DE GRUYTER OPEN

Land Forces Academy Review

Vol. XXIII, No 1(89), 2018

A CYBER THREAT MODEL OF A NATION CYBER INFRASTRUCTURE BASED ON GOEL-OKUMOTO PORT APPROACH

Florin OGÎGĂU-NEAMȚIU
Regional Department of Defense Resources Management, Braşov, Romania
florinbvmail@yahoo.com

Horațiu MOGA
The National Agency for Fiscal Administration, Braşov, Romania
horatiu.moga@gmail.com

ABSTRACT

Information assurance plays a critical role in modern countries around the globe and IT systems are key elements in this environment. Enabling or disabling such capabilities are strategic goals which dramatically influence a nation capacity to perform thus drawing considerate attention of stakeholders. This research defines a method to deal with cyber threats focused on attacker by using the game theory approach and canonic strategies specific to informational war. The cyber threats corresponding risks are treated through the bimatrix game theory and the strategies for Defender and Challenger game players are adapted from the informational war theory. The authors consider cyber-attacks to be a subcomponent of the informational war and thus they can be handled, with minimal alterations, with instruments from the same wide informational war framework.

KEYWORDS: cyber-attacks, information security, game theory, information war, cyber infrastructure

1. Introduction

A cyber threat model can be defined as a mathematical tool of a risk analysis which can be used to analyze the security aspect of a cyber event. Developing such a mathematical process is done in two different stages. In the first part the detection method of the information system attacks are being analyzed while in the second part a mathematical model of the systems risks are being developed. In this research the authors used for the first stage detection tools included in Kali Linux (Pritchett & Smet, 2013; Heriyanto & Allen, 2014) and for constructing the mathematical model the authors based their approach on the bimatrix game theory (Barron, 2013).

In the area of cyber security one can identify three threat models used to perform system security analyses from different perspectives: the first model is based on threats focused on assets which take in consideration the network hardware equipment, the second aims modeling threats targeting the software component of

DOI: 10.2478/raft-2018-0010

the network and the third model focuses on the human factor – the attacker either nation-state actor (Moga & Ogîgău-Neamțiu, 2017) or non-state hacker (Ogîgău-Neamțiu & Moga, 2017).

This research is focused on modeling the cyber attacker. A cyber threat model focused on state actor attacker represents a way of evaluating from the risks perspective the process by which an aggressor (further referred as Challenger) is attacking the national cyber infrastructure of another state (further referred as Defender). The national cyberinfrastructure is a critical component of a country which is used to describe the environment that support advanced data acquisition, data storage, data management, data integration, data mining, data visualization and other computing and information processing services distributed over the Internet beyond the scope of a single institution (Moga & Boşcoianu, 2015; Moga & Boşcoianu, 2016).

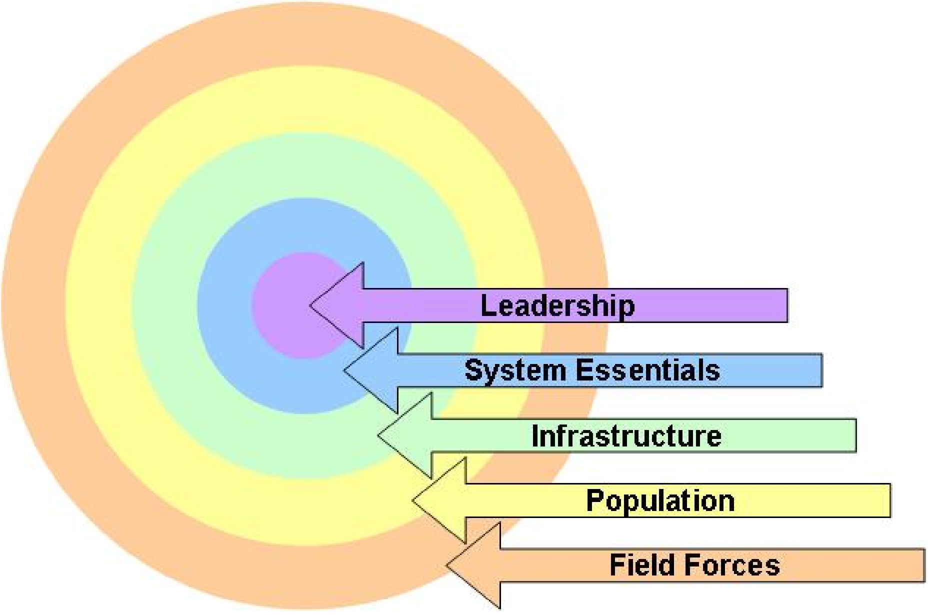

Figure no 1: Five Ring model
(source: http://customerinnovations.com/centers-of-gravity-levers-for-shifting-the-customer-experience/)

The cyberinfrastructure consists of three asset types: servers which offer services, clients which benefit upon those services and the data transport infrastructure which is used to transfers data between the two parties. In a cyber war actions are performed in order to limit the functionality of the critical infrastructure partially or totally. By doing so there are no direct victims but the Defender has limitations in conducting its operations and suffers economical losses or is unable to fully coordinate its kinetical actions (Moga & Boşcoianu, 2015; Moga & Boşcoianu, 2016).

In order to create the structure model of a state cyber infrastructure we will use the five concentric rings defined by U.S.A. COL John Warden the III (2000). He developed and used this model in order to analyze enemy threats to a nation and create strategic responses to those threats. He envisioned the state as a system composed of five concentric rings, each ring representing an enemy‘s center of gravity that if attacked would make war prohibitively expensive for the enemy or eliminate temporarily or permanently the enemy‘s ability to wage war. The first exterior ring (field forces) comprises the military and nonmilitary forces which act as a fighting mechanism that defends the state, the second ring (population) is composed of the population from that country, the next ring (infrastructure) is represented by fundamental facilities and systems serving a country, the next ring (system essentials) also known as organic comprises key elements which are critical for the state survival (oil, electricity, food and money) and the inner ring (leadership) is formed of the people and structures which lead the system and which make strategic decisions.

By applying the above framework the cybernetic structure of a country could be categorized in four groups:

- The military cyber infrastructure component – comprises all computer networks LANs, MANs, WANs supporting capabilities provided to the military apparatus of a country;
- The social media cyber infrastructure component – comprising all computer networks LANs, MANs, WANs supporting capabilities provided to the "population" levels of the COL Warden's theory;
- The economic cyber infrastructure component – comprising all computer networks LANs, MANs, WANs supporting capabilities provided to the "system essentials" and "infrastructure" levels of the COL Warden's theory. The authors opted for coupling the two domains because from the cybernetic view have many similarities and will make the analysis simpler;
- The governmental cyber infrastructure component – comprises all computer networks LANs, MANs, WANs which offer support for conducting governance and leadership activities.

For the purpose of this article the authors employed the canonical strategies of the informational war combined with bi-matrix games theory for modeling the risk in the cyber environment and, the Goel-Okumoto virtual port model for performing the calculus of utility functions of the bi-matrix games.

2. Theoretical Aspects

Information warfare (IW) is a term describing the usage of information by one party for obtaining advantages over the other party. The concept can be applied to classical military operations, but also to the business, social or other environments. One of area benefiting of the most attention in the last years is the cyber environment and in this article the authors are conduction a study of the strategies adopted by attackers to conduct their missions.

3. Borden-Kopp IW Model

Based on Shannon information theory, Borden, Kopp and Poisel (2013) developed and aligned the information war (IW) model to the cyber warfare by analyzing 5 categories or canonical strategies. This study further develops those strategies and aligns its concepts to the cyber environment.

1. Denial of information (data)/ passive denial – is a strategy where the attacker adopts an undercover/stealth position and by deploying specialized tools he tries to insert noise like signal to alter the genuine data flow in order to limit the operational capabilities of the victims systems. The main characteristic of this strategy is that the victim cannot acknowledge that the data flow has been compromised and is unaware of the attacker's presence. In such cases the lack of data flow is associated by the victim with other causes and reactive measures are not deployed on time or misconfigured. Examples: Slowloris apache server attack consists of actions in which an automated software simulates the establishment of a legitimate connection to a web apache server. By keeping the connection open indefinitely the system performance could be affected and the effect maximized if multiple such connections could be established from a controlled botnet network. Another example is a mail-open relay attack in which the email server is

performing operations on behalf of illegitimate users and thus hampering systems performance. TCP SYN flood and TCP reset attacks could be associated with such strategy as their main goal is to stealthy crash TCP established connections and prevent legitimate data transfers. In this category one can assign also various malicious programs actions like viruses or malware which limit the systems performance by inducing delays or modifying the genuine data flow.

2. Disruption and destruction/active denial – is a strategy adopted by an attacker which consists of evident actions of inserting/manipulating data/software into the victims IT systems which alters their normal functioning and resulting in compromised outputs, operational deterioration or even system destruction. In this case the attacker conducts observable actions and is not concerned about maintaining a camouflaged position but he focuses on the degradation of network performance, denying or hardening legitimate user access to a specific resource (most often a website), various network service quality degradation (DHCP, DNS, email), etc. Example: the largest category of attacks related to this strategy is the denial of service attacks whose mail goal is to deny the legitimate users access to IT resources. Such attacks target a variety of network services like Dynamic Host Configuration Protocol (DHCP) in DHCP starvation attack, Domain Name Servers (DNS) in DNS flood, DNS poisoning or DNS amplification attacks, Internet Control Message Protocol (ICMP) protocol in ICMP flood or SMURF attacks, User Datagram Protocol (UDP) protocol in UDP flood or distributed denial of services attacks or email in email bombing attack, etc.

3. Deception and mimicry – is a strategy which consists of actions in which the attacker attempts to insert misleading data into the victims systems which mimics so well the legitimate data that is impossible for the victim to distinguish between the two of them. The attacker can corrupt original data packets and forge them substituting the valid data and then releasing them on the network. The receiving devices will alter their behavior based on the new delivered parameters. In some cases the attacker will mimic only data packets but sometimes the attacker will emulate network switching and routing devices, servers and wireless access points in trying to alter the normal network traffic.

Example: A typical deception and mimicry attack is a man-in-the-middle attack where an attacker inserts an intermediate device in the normal traffic flow by exploiting the vulnerabilities of the STP protocol, the communication establishment process between a wireless access point and a client or other resource. Having the communication routed through a controlled device, allows the attacker to alter the data flow, capture the traffic and perform data analyzing processes on it. ARP cache poisoning, DHCP spoofing, DNS hijack, email spoofing are another attacks which can be included in this category as the objective of the attacker is to insert into the victims IT systems forged packets which will denaturate the normal behavior of attacked services. VLAN hopping is a deception and mimicry attack where the attacker targets a network switch and sends to it forged packets in order to alter its normal behavior and ultimately send data packets to a restricted VLAN. Also from this category are attacks like identify theft, phishing, spamming which mimic the normal behavior of a legitimate user but in fact are malicious actions performed to get access to restricted resources, compromise user credentials or just hampering systems functionality.

4. Subversion – is a strategy which consists of actions in which the attackers insert hardware or software elements into the victim’s IT systems which can trigger or can

be further exploited to crash those systems. The insertion of the subversive payload can be performed at any phase of the system lifecycle with different consequences on the difficulty, effectiveness, and ability to avoid discovery. In this attack category could be assign logic bombs – small programs hidden within IT systems which can be triggered by certain events or trojan horses – programs once executed will perform actions that the user is unaware of like opening ports, establishing connections with external systems and thus providing the attacker means to further conduct malicious actions on the victims IT systems, etc. Other examples are "ping of death" or "teardrop" attacks when the attacker sends packets which apparently are legitimate but which contain forged data and determine the crash or the targeted systems.

5. Exploitation – is a strategy which aims at collecting information about the victims IT systems and the data flows which pass through them. This strategy is different from the first four as it does not have a direct negative impact on the victims systems rather it is an intelligence gathering strategy. The strategy contains actions involving system monitoring, device identification, network discovery, data discovery, data exfiltration, etc. The gathered intelligence can be further leveraged for the development of a future course of action with a maximized impact or can be capitalized on for financial benefits.

Example: attacks from this category could be considered the followings: packet sniffing which consists of capturing the traffic passing through a specific device and then using specialized software to perform traffic analysis or "ICMP sweep", "TCP and UDP port scan" performed to reveal the systems open ports. "War driving" is another attacking techniques where the attacker travels in a certain area and scans for access points which can be compromised. "Dumpster diving" consists of searching for compromising information in discarded IT equipment or trash and exploits the inappropriate disposal of media which contained confidential information. Another attack from this category is the "heartbleed" attack which exploits the OpenSSL protocol, creates a "buffer over-read" situation which allows the attacker to get access to restricted information.

It is worth to be mentioned that many of the attacks presented here contain elements of multiple strategies based on to the needs or goals of the developers. The assignment of an attack to a certain canonic strategy has been done according to the main effort and is prone to author's subjectivism and their understanding.

In order to determine all network nodes for two national cyber infrastructures belonging to two different nations (Defender and Challenger) – which can perform reciprocal scanning processes using Kali Linux instruments – we will consider the following stages being applied to each of the four national cyber infrastructure components (Pritchett & Smet, 2013; Heriyanto & Allen, 2014:

- DNS server IP identification of all networks (LANs, MANs and WANs) for all by using the scripts A.1.1 and A.1.2 from Appendix A;
- Identification of all IP address intervals of all networks (LANs, MANs and WANs) by using the script A.1.3 from Appendix A;
- Discover all open ports from all networks by using the script A.1.4 from Appendix A;
- Identify the operating system of all computers from those networks by using the script A.1.5 from Appendix A;
- Identify the service daemons running on all computers by using the script A 1.6 from Appendix A.

4. The Goel-Okumoto Model

This model has been chosen in order to perform the evaluation of the utility function. The two authors defined this model in 1979 in order to model the virtual ports of a computing system (switch, router, server) (Min Xie Yuan-Shun Dai and Poh, 2004). They consider that the failure of a network port subjected to cyber-attacks could be modeled by a NHPP process and its behavior can be characterized by a simple function which describes the media of this failure (Min Xie Yuan-Shun Dai & Poh, 2004). This model is worldwide accepted as being a reference model for estimating the reliability of a software product. The model is being based on three premises (Min Xie Yuan-Shun Dai & Poh, 2004):

- The total number of cyber-attacks/ faults which could occur in a certain moment is based on a Poisson distribution;
- All cyber-attacks/faults are independent and have the same chance of being detected;
- All detected cyber-attacks/faults are immediately remediated and there are no more new cyber-attacks/faults conducted upon the target system.

The function of failure (Min Xie Yuan-Shun Dai & Poh, 2004) which characterizes the NHPP (No Homogeneous Poisson Process) process is the following:

$$m(t) = a \cdot [1 - \exp(-b \cdot t)], a > 0, b > 0 \qquad (1)$$

For a single *i* rank communication port belonging to a network node with n ports failure process is modeled by an NHPP model with mean value function m(t) given by

$$m_i = a_i[1 - \exp(-b_i \cdot t)] \qquad (2)$$

The failure function for that network node (computer/server, switch or router) is defined by the following relation:

$$m = \prod_{i=1}^{n} m_i \longrightarrow \prod_{i=1}^{n} a_i \qquad (3)$$

If we consider all ports to be identical equation no (3) will become:

$$m = \prod_{i=1}^{n} m_i \longrightarrow a^n, a_i = a, i = \overline{1,n} \qquad (4)$$

The Utility function will be calculated as the following media where N represents the product between the maximum number of devices (computer/server, switch or router) also represented by the total number of network ports corresponding to a certain OSI level and a certain infrastructure type defined by the Goel-Okumoto methodology. By using equations (1)-(4) we can calculate the utility function by creating the media of Goel-Okumoto failure functions. We consider the cyber-attacks employed by the two states as performing upon the bimatrix game theory.

$$U = \frac{1}{N} \cdot \int dm = \frac{1}{N} \cdot \int d\left(\prod_{i=1}^{n} m_i\right) \qquad (5)$$

The result will be defined by using canonical strategies of the informational war (Disruption and destruction, Subversion, Exploit) which characterizes the game theory with complete information as is the case in the bimatrix functions employed below. We consider that the equation defining an element of the decision matrix has the following structure:

$$\begin{cases} U_{Defender} = \left(p_1, p_2, 1-p_1-p_2\right) \cdot \begin{bmatrix} U_{D11} & U_{D12} & U_{D13} \\ U_{D21} & U_{D22} & U_{D23} \\ U_{D31} & U_{D32} & U_{D33} \end{bmatrix} \cdot \begin{pmatrix} q_1 \\ q_2 \\ 1-q_1-q_2 \end{pmatrix} \\ U_{Challenger} = \left(p_1, p_2, 1-p_1-p_2\right) \cdot \begin{bmatrix} U_{C11} & U_{C12} & U_{C13} \\ U_{C21} & U_{C22} & U_{C23} \\ U_{C31} & U_{C32} & U_{C33} \end{bmatrix} \cdot \begin{pmatrix} q_1 \\ q_2 \\ 1-q_1-q_2 \end{pmatrix} \end{cases} \tag{6}$$

Where:

U_{D11} – the utility function of Defender, when its strategies and the Challenger's strategies are Disruption and destruction; U_{D12} – the utility function of Defender when its strategy is Disruption and destruction and the Challenger's strategy is Subversion; U_{D13} – the utility function of Defender when its strategy is Disruption and destruction and the Challenger's strategy is Exploit; U_{D21} – the utility function of Defender when its strategy is Subversion and the Challenger's strategy is Disruption and destruction; U_{D22} – the utility function of Defender when the strategy of both actors is Subversion; U_{D23} – the utility function of Defender when its strategy is Subversion and the Challenger's strategy is Exploit; U_{D31} – the utility function of Defender when its strategy is Exploit and the Challenger's strategy is Disruption and destruction; U_{D32} – the utility function of Defender when its strategy is Exploit and the Challenger's strategy is Subversion; U_{D33} – the utility function of Defender, when its strategies and the Challenger's strategies are Exploit.

U_{C11} – the utility function of the Challenger, when its strategies and the Defender's strategies are Disruption and destruction; U_{C12} – the utility function of the Challenger when its strategy is Subversion and the Defender's strategy is Disruption and destruction;U_{C13} – the utility function of the Challenger when its strategy is Disruption and destruction and the Defender's strategy is Exploit; U_{C21} – the utility function of the Challenger when its strategy is Disruption and destruction and the Defender's strategy is Subversion; U_{C22} – the utility function of the Challenger when the strategy of both actors is Subversion; U_{C23} – the utility function of the Challenger when its strategy is Subversion and the Defender's strategy is Exploit;U_{C31} – the utility function of the Challenger when its strategy is Exploit and the Defender's strategy is Disruption and destruction;U_{C32} – the utility function of the Challenger when its strategy is Exploit and the Defender's strategy is Subversion; U_{C33} – the utility function of the Challenger, when its strategies and the Defender's strategies are Exploit.

5. Results and Discussions

The solution of such a system can be reduced to calculating the Nash point by using Lagrange multipliers for the four equations. The relation (6) will become:

$$\begin{cases} \dfrac{\partial U_{Defender}}{\partial p_1} = 0 \quad \dfrac{\partial U_{Defender}}{\partial p_2} = 0 \\ \dfrac{\partial U_{Challenger}}{\partial q_1} = 0 \quad \dfrac{\partial U_{Challenger}}{\partial q_2} = 0 \end{cases} \Leftrightarrow \tag{7}$$

or

$$\frac{\partial U_{Defender}}{\partial p_1} = (1,0,-1)\cdot\begin{bmatrix} U_{D11} & U_{D12} & U_{D13} \\ U_{D21} & U_{D22} & U_{D23} \\ U_{D31} & U_{D32} & U_{D33} \end{bmatrix}\cdot\begin{pmatrix} q_1 \\ q_2 \\ 1-q_1-q_2 \end{pmatrix} = 0$$

$$\frac{\partial U_{Defender}}{\partial p_2} = (0,1,-1)\cdot\begin{bmatrix} U_{D11} & U_{D12} & U_{D13} \\ U_{D21} & U_{D22} & U_{D23} \\ U_{D31} & U_{D32} & U_{D33} \end{bmatrix}\cdot\begin{pmatrix} q_1 \\ q_2 \\ 1-q_1-q_2 \end{pmatrix} = 0$$

$$\frac{\partial U_{Challenger}}{\partial q_1} = (p_1, p_2, 1-p_1-p_2)\cdot\begin{bmatrix} U_{C11} & U_{C12} & U_{C13} \\ U_{C21} & U_{C22} & U_{C23} \\ U_{C31} & U_{C32} & U_{C33} \end{bmatrix}\cdot\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = 0$$

$$\frac{\partial U_{Challenger}}{\partial q_2} = (p_1, p_2, 1-p_1-p_2)\cdot\begin{bmatrix} U_{C11} & U_{C12} & U_{C13} \\ U_{C21} & U_{C22} & U_{C23} \\ U_{C31} & U_{C32} & U_{C33} \end{bmatrix}\cdot\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} = 0$$

Which is equivalent with the following relations:

$$\left\{\begin{array}{l} \dfrac{\partial U_{Defender}}{\partial p_1} = (1,0,-1)\cdot\begin{bmatrix} U_{D11} & U_{D12} & U_{D13} \\ U_{D21} & U_{D22} & U_{D23} \\ U_{D31} & U_{D32} & U_{D33} \end{bmatrix}\cdot\begin{pmatrix} q_1 \\ q_2 \\ 1-q_1-q_2 \end{pmatrix} = 0 \\ \dfrac{\partial U^{kj}_{Defender}}{\partial p^{kj}_2} = (0,1,-1)\cdot\begin{bmatrix} U_{D11} & U_{D12} & U_{D13} \\ U_{D21} & U_{D22} & U_{D23} \\ U_{D31} & U_{D32} & U_{D33} \end{bmatrix}\cdot\begin{pmatrix} q_1 \\ q_2 \\ 1-q_1-q_2 \end{pmatrix} = 0 \\ \dfrac{\partial U_{Challengerr}}{\partial q_1} = (p_1, p_2, 1-p_1-p_2)\cdot\begin{bmatrix} U_{C11} & U_{C12} & U_{C13} \\ U_{C21} & U_{C22} & U_{C23} \\ U_{C31} & U_{C32} & U_{C33} \end{bmatrix}\cdot\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = 0 \\ \dfrac{\partial U_{Challengerr}}{\partial q_2} = (p_1, p_2, 1-p_1-p_2)\cdot\begin{bmatrix} U_{C11} & U_{C12} & U_{C13} \\ U_{C21} & U_{C22} & U_{C23} \\ U_{C31} & U_{C32} & U_{C33} \end{bmatrix}\cdot\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} = 0 \end{array}\right. \Leftrightarrow$$

$$\begin{cases} \dfrac{\partial U_{Defender}}{\partial p_1} = \left[U_{D11}-U_{D31}, U_{D12}-U_{D32}, U_{D13}-U_{D33}\right]\cdot \begin{pmatrix} q_1 \\ q_2 \\ 1-q_1-q_2 \end{pmatrix} = 0 \\ \dfrac{\partial U_{Defender}}{\partial p_2} = \left[U_{D21}-U_{D31}, U_{D22}-U_{D32}, U_{D23}-U_{D33}\right]\cdot \begin{pmatrix} q_1 \\ q_2 \\ 1-q_1-q_2 \end{pmatrix} = 0 \\ \dfrac{\partial U_{Challenger}}{\partial q_1} = \left(p_1, p_2, 1-p_1-p_2\right)\cdot \begin{bmatrix} U_{C11}-U_{C13} \\ U_{C21}-U_{C23} \\ U_{C31}-U_{C33} \end{bmatrix} = 0 \\ \dfrac{\partial U_{Challenger}}{\partial q_2} = \left(p_1, p_2, 1-p_1-p_2\right)\cdot \begin{bmatrix} U_{C12}-U_{C13} \\ U_{C22}-U_{C23} \\ U_{C32}-U_{C33} \end{bmatrix} = 0 \end{cases} \Leftrightarrow$$

$$\begin{cases} \left[U_{D11}-U_{D31}, U_{D12}-U_{D32}, U_{D13}-U_{D33}\right]\cdot \begin{pmatrix} q_1 \\ q_2 \\ 1-q_1-q_2 \end{pmatrix} = 0 \\ \left[U_{D21}-U_{D31}, U_{D22}-U_{D32}, U_{D23}-U_{D33}\right]\cdot \begin{pmatrix} q_1 \\ q_2 \\ 1-q_1-q_2 \end{pmatrix} = 0 \\ \left(p_1, p_2, 1-p_1-p_2\right)\cdot \begin{bmatrix} U_{C11}-U_{C13} \\ U_{C21}-U_{C23} \\ U_{C31}-U_{C33} \end{bmatrix} = 0 \\ \left(p_1, p_2, 1-p_1-p_2\right)\cdot \begin{bmatrix} U_{C12}-U_{C13} \\ U_{C22}-U_{C23} \\ U_{C32}-U_{C33} \end{bmatrix} = 0 \end{cases} \Leftrightarrow$$

$$\begin{cases} \left(U_{D11}-U_{D31}\right)\cdot q_1 + \left(U_{D12}-U_{D32}\right)\cdot q_2 + \left(U_{D13}-U_{D33}\right)\cdot\left(1-q_1-q_2\right) = 0 \\ \left(U_{D21}-U_{D31}\right)\cdot q_1 + \left(U_{D22}-U_{D32}\right)\cdot q_2 + \left(U_{D23}-U_{D33}\right)\cdot\left(1-q_1-q_2\right) = 0 \\ \left(U_{C11}-U_{C13}\right)\cdot p_1 + \left(U_{C21}-U_{C23}\right)\cdot p_2 + \left(U_{C31}-U_{C33}\right)\cdot\left(1-p_1-p_2\right) = 0 \\ \left(U_{C12}-U_{C13}\right)\cdot p_1 + \left(U_{C22}-U_{C23}\right)\cdot p_2 + \left(U_{C32}-U_{C33}\right)\cdot\left(1-p_1-p_2\right) = 0 \end{cases} \Leftrightarrow$$

$$\begin{cases} \left[\left(U_{D11}-U_{D31}\right)-\left(U_{D13}-U_{D33}\right)\right]\cdot q_1 + \left[\left(U_{D12}-U_{D32}\right)-\left(U_{D13}-U_{D33}\right)\right]\cdot q_2 + \left(U_{D13}-U_{D33}\right) = 0 \\ \left[\left(U_{D21}-U_{D31}\right)-\left(U_{D23}-U_{D33}\right)\right]\cdot q_1 + \left[\left(U_{D22}-U_{D32}\right)-\left(U_{D23}-U_{D33}\right)\right]\cdot q_2 + \left(U_{D23}-U_{D33}\right) = 0 \\ \left[\left(U_{C11}-U_{C13}\right)-\left(U_{C31}-U_{C33}\right)\right]\cdot p_1 + \left[\left(U_{C21}-U_{C23}\right)-\left(U_{C31}-U_{C33}\right)\right]\cdot p_2 + \left(U_{C31}-U_{C33}\right) = 0 \\ \left[\left(U_{C12}-U_{C13}\right)-\left(U_{C32}-U_{C33}\right)\right]\cdot p_1 + \left[\left(U_{C22}-U_{C23}\right)-\left(U_{C32}-U_{C33}\right)\right]\cdot p_2 + \left(U_{C32}-U_{C33}\right) = 0 \end{cases} \Leftrightarrow$$

By making the substitutions the relation will have the following Nash solution:

$$\begin{cases} a_{11} = \left[\left(U_{D11} - U_{D31}\right) - \left(U_{D13} - U_{D33}\right)\right] & a_{12} = \left[\left(U_{D12} - U_{D32}\right) - \left(U_{D13} - U_{D33}\right)\right] \quad b_1 = \left(U_{D13} - U_{D33}\right) \\ a_{21} = \left[\left(U_{D21} - U_{D31}\right) - \left(U_{D23} - U_{D33}\right)\right] & a_{22} = \left[\left(U_{D22} - U_{D32}\right) - \left(U_{D23} - U_{D33}\right)\right] \quad b_2 = \left(U_{D23} - U_{D33}\right) \\ a_{31} = \left[\left(U_{C11} - U_{C13}\right) - \left(U_{C31} - U_{C33}\right)\right] & a_{32} = \left[\left(U_{C21} - U_{C23}\right) - \left(U_{C31} - U_{C33}\right)\right] \quad b_3 = \left(U_{C31} - U_{C33}\right) \\ a_{41} = \left[\left(U_{C12} - U_{C13}\right) - \left(U_{C32} - U_{C33}\right)\right] & a_{42} = \left[\left(U_{C21} - U_{C23}\right) - \left(U_{C31} - U_{C33}\right)\right] \quad b_4 = \left(U_{C32} - U_{C33}\right) \end{cases}$$

The values for the probabilities are presented below:

$$\begin{cases} a_{11} \cdot q_1 + a_{12} \cdot q_2 + b_1 = 0 \\ a_{21} \cdot q_1 + a_{22} \cdot q_2 + b_2 = 0 \\ a_{31} \cdot p_1 + a_{32} \cdot p_2 + b_3 = 0 \\ a_{41} \cdot p_1 + a_{42} \cdot p_2 + b_4 = 0 \end{cases} \Leftrightarrow \begin{cases} q_{01} = -\dfrac{b_1 \cdot a_{22} - b_2 \cdot a_{12}}{a_{11} \cdot a_{22} - a_{12} \cdot a_{21}} \\ q_{02} = -\dfrac{b_2 \cdot a_{11} - b_1 \cdot a_{21}}{a_{11} \cdot a_{22} - a_{12} \cdot a_{21}} \\ p_{01} = -\dfrac{b_3 \cdot a_{42} - b_4 \cdot a_{32}}{a_{31} \cdot a_{42} - a_{32} \cdot a_{41}} \\ p_{02} = -\dfrac{b_4 \cdot a_{31} - b_3 \cdot a_{41}}{a_{31} \cdot a_{42} - a_{32} \cdot a_{41}} \end{cases} \Leftrightarrow$$

The values for utility functions for the Nash point are calculated by using the following equation system:

$$\Rightarrow \begin{cases} U_{0Defender} = \left(p_{01}, p_{02}, 1 - p_{01} - p_{02}\right) \cdot \begin{bmatrix} U_{D11} & U_{D12} & U_{D13} \\ U_{D21} & U_{D22} & U_{D23} \\ U_{D31} & U_{D32} & U_{D33} \end{bmatrix} \cdot \begin{pmatrix} q_{01} \\ q_{02} \\ 1 - q_{01} - q_{02} \end{pmatrix} \\ U_{0Challenger} = \left(p_{01}, p_{02}, 1 - p_{01} - p_{02}\right) \cdot \begin{bmatrix} U_{C11} & U_{C12} & U_{C13} \\ U_{C21} & U_{C22} & U_{C23} \\ U_{C31} & U_{C32} & U_{C33} \end{bmatrix} \cdot \begin{pmatrix} q_{01} \\ q_{02} \\ 1 - q_{01} - q_{02} \end{pmatrix} \end{cases} \Leftrightarrow \quad (8)$$

$$\Leftrightarrow \left(U_{0Defender}, U_{0Challenger}\right)$$

By analyzing the Nash points one can determine for the Defender and Challenger the direction of their decision in order to minimize loses within their national cyber infrastructure or to maximize the effectiveness of their attacks upon the adversary's national cyber infrastructure. The rezult can be applied for each of the four national cyber infrastructure domains defined at the beginning of this article by using the COL Warden's theory (The military cyber infrastructure component; The social media cyber infrastructure component; The economic cyber infrastructure component; The governmental cyber infrastructure component).

6. Conclusions and Future Works

The main goal of this research is to create and analyze a cyber threat model focused on attacker. Building such a model will help understand and predict cyber-attacks and thus improve the defenders ability to identify weaknesses in its cyber infrastructure, adopt strategic measures to overcome those limitations and overall increase the cyber infrastructure capabilities.

Another novelty introduced in the article is the approach method employed for modeling the nations state cyber infrastructure. In this direction the authors based their approach on the COL Warden's five ring theory and defined a model composed of four dimensions. This model allows the performance of the risk analysis processes of the cyber threats from the national perspective and can be used by Challenger nations to identify the most effective attack directions and by Defender nations to identify the weakest defensive points.

The actual estimations and calculus was performed by using concepts from the bimatrix game theory and three canonical strategies specific to the informational war. The most important novelty of this paper is the employment of the Goel-Okumoto software failure model for building the utility functions utilized in the cyber threat risk analysis. In this way the nations will have a mathematical tool for founding future strategic measures.

In the article the authors performed a classification of the attacking strategies based on the five canonical strategies of the information war model (Barron, 2013; Moga & Ogîgău-Neamțiu, 2017; Ogîgău-Neamțiu & Moga, 2017). The classification will help the Challenger to identify the measures required to implement once decision on which strategy is made but can be employed also by the Defender to uncover the Challenger's goals.

This research could be further developed by adding to the games theory a more complex agent model will contain cultural characteristics and previous Defender and Challenger experience.

Appendix A

The discovery of the IP addresses for the DNS servers was performed by scanning each of the four subcomponents of the national cyber infrastructure. For this process it was used the (A 1.1.) script, the ServiceEnumeration() function providing the requested data. The identification of the IP address range for the LAN, MAN and WAN network from each of the components of the national cyberinfrastructure is performed by using the function DeterminingNetworkRange() from the script (A 1.2). Those scripts are contained in Kali Linux distributions.

```
ServiceEnumeration(internetDomain) {
cd /usr/bin
ListOfDNSserversOfInternetDomain
= ./dnsenum -- enum internetDomanin          (A1.1)
return
ListOfDNSserversOfInternetDomain
}
```

```
DeterminingNetworkRange(internetDo
main){
dmitry -wnspb internetDomain -o
/root/Desktop/dmitry-result                  (A1.2)
return dmitry-result.txt
}
```

In order to identify all running machines from the national cyber infrastructure there will be utilized tools from Kali Linux, more specifically Nmap. The function IdentifyingActiveMachines() from script (A 1.3) will have as input the results of script (A 1.2). The identification of the open ports, operating systems and service daemons installed on machines will be conducted by running the scripts (A 1.4), (A 1.5) and (A 1.6).

```
IdentifyingActiveMachines (dmitry-
result.txt){
Define ActiveMachineList
Foreach(IP address of  dmitry-result.txt){
ActivMachine = Nmap –sP IP
Add  ActiveMachine to                        (A1.3)
ActiveMachineList
}
return  ActiveMachineList
}
```

```
FindingOpenPorts(ActiveMachineIP){
Define ActiveMachinePortsList
ActiveMachinePortsList = Nmap
ActiveMachineIP
Select only open ports of
ActiveMachinePortsList                       (A1.4)
return ActiveMachinePortsList
}
```

```
OperatingSystemFingerprinting(ActiveMachineIP){
Define
ActiveMachineOSFingerprintingList
ActiveMachineOSFingerprintingList =
Nmap –O ActiveMachineIP
return
ActiveMachineOSFingerprintingList
}
```
(A1.5)

```
Servicefingerprinting(ActiveMachineIP){
Define ActiveMachine
Servicefingerprinting List
ActiveMachine Servicefingerprinting
List = Nmap –sV ActiveMachineIP
return ActiveMachine
Servicefingerprinting List
}
```
(A1.6)

The joined outputs of all used scripts will be synthetized with script no. (A 1.7) which will provide information about: DNS IP addresses, IP addresses range, open ports, operating systems, installed service daemons, etc. from all computer networks LANs, MANs and WANs for each of the components of the national cyber infrastructure

```
InformationGathering(InternetDomain){
ServiceEnumeration(internetDomain)
dmitry-result.txt =
DeterminingNetworkRange(internetDomain)
ActiveMachinesList =
IdentifyingActiveMachines (dmitry-result.txt)
Define
FindingOpenPortsListOfInternetDomain
OperatingSystemFingerprintingListOfInternet
Domain
ServicefingerprintingListOfInternetDomain
Foreach(IPActiveMachines of
ActiveMachinesList){
FindingOpenPortsItem  =
FindingOpenPorts(IPActiveMachine)
OperatingSystemFingerprintingItem  =
OperatingSystemFingerprinting(IPActiveMachine)
ServicefingerprintingItem =
Servicefingerprinting(IPActiveMachine)
FindingOpenPortsItem  Add
FindingOpenPortsListOfInternetDomain
OperatingSystemFingerprintingItem  Add
OperatingSystemFingerprintingListOfInternetD
omain
ServicefingerprintingItem  Add
ServicefingerprintingListOfInternetDomain
}
return FindingOpenPortsListOfInternetDomain
OperatingSystemFingerprintingListOf
InternetDomain
ServicefingerprintingListOfInternetDomain
}
```
(A1.7)

```
ServersListOfInternetDomain =
Analyze nature of demons of
ServicefingerprintingListOf
InternetDomain and

OperatingSystemFingerprintingListOf
InternetDomain
```
(A1.8)

```
InternetDomainList = {
Government,
Military,
Economy,
Social Media-Social Network              }
```
(A1.9)

The outputs provided by scripts (A 1.7), (A 1.8) and (A 1.9) will allow each state to create the image about the adversaries national cyberinfrastructure with detailed information about the number of routers, switches, computers, servers, open ports on each of the four levels defined in the beginning of the article. The obtained data can be further used, by applying the Goel-Okumoto model to emulate that infrastructure and estimate, by using games theory bimatrix techniques, how the infrastructure will behave when different types of attacks will be conducted upon it. The defender can also use these techniques in order to analyze its own infrastructure and identify high risk areas and use that information in order to base its further strategic decisions for increasing its cyber infrastructure resiliency.

REFERENCES

Barron, E. (2013). *Game Theory, an Introduction*, *Second Edition*, ch. 3., John Wiley & Sons, Inc.

Heriyanto, T., & Allen, L. (2014). *Kali Linux: Assuring Security by Penetration Testing*, Birmingham: Packt Publishing.

Min Xie Yuan-Shun Dai, & K.-L. Poh. (2004). Computing System Reliability Models and Analysis, *Kluwer Academic Publishers*, 101-104.

Moga, H., & Boşcoianu, M. (2015). Massive Cyber-attacks Patterns Implemented with BDI Agents, *6th International Conference on Aerospace, Robotics, Manufacturing Systems, Mechanical Systems, Mechanical Engineering, Biomechatronics and Neurorehabilitation* (*Applied Mechanics and Materials*. *OPTIROB, ICAEM, ICREB 2015), Vol. 811*, 383-389.

Moga, H., & Boşcoianu, M. (2016). Using BDI Agents in Flexible Patterns for Cyber-Attacks over Electrical Power Infrastructures, *Applied Mechanics and Materials, IACSIT/IACT/UASTRO OPTIROB*, 97-104.

Moga, H., & Ogîgău-Neamțiu, F. (2017). Modelarea amenințării cibernetice interstatale utilizând evaluarea polieuristică a deciziilor, In *Managementul situațiilor de risc în contextul crizelor de securitate*, Sibiu: Editura Academiei Forțelor Terestre „Nicolae Bălcescu”.

Ogîgău-Neamțiu, F., & Moga, H. (2017). Profilul psihologic al războinicului cibernetic și hackerului non-statal bazat pe matricea de decizie polieuristică, In *Managementul situațiilor de risc în contextul crizelor de securitate,* Sibiu: Editura Academiei Forțelor Terestre „Nicolae Bălcescu”.

Poisel, R. A. (2013). Information Warfare and Electronic Warfare Systems, In *Artech House Electronic Warfare Library, ch. 4*, 107-139, Boston, London: Artech House Publishers.

Pritchett, W. L., & Smet, D. (2013). *Kali Linux Cookbook.* Birmingham: Packt Publishing.

Warden, J. A. (2000). *The Enemy as a System*, available at: http://www.ciar.org/ttk/mbt/strategy.Warden.enemy-as-a-system.html.