keywords—*:* Cyber security, Cybercrime, Cyber attack, Risk management, Yoruba.

1. INTRODUCTION

Cyber security is among the most complex and rapidly evolving issues with which present day organizations are focusing attentions (Alese et al., 2014). Risk is present in everything we do, therefore, there is need to manage risk so that life can be meaningful. If the risk is associated with “cyber” activities, it is referred to as cyber risk.

Reports of breaches of information and damage to organizational IT infrastructure have become increasingly common in recent years and developments in mobile technology, cloud computing and social media has continued to impact the IT risk landscape (Deloitte, 2013). In Alese (2014), the author admitted that Cyber threats have constantly evolved with increasing intensity and complexity. In the opinion of the scholar, it is believed that as the number of users of cyber space increases, the number of criminal among them also increases at almost the same rate. Nowadays, organizations are increasingly reliant on information systems and the Internet for effective service delivery.

Though the historical development of computer programming started from machine to object orientation and Service oriented Architecture (SOA) one basic thing is that, for any Internet service to take place, it requires some aspects of programming tools. Sometimes it combines various programming tools to achieve the required results. For better Quality of Service (QoS) delivery, issues of performance of these tools and that of security especially the cyber aspect must be critically looked into. Another issue is the construct of this language. Most languages are constructed based on the conventional English and French languages as the basic building blocks. This has made the issues of performance and security difficult especially to non-English and French speaking countries to catch easily with those languages. For example, African countries like Nigeria especially the Yoruba speaking country. To resolve this issue, Adekunle Ajasin Centre for Research and Development is currently on a project of computer language interpretation from the convention English or French to Yoruba language.

The Centre has various groups like Natural Language Processing (NLP) group, Cyber Security (CS) and others. Our contribution to this research is in the area Cyber security which is among the most complex and rapidly evolving issues with which the society must contend. This paper proposes a Theoretical Framework on Cyber Security Risk Management on the Computer Language Interpretation to Yoruba Language Project. One contribution of this work is the formulation of a theoretical framework that determines the risk involved. Another is that of the proposed risk treatment in the context of Yoruba language interpretation. The organization of this paper is as follows: Section 2 presents the literature review while section 3 discusses the theoretical framework. Section 4 proposes solution and suggests how the solutions can be achieved when the interpretation mechanism is fully on course. The conclusion is drawn in Sections 5.

2. LITERATURE REVIEW

Lack of applications tailored to meet the unique needs of developing countries most importantly, language barriers is the reasons for ICT's failure to deliver on some of its more overheated hype in Africa. Language barrier have brought about digital divide in Africa resulting into lack of development of Information and Communication Technologies (ICTs) especially in Nigeria. Sinclair (1995) noted that language and culture have become powerful forces in making and breaking international markets. In this connection, service providers in Asia have found that they have to take account of linguistic, religious and other cultural factors in establishing their markets.

On the subject of language, Lambert (1996) observes that "access to the Internet depends not only on ready access to terminals, efficient phone lines and telecommunications infrastructure but also a working command of English, the language of cyberspace. Without this, negotiating one's way through all the various interfaces on the Internet and accessing information is very difficult." He noted how lack of familiarity with English, the major language of the Internet, has affected to the extent to which the Japanese use the Internet compared to the massive use of the Internet in Singapore -- "where English is an official language".

Abidi (1991) has argued that by use of the dominant languages not only in the Internet but also in the mass media, indigenous languages are suppressed and hence local cultures and traditions are rendered subordinate to the cultural images that are depicted in powerful foreign media. In this context, the media audience in developing societies are turned into passive participants. Computer languages (low and high level) are written in either English or French which is difficult for the Africans to understand. A good number of Nigerians who do not understand English have potentials to be another "Bill Gate" but could not maximise their potentials due to language restriction to which one can program the computer. Our experiences over the years as ICT professionals have shown that the ability to write computer codes or program is not dependent how you are sound grammatically because a computer language does not have to follow any correct grammatical structure. In this regards, if the program is written in Yoruba or any other indigenous language it will equally work provided there is provision for indigenous language compilers and interpreters.

In the same vein, there is need to also develop operating systems (OS) and software drivers in indigenous languages thus making the proposed framework to be able to handshake with the Internet. The idea of applying Game theory to solve various security problems is not new. For example, Ibidunmoye *et al*., (2013) proposed a game-theoretic modeling of computer security using a security attack scenarios as an optimization game comprising of multiple players, the attackers and the defenders.

The research analyzed a two-player zero-sum stochastic game model of the interaction between malicious users and network administrators and also introduced a hypothetical network of a typical scenario to show the applicability of the model. State games were encoded using a binary scheme resulting into reducing each state game into a min and max linear programming problems for both the defender and attacker. A combination of pivotal and custom stochastic algorithms was proposed for computing the optimal strategies for the players at each state. Though the model produced promising results, it could not predict how vulnerabilities are exploited by attackers nor analyze attacker's behaviour. Carin *et al*., (2008) presented a computational approach to quantitative risk assessment for investment efficient strategies in cyber security.

The work focused on protection of critical intellectual property in private and public sectors by placing assumption on the possibility of reverse engineering attacks. An attack/protect economic model cast in a game theoretic context was also developed. A small scale simulation was done, which may be unrealistic in complex systems under attack by rational and capable adversaries. Also, Patcha and Park, (2004) proposed a game theoretic approach to model intrusion detection in mobile ad-hoc networks. The authors viewed intrusion detection as a game played between the attacker node and the IDS hosted on the target node. The objective of the attacker is to send a malicious message with the intention of attacking the target node. However, this game theoretic approach does not take into account selfish nodes and groups of colluding attackers. Such security countermeasures against node misbehavior and denial of service attacks are necessary for the model to be practicable.

While all these authors have applied game theoretic solution to various areas, the issue of how this could be used in the context of software development is yet to be addressed to the best of our knowledge. The application of game theoretic approach to solve cyber security problem in the context of language development differentiate our work from others.

3. PROPOSED CYBER SECURITY RISK MANAGEMENT FRAMEWORK

The framework looks at the security issue as defense – attack problem. The language security software (B) serves as the defender while the attacker (A) is the program that aims to attack the software. For example, we have the attacker in red shirt (A) and the defender (B) in black and white shirt. The red shirt player represents our software attackers while the white and black shirt represents the proposed cyber language security software. It is a gain to the attacker when the proposed software is attacked. This is also a loss to the security software designer. The attacker wants to gain by maximizing the minimum profit (Max-Min) obtained based on the B's strategy. The defender will also like to minimise the maximum loss (Min- Max) incurred from the attacker. The framework is given in Figure. 1

Figure 1: Offensive-Defensive Operation of the Proposed Model.

Because this work is like having two groups of people playing offensive –defensive game as shown in Figure1, we propose a deterministic game theoretic approach as our solution approach. The idea is that the attacker (A) has some strategies (P1 and P2) to use for maximizing the minimum profit and the defenders also has some strategies (Q1and Q2) to play to minimize the maximum loss. For example, if the defender continuously plays strategy q1, then the attacker will change and play strategy p1 to have minimum profit of C1. This minimum profit is what the attacker will like to maximize. As soon as the defender notices this, it changes to strategy q2 so that the attacker will be at a loss of C2 but the attacker will also change it strategy to play strategy p2 to have a gain of C4. To get this framework in place, one needs to know the proportion of time A will play strategy p1 and the proportion to play strategy p2 respectively. Also, we need to know the proportion of time B will also play strategy q1 and q2. One assumption in this work is that players of the game can switch from one strategy to another.

The **Offensive-Defensive** game is conceptualized in Figure 2. The relation between the defender (B) and the attacker (A) is modeled as a game across the time dimension for effective defensive actions and reaction to attacks. The deterministic game theoretic approach is used to model the interaction between attacker and defender as a proof of concept.

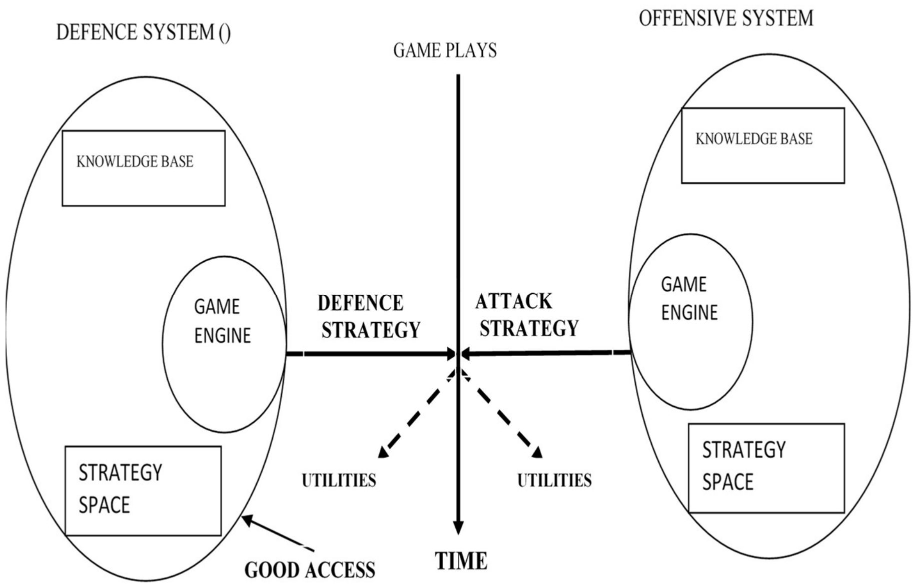

Figure 2: The Offensive-Defensive Game

Given two players A and B with some known values such that A can play strategy p1 or p2 and also B plays any of the q1or q2 strategies as show in the matrix of equation 1.

$$A \quad \begin{matrix} p_1 \\ p_2 \end{matrix} \begin{bmatrix} c_1 & -c_1 \\ -c_1 & c_1 \end{bmatrix} \ldots\ldots\ldots\ldots\ldots (1)$$

We model the A's pay off as

$$\sum_{i-1}^{k} p_1 \ldots\ldots\ldots\ldots\ldots (2)$$

Where k = 1, 2…..n and p_i means the probability of playing *i*th game

The decision variables are:

$$c_{11}\ p_1 + \ (-\ c_{21}\ p_1) \ldots\ldots\ldots\ldots\ldots (3)$$

$$-\ c_{12}\ p_1 \ + \ c_{22}\ p_1 \ldots\ldots\ldots\ldots\ldots (4)$$

Using Equation 3 then it becomes

$$c_{11}\ p_1 - \ c_{21}\ p_1 \ldots\ldots\ldots\ldots\ldots (5)$$

$$-\ c_{12}\ p_1 \ + \ c_{22}\ p_1 \ldots\ldots\ldots\ldots\ldots (6)$$

The concept of A is to Max (Min Profit)

Let u = Min Profit

then this equivalent to Max(u) where

$u \leq c_{11}\, p_1 - c_{21}\, p_1$ ……(7)

and $u \leq -c_{12}\, p_1 + c_{22}\, p_1$ ……(8)

$p_1, p_2 \geq 0$ ……(9)

u is unrestricted in sign

A's problem is

Maximize u

$u - c_{11}\, p_1 + c_{21}\, p_1$ ……(10)

$u + (\, c_{12}\, p_1\,) - c_{22}\, p_1$……(11)

$p_1, p_2 \geq 0$

u is unrestricted in sign

We model B's pay off from equation 1

$\sum_{i-1}^{k} q_1$ ……(12)

Where k = 1, 2…..n and q_i means the probability of playing *i*th game

The decision variables are:

$c_{11}\, q_1 + (-c_{12}\, q_1)$ ……(13)

$-c_{21}\, q_1 + c_{22}\, q_1$ ……(14)

=

$c_{11}\, q_1 - c_{12}\, q_1$ ……(15)

$-c_{21}\, q_1 + c_{22}\, q$ ……(16)

The concept of B is to

Min(Max Loss)

Let v = Max Loss

This equivalent to

Min(v) where

$$v \geq c_{11}\ q_1 - c_{12}\ q_1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (17)$$

and

$$v \geq -c_{21}\ q_1 \ + c_{22}\ q_1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (18)$$

$$p_1, p_2 \geq 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(19)}$$

$$v \ is\ unrestricted\ in\ sign$$

B's problem is

Minimize v

$$v - c_{11}\ q_1 + c_{21}\ q_1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(20)}$$

$$v + (\ c_{12}\ q_1\ ) - c_{22}\ q \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(21)}$$

$$q_1, q_2 \geq 0$$

$$v\ is\ unrestricted\ in\ sign$$

We then

Let v = L

We studied the work of two authors about risk calculation, in Patel *et al.* (2008), the risk R is calculated as follows:

$$R_{\mathrm{i}} = L_i p(L_i) \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(22)}$$

$$R_{total} = \sum_i L_i\ P(L_i) \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(23)}$$

Where L is the magnitude of the potential loss and p is the probability that the loss will occur.

In order to be able to measure risk, it is necessary to identify or develop a method of evaluating risk. Alese et al (2014) used the probability function and set theory to model the set of likely attacks *T*, given as;

The probability that an attack will occur is given as;

$$P(t_i) = \frac{x}{y} \quad \text{.....(24)}$$

Where *x* is the number of possible attacks and *y* is the total number of assets

$$T = \{t_1, t_2, t_3, \dots, t_n\} \quad \text{.....(25)}$$

Where t_i represents threats.

The set of assets A, given as;

$$A = \{a_1, a_2, a_3, \dots, a_n\} \quad \text{.....(26)}$$

Where a_i, represents assets.

The risk (R) on the assets is then computed as;

$$R = P(t_i) * V(a_i) \quad \text{.....(27)}$$

Where $P(t_i)$ is the probability of attacks and $V(a_i)$ is the value of assets with range $[1 : 10]$

In our work we adopt the work of Hewett *et al.* (2014). We first calculate the impact of an adverse event denoted by μ

$$\mu(a) = W_c C(a) + W_i I(a) + W_a A(a) \quad \text{.....(28)}$$

Where w_c, w_i, and w_a are weights of Confidentiality, Integrity and Availability respectively and $C(a)$, $I(a)$ and $A(a)$ are the impact of action (a) on Confidentiality Integrity and Availability. We then use the idea of Patel *et al.* (2008) to get the probability of likelihood estimation (L).

Then the risk (R) is given as:

R = L* μ

The risk function is computed to determine the level of risk involved as follows:

$$f(R) = \begin{cases} 0.1000 \geq R \geq 0.0800 & Very\ High \\ 0.0700 \geq R \geq 0.0600 & High \\ 0.0500 \geq R \geq 0.0400 & Medium \\ 0.0300 \geq R \geq 0.0200 & Low \\ R \leq 0.0100 & Very\ Low \end{cases} \quad \text{---------- (29)}$$

From Equation (29), the risk is very high if its value ranges from 0.0800 to 0.1000, it is high if it ranges from 0.0600 to 0.0700, it is medium if it ranges from 0.0400 to 0.0500, it is low if it ranges from 0.0200 to 0.0300 and very low if the risk level is less than 0.0200.

Our risk results will be based under the following category.

1. If the risk is very high or high, it implies that the threat-source is very strong and security controls to prevent the vulnerability from being exercised are ineffective.
2. If the risk is medium, it implies that the threat-source is very strong but security controls are in place and good enough to prevent successful exercise of the vulnerabilities.
3. If the risk is low or very low, it implies that the threat-source is weak or appropriate security controls are in place to prevent or at least significantly impede the exercise of the vulnerabilities from being exercised.

Another contribution of this work is the proposed treatment mechanism we have introduced on the category of the risk involved. The mechanism for selection was based on VHH (Very High and High), M (Medium) LVL (Low and Very Low). We set up a threshold (*t)* for the risk involved.

Then
If $R \leq t$ *then threat is insignificant therefore the risk is accepted*
If $0.0003 \geq R \leq 0.0005$ *then risk is partially significant therefore the risk is to be handled by administrator.*
If $R \geq 0.0006$ *then risk is very significant therefore the risk is to be handled by snort.*

4. EXPERIMENTAL SETUP, RESULTS AND DISCUSSION

4.1 Experimental Setup

The experimental setup was done with the aid of Microsoft Excel as the tool. Risk estimation for a period of three (3) months was carried out. The metric table was set up in rows and columns. Player A takes the row while player B takes the column. Based on the earlier proposed equations, the payoff table was derived and this further enables us to have the row table containing player B's best response to player A and the column table containing player A's best response to player B. The Minimax (Risk Avoider), Maximin (Risk Taker) and weighted average were then derived. Derivation of these tables enables us to have the Nash Equilibrium table. This then enables us to get various significance, consequence and other parameters. The results are explained under the results and discussion section.

4.2 Results and Discussion

We determined the risk estimation based on different parameters as discussed under our experimental set up. For example, when the significance and consequence were set to 2, the confidentiality was 4 and that of integrity and availability were both 4. Then the impact is 12.0. These three factors determine the impact (I). We determined the likelihood by selecting a particular threat-source and apply appropriate defense strategies. The likelihood is described as High, Medium, and Low using range scale 0.70-1.00, 0.30-0.69, 0.00-0.29 respectively. For example, if the threat, defense strategies are DOS and Firewall respectively then the likelihood is 0.0036, the risk is then 0.0432. This is depicted in Figure 3. Based on this result the risk falls under the medium category. That is, the risk is medium, it implies that the threat-source is very strong but security controls are in place and good enough to prevent successful exercise of the vulnerabilities.

Journal, Advances in Mathematical & Computational Sciences
Vol. 8 No. 1, March 2020
www.mathematics-computationaljournal.info

Figure 3: Risk Estimation

Figure 4 shows the results of the treatment mechanism. Risk estimation experiment for a period of three (3) months was carried out as earlier discussed. From our result as depicted in Figure 4, we observed that the number of risk handled by the administrator is almost linear between January and February. However, between mid- January and March the number of risk treated by the administrator is almost constant. On the risk treated by firewall, we observed that the number of risk treatment seems to be higher than that of the administrator. On the risk treatment by Snort, between January 1 to January 9, nearly all the risks under this range were treated but from January 10 to March 19 most risk group under this level were not treated except in February 19 to February 27 and March 7.

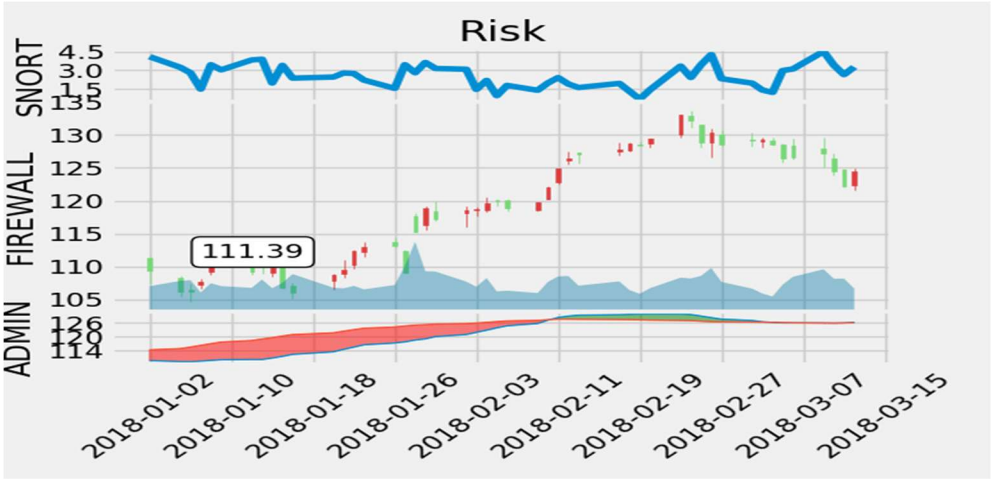

Figure 4: Mechanism for Risk Treatment

5. CONCLUSION

ICT is highly versatile and it can be tailored to meet a variety of diverse challenges. Cyber security risk management is an emerging research area with a big scope for the development of several techniques. Language barrier has contributed to the digital divide in Africa. To transcend barriers of language, there is need to interpret computer language to indigenous languages as well as develop better techniques that can be used to model its security in a more realistic manner. To support this drive, the Centre for Research and Development of Adekunle Ajasin University has embarked on a project of computer language interpretation from the convention English or French to Yoruba language.

The Centre has various groups like Natural Language Processing (NLP) group, Cyber Security (CS) and others. The focus of this research is in the area of Cyber Security, we studied Cyber Security Risk Management as defense- attack problem. Experiments were conducted and the risk and treatment results were obtained. For example, some of our risk results were under the medium category while some on low. On the medium side, it implies that the threat-source was very strong but security controls were in place and good enough to prevent successful exercise of the vulnerabilities. Under the treatment, we observed that the number of risk handled by the administrator was almost linear between January and February 2018.

However, between mid- January and March 2018 the number of risk treated by the administrator was almost constant. The contributions of this work are two folds. First is that of the theoretical framework formulation, the second is that of the proposed risk treatment in the context of Yoruba language interpretation. This to the best of our knowledge is yet to appear in the literature. On future work, we aim at looking on how expert systems could be developed to teach computer language in Yoruba. This will assist students to further understand the concept of computer programming.

REFERENCES

1. Abidi, Syed A.H. (1991) Communication, information and development in Africa. Uganda: Bano Abidi Publications.
2. Alese, B. K., (2014): Security Issues in Nigeria: Getting ready for the Digital Challenge. 'Annual Lecture' First Bank of Nigeria Plc Professorial Chair in Computer Science Delivered at the Federal University of Technology, Akure, Nigeria on Tuesday, April 29.
3. Alese, B. K., Arome, G.J., Olukayode O. and Daramola O.A. (2014). "Modelling of Risk Management Procedures for Cybercrime Control Systems" Proceedings of the World Congress on Engineering 2014 Vol I, WCE 2014, July 2 - 4, 2014, London, U.K.
4. Alpcan, T. and Pavel, L. (2009) Nash equilibrium design and optimization. International Conference on Game Theory for Networks, GameNets.
5. Baldi S., Gelbstein E. and Kurbalija J., (2010) Hacktivism, Cyber-Terrorism and Cyberwar, The Information Society Library, DiploFoundation, Geneva, Switzerland, 2003 and US Government Accountability Office (GAO) Report "Cyberspace", Washington, DC, GAO-10-606, July 2010.
6. Bloem, M. Alpcan, T. and Basar, T. (2006). Intrusion response as a resource allocation problem. IEEE Conference on Descision and Control.
7. Carin, L., Cybenko, G. and Hughes, J.(2008). Quantitative evaluation of risk for investment efficient strategies in cybersecurity: The queries methodology. IEEE Computer.

8. Deloitte (2013) “Audit Committee Brief” August 2013 http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/USEng/Documents/Deloitte%20Periodicals/Audit%20Committee%20Brief/ACBrief_October2013.pdf
9. Diana, K. (2014) “Application Security Risk Management and the NIST Cybersecurity Framework”.http://securityintelligence.com/nist-cybersecurity-framework-application-security-risk-management
10. Garg, S and Aujla, G.S. (2014). An Attack Tree Based Comprehensive Framework for the Risk and Security Assessment of VANET using the Concepts of Game Theory and Fuzzy Logic. Journal Of Emerging Technologies In Web Intelligence, Vol. 6, No. 2, May 2014.
11. Gordon,L.(2014) cybersecurity management http://www.rhsmith.umd.edu/faculty/lgordon/cybersecurity/Cybersecurity
12. Gueye A. (2011) “A Game Theoretical Approach to Communication Security” Electrical Engineering and Computer Sciences Dept. University of California, Berkeley, PhD Thesis.
13. He, F., Zhuang, J. and Rao, N.S.V. (2012). Game-Theoretic Analysis of Attack and Defense in Cyber-Physical Network Infrastructures. Proceedings of the 2012 Industrial and Systems Engineering Research Conference G. Lim and J.W. Herrmann, eds.
14. Hewett, R., Rudrapattana, S. and Kijsanayothin, P. (2014) “Cyber-security Analysis of Smart Grid SCADA Systems
15. with Game Models” Proceedings of the 9th Annual Cyber and Information Security Research Conference, ACM, 109-112.
16. Ibidunmoye, E.O., Alese, B. K. and Ogundele O.S. (2013): Modeling Attacker-Defender Interaction as a Zero-Sum Stochastic Game. Journal of Computer Sciences and Applications, 2013, Vol. 1, No. 2, 27-32.
17. Jormakka, J. and Molsa, J. V. E. (2005). Modelling information warfare as a game. Journal of Information Warfare; Vol. 4(2).
18. Lambert, Andrew (1996) "How the world's rules in telecommunications and media are shaping up in cyberspace: North Asia generally and Korea as a case study." Paper presented at a forum of the International Institute of Communications (Australian Chapter): How the world's rules in telecommunications and media are shaping up in cyberspace, 14 May.
19. Liu, P., Zang, W. and Yu, M. (2005). Incentive-based modeling and inference of attacker intent, objectives and strategies. ACM Transactions on Information and System Security 8(1), 78–118 DOI http://doi.acm.org/10.1145/1053
20. Liu, Y., Comaniciu, C.and Man, H. (2006). A bayesian game approach for intrusion detection in wireless ad hoc networks. ACM International Conference Proceeding Series; Vol. 199.Lye, K. and Wing, J. (2002). Game strategies in network security. Proceedings of the Foundations of Computer Security.
21. Nguyen, K. C. Alpcan, T. and Basar, T. (2009) Stochastic games for security in networks with interdependent nodes. Proc. Of Intl. Conf. on Game Theory for Networks (GameNets).
22. Patel, S. C., Graham, J. H. and Ralston, P. S. (2008).“Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements,” International Journal of Information Management, 28(6), 483-491.
23. Patcha, A. and Park, J. (2004) A game theoretic approach to modeling intrusion detection in mobile ad hoc networks. Proceedings of the 2004 IEEE workshop on Information Assurance and Security.
24. Sinclair, John (1995) "The business of international broadcasting: Cultural bridges and barriers," International Business: Australia and Asia. Centre for International research on Communication and Information Technologies (CIRCIT).