Computers and Electrical Engineering 73 (2019) 128–144

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Turkish national cyber-firewall to mitigate countrywide cyber-attacks☆

Arif Sari

Department of Management Information Systems, Girne American University, Canterbury, United Kingdom

ARTICLE INFO

Article history:
Received 25 November 2017
Revised 6 November 2018
Accepted 7 November 2018

Index terms:
National cyber firewall
Artificial neural networks
Radial basis function
Turkey
Cyber-attack
Intrusion Detection System
DoS
National security

ABSTRACT

This research introduces "Seddulbahir," the first Turkish national cyber-firewall system. Proposed as the first of its kind, Seddulbahir resists possible cyber-attack threats against Turkey's internet infrastructure. Seddulbahir uses the artificial neural network radial basis function (RBF-NN) approach to generate rules that can detect 21 different attacks classified as probing, DoS (Denial of Service), U2R (User-to-Root), and R2L (Remote-to-Local) through the analysis of 66 different network service flows and based on three communication protocols. Results indicate that our proposed approach detects abnormal traffic with high efficiency, low cost, and has a wide detection range, providing accurate, flexible, and effective results in contrast to traditional methods. This paper also outlines the current state of cyberspace in Turkey, provides an analysis and detailed model of the latest cyber-attacks generated against Turkey, and investigates the working mechanisms of national cyber firewall systems used by developed countries such as Russia, China, and the United States.

1. Introduction

In developed countries such as the U.S.A., U.S.S.R., the United Kingdom, and China and after World War II, the superpowers diversified their investments in various innovative cyber infrastructures. Since then, these governments have developed new cyber security approaches and policies, established cyber-armies, and designed new hardware and software technologies in order to emerge as global cyber-powers. The main theme behind these investments was not "how to harm" but "how to benefit by inflicting harm" through using aggressive Internet tactics that would hinder and/or stop potential perpetrators.

One of the main reasons, among others, of this diversification of development in cyberspace is that traditional military strikes are observable by the people under attack at the moment they occur, and their effects can be anticipated. On the other hand, a cyber-weapon attack is not seen or easily anticipated, and the attack itself typically involves temporary damage and no permanent harm.

The possible military wars that might occur between developed countries leads to permanent harm and considerable loss in terms of power, politic, demographic, societal, financial, economic and international dimensions, as experienced in WWII. For this reason, cyber weapons emerged and are used in war between developed countries. Today, these wars take place in the cyber world. However, in developing or underdeveloped countries, this advancement seems less while military battles continue.

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. Martinez Perez

E-mail address: arifsarii@gmail.com

https://doi.org/10.1016/j.compeleceng.2018.11.008
0045-7906/

The 21st century's cyber wars have become more visible with the development of cyber weapons. They have led to the diversification of cyber-attacks and have spread into all dimensions of everyday life, including financial markets, hospitals, airports, universities, shopping centers, hotels, cafes, and restaurants. For this reason, countries have invested considerable budgets for research and development on the basis of the country's cyber policies.

Cyber firewall projects have been developed by the world's leading countries such as Russia, China, and the U.S.A. in order to provide cyber intelligence infrastructure and security for their own countries. Unlike many well-known firewall working mechanisms, the firewalls that these countries have developed have technology that can provide system security and counter-attack measures in various situations.

According to an analysis presented in 2015, the U.S.A., China, Taiwan, and Russia are the leading countries of origin for cyber-attacks generated against Turkey [1]. In addition to this, Turkey holds the 9th place for having the highest number of attacks out of twenty countries while representing 3% of the total global malicious activities, and they rank at 15th regarding malicious codes [2]. Even though Turkey has increased its activities and presence in cyberspace, it still continues to lag behind its key allies such as the U.S.A. and Russia. The evidence can be observed from the consequences of large-scale country-wide cyber-attacks that originated from allied countries against Turkey in 2015.

The development of national cyber weapons is an inevitable need in order to provide country-wide protection against large-scale volumetric cyber-attacks. However due to lack of infrastructural developments, demographic structures, educational systems, political barriers, limitations in the industrial market, and technological know-how, such advancement in cyber warfare becomes restricted in Turkey.

The major contributions of this paper are:

A proposal for the first Turkish national cyber-firewall system called "Seddulbahir," which provides a novel approach to using artificial intelligence for classification and correlation of network flows in order to detect DDoS attacks with high efficiency and low cost.

In addition, an analysis of the KDD CUP 99 intrusion detection full data set with deployment of an artificial neural network radial basis function (RBF-NN) approach is proposed for accurate classification of 21 different attacks (categorized as: probing, DoS, U2R and R2L) and through the analysis of 66 different network service flows based on three communication protocols (TCP, UDP and ICMP) against different type of cyber-attacks.

The rest of the paper is organized as follows:

In Section 2, the current state of Turkey in cyberspace and recent initiatives are described. Next, in Section 3 the latest large-scale country-wide cyber-attacks generated against Turkey are elaborated upon and is based on different aspects. Presented in Section 4 are the working mechanisms, attacks, and defenses made through the national cyber firewall systems of China and the U.S.A. In addition the Chinese Great Firewall/Great Cannon, the NSA Quantum Insert (QI), and Russia's Roskomnadzor are described. Background and related work are discussed in Section 5. Section 6 defines the proposed national firewall system architecture, RBF-NN simulation, and makes a comparison of the existing systems and further deployment policy and integration of the first Turkish national cyber-firewall system to enhance country-wide security. Finally, Section 7 concludes the paper.

2. Current state and recent initiatives of Turkey in cyberspace

Cyber-intelligence provides a significant advantage for countries to collect information about a state or a non-state actor. The National Intelligence Service (MIT) is one of the authorized units that collects intelligence to prevent possible cyber-attacks and threats in Turkey. Since MIT is authorized through legal regulations to prevent cyber-attacks, the organizational infrastructure of MIT has been reformed with a special workforce. MIT started to seek experts in the fields of Signal Analysis and Applications, Crypto and Crypto Analysis, Cyber Activities, Satellite Communication, Geographical Information Systems, Telecommunications Systems, Software Development, Hardware Development, Mobile Application Development, Information Security and Internet Technologies, System Analysis, Mechanical System Design, System Support and Training and Data Processing.

In order to provide public safety against cyber-threats, in 2011 the Turkish National Police (TNP) established a "Combating Cyber Crimes Department," which belongs to the Ministry of Interior Affairs to fight against cyber-crimes in Turkey [3].

The Information Technologies and Communications Authority (BTK) is the institution that regulates and supervises the telecommunications sector in Turkey. The BTK was established on January 29, 2000 [4]. The report presented by BTK in May 2009 contained suggestions related to the investigations on how cyber-attacks should inspected, how evidences should be gathered, and how legislation authorities will clarify the security forces and judiciary on the corresponding cyber-threat topic.

The Technological Research Council of Turkey (TÜBİTAK) was established in 1997 as a new network security group, and a contract was signed with the Ministry of National Defense in 2000. The National Research Institute of Electronics and Cryptology (UEKAE) collaborated with TÜBİTAK and participated in NATO exercises that developed and coordinated the Cyber Emergency Response Team (CERT) [5].

So far there have been 3 national cyber-security exercises conducted in Turkey in 2008, 2011 and 2013, which was supported through the cooperation of TUBITAK and BTK. In these exercises, topics related with log analysis, port scanning, distributed denial of service (DDoS), WEB security scan, WEB application scan, social engineering, and the capture the flag contest were covered [5].

The authorities known as the main actors of the country's cyber security include the Cyber Security Council, which belongs to the Ministry of Transport, Maritime Affairs and Communications, the National Cybercrime Intervention Center (USOM), the Information Technologies and Communications Authority (BTK), and the Telecommunication Communication Presidency (TIB). These agencies published a strategic report that related to the latest attacks and made specific reference to backdoors, built-in malware, and other vulnerabilities that may be present in imported hardware, and they also stated the importance of continued development of its national hardware as well as a national Operating System (OS), search engines, social websites, and web browsers [6]. In addition to this, the report stated the importance of national research and development of cyber-security oriented products and the need for development of technological know-how around the country.

3. Country-wide large-scale cyber-attacks in Turkey

In network system infrastructure designs, specific parameters such as, total bandwidth, total number of users, total server load, and the numbers of instant requests per second are taken into consideration for the determination of optimal load capacity for system resource consumption. The values such as optimal processing speed, optimal load capacity, fault-tolerance level, etc., are determined in order to expose the configuration of an optimal server system. Based on this determination, the proposed network infrastructure design is deployed by slightly exceeding the proposed values to prevent any negative circumstances or occurrences.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are two well-known cyber-attacks that have been generated on network systems often. A DoS attack is an attack type that prevents systems from being accessed by legitimate users by flooding the server or server's bandwidth with malicious instant requests.

In the case of DoS/DDoS attacks, a targeted system is flooded with instant requests which exceed the optimal load capacity of the system and this causes the system to become exhausted. In addition to this, the accessibility of the system can be targeted by flooding these instant requests into a targeted system's bandwidth.

The hacker group "Anonymous" has accused Turkey of helping ISIS since November 26, 2015 [7]. Due to these arguments, the hacker group has attacked a variety of public and private sector websites belonging to Turkey. Two large-scale cyber-attacks were generated against Turkey on December 14, 2015 and December 24, 2015.

A large-scale cyber-attack generated against Turkey targeted the Turkish Domain Name Servers (NIC.TR) hosted at Middle East Technical University (METU). The type of cyber-attack has been detected as one of the well-known cyber-attack types that is called the Distributed Denial of Service (DDoS) attack. This attack originated from an unknown location and succeeded in slowing down the overall Internet connection within Turkey.

The following subsections of this research paper expose the anatomy of the attack, the economic consequences of the attack, and the perception of the operational dimensions in detail.

3.1. Anatomy of the attack

The attack by the hacker group Anonymous targeted the Turkish DNS servers with a total load capacity of 40 Gbps on the 14th of December 2015 and had a DDoS speed and volume that reached up to 220 Gbps and which led to approximately 40,000 Turkish domain names being shut down and out of service. The main aim of this attack was to make the targeted servers ineffective and unreachable by flooding more instant requests than the capacity of its available resources. More than 40,000 web pages with a ".tr" extension (Turkish DNS servers) were disabled and unreachable during the attack.

Attacks targeted many services that are used by a majority of the society in everyday life such as DNS servers and banks and e-government services in order to spread the effect of the attack and to increase the impact of the reactions.

One of the NIC.TR servers in Europe is managed by the RIPE (European IP Networks) headquarters, which is responsible for DNS servers and IP allocation in Europe. RIPE explained that the DNS attack generated against the "NIC.TR" servers was very sophisticated and that the attackers were constantly changing their attack methods during the attack.

Based on previously documented cyber-attacks, the speed of an average DDoS attack is around 2 Gbps, and the attack in Turkey was around 40 Gbps. This increase in speed indicates that the attack was considerably serious compared to other attacks observed globally. In addition to this, the capacity and the impact of the attack included both the country-wide Internet traffic and the regional Internet service providers and it lasted for a total of 10 days.

The Cloud Flare attack was used by Turkey against this cyber-attack. Because of the volume, duration and sophistication of the cyber-attack generated on December 14, 2015 against Turkey, the use of the Cloud Flare system was not successful in mitigating the impact of the attack.

3.2. The economic aspect of the attack

As a result of the DDoS attack generated on Turkish DNS servers in 2015, Internet services have considerably slowed down, and the online banking systems of many Turkish banks collapsed and failed to provide online banking services for a period of time and, as a result of the attacks, generated on E-government services.

The wide spread effect of the attack caused the unavailability of post devices that prevented the use of credit cards throughout the country. The event caused financial and moral losses in civil society as well as disrupting the community's

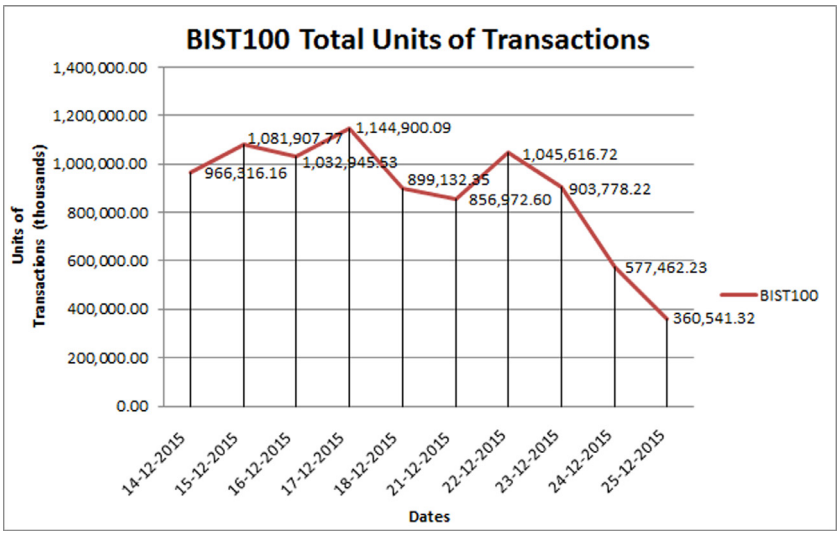

Fig. 1. Istanbul stock exchange index (BİST100) total units of transactions (thousands units).

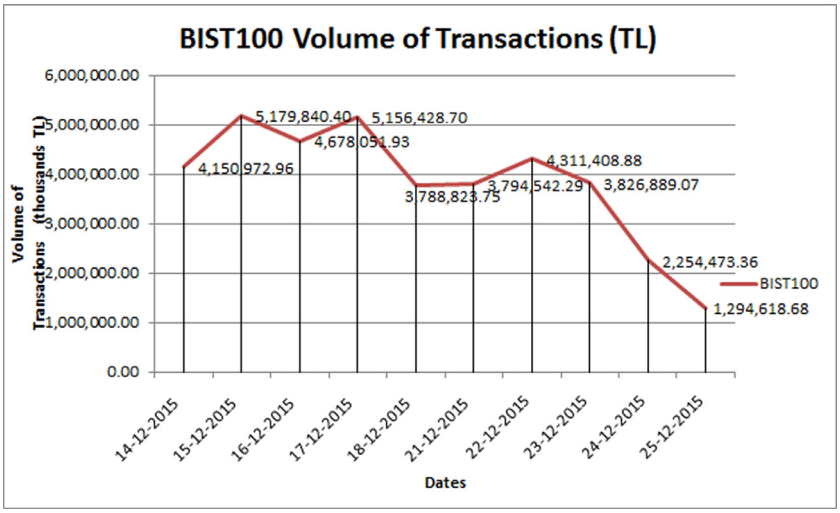

Fig. 2. Istanbul stock exchange index (BİST100) total volume of transactions in terms of Turkish Lira (thousands).

businesses (tradesmen, restaurants, bars, cafes, pharmacies, shopping malls, etc.). In addition, there were major losses in the stock market due to the disruptions of the Internet, and many banks experienced difficulties in stock trading and online transactions.

The financial details of the Turkish stock market and bank operations indicated concretely that the bank customers and the people who make a profit through operating transactions such as gold, dollars, stocks, funds, and bonds became victims of the collapse of the online services of those banks which were caught unprepared for the massive attack.

During a 2 week period, the Istanbul Stock Exchange investigated and measured the impact of the attack on the Exchange. As can be seen from Fig. 1 below, the number of transactions for BIST100 fluctuated between 900,000 to 1200,000 of units daily between December 14, 2015 and December 23, 2015. In the first wave of the attack on December 24, 2015, the number of transactions on the Istanbul Stock Exchange index (BIST100) was 577,462 (thousands) units at the end of the day and the trading volume of the BIST 100 reached to 2,254,473 TL. As of December 25, 2015, this figure has fallen to levels of 360,541 units of transactions and 1,294,618 TL [8]. Figs. 1 and 2 below illustrate the pre and post state of the market during the attack and signify an impact on the Istanbul Stock Exchange in terms of the units of transactions and the volume of transactions.

As can be seen from Fig. 1 above, the total units of transactions conducted on December 21, 2015 was 856,972.60, and this number increased to 1,045,6161.72 on December 22,2015 and slightly decreased to 903,778.22 units on December 23, 2015. However, the country-wide Internet disruptions were due to the massive attack and created a significant impact on the diminishing total units of transactions of the BIST100 index to the level of 577,462.23. The continuous impact of the attack

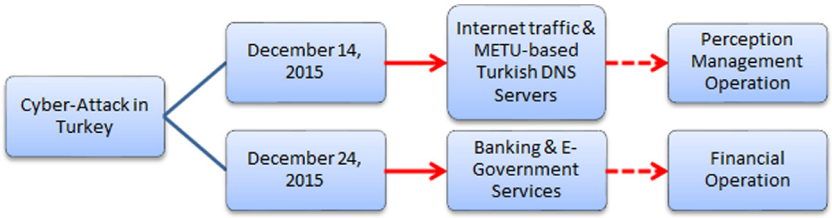

Fig. 3. Organization of cyber-attack on Turkey in December 2015.

on December 25, 2015 influenced the decline of total units of transactions of the BIST100 index to the level of 360,541.32, which is considered the least number of transactions for BIST100 since 2012 [8]. Fig. 2 below illustrates the impact of an attack on the BIST100 index in terms of the volume of transactions in Turkish Lira.

Fig. 2 also illustrates a significant decrease of total volume of transactions in the BIST100 index during the attack in December 2015. The BIST100 index total volume of transactions were around 3,794,542.29 (thousands TL) and it slightly increased to 4,311,408.88 on December 22, 2015 and declined to 3,826,889.07 on December 23, 2015. However, all of these short-term soft decreases changed with the massive attack on December 24, 2015. The Total volume of transactions in the BIST100 index declined sharply to 2,254,473,36 (thousands) TL. This decline continued sharply on December 25, 2015 to the level of 1,294,618.68 (thousands) TL.

These figures simply show that the cyber-attack on December 24, 2015 caused a huge blow to the volume of transactions in the stock exchange market that led to the loss of hundreds of millions of TL in only one day. In addition, it is observed that the brokerage institutions in the Turkish market had a loss of 3–4 million TL in daily commissions. Even though the attack led to serious damage in Turkey's financial market and caused significant economic damage, no research, report, or explanation has been carried out by the authorities in order to expose the analysis of the current economic loss and moral damage.

3.3. "Perception of the operation": an aspect of the attack

The attack on December 14, 2015 was targeted on the METU-based Turkish DNS servers, which are a national DNS extension representative of Turkey (a.k.a. NIC.TR) that provides access to web pages with ".tr" extensions. The intention of the attack was to degrade the reputation and trust created against the public through 4 well-known strategic powers of the Turkish government, which include the land forces, air force, naval forces and space forces, and the attack was meant to disengage the national image of the country through disrupting the Turkish DNS servers and all of the related services.

The national Turkish banks that operate within Turkey became inoperable and all of the online services that are integrated with the e-government were disabled due to attack. The credit cards issued by the national Turkish Banks became unusable during the attack, which led to a significant loss in the public both financially and morally. The intention was to create a perception of "governmental inadequacy" against the public safety and to degrade the state through this perception.

This attack was organized as a "perception operation" to create a negative view against the state by representing the state as "inadequate" to protect the public and to prevent victimization of its citizens. In the public's perception which is less familiar with the IT and information infrastructure, the attack was damaging.

3.4. General findings of the attack

The hacker group Anonymous undertook this high-volume and large-scale attack [9]. However, when all of the DDoS attacks that were generated by Anonymous were analyzed to date, there were several significant and different aspects that arose between them and the DDoS attack that targeted Turkey in December 2015. These findings can be concluded as:

a) This cyber-attack was organized to hit 2 different targets at different times in December 2015. The first wave of the attack took place on December 14, 2015 and targeted Turkey's Internet traffic and METU-based DNS servers. The second wave of the attack took place on December 24, 2015 and targeted the banking and e-government services. Fig. 3 illustrates the organizational scheme of the attack.

The different targets simply expose the intention of the second wave of the attack as it is shown in Fig. 3 above. The first attack was intended to skew the perception of the management operation while the second wave of the attack aimed to create a financial loss as a result of the financial operation itself.

Turkey shot down a Russian warplane near the Turkish-Syrian border due to the Russian aircraft ignoring warnings and violating Turkish airspace on November 24, 2015. This event was known as the first time in decades that a NATO country shot down a Russian war plane. The Russian President Vladimir Putin said that the downing of the jet is "a stab in the back by the terrorists' accomplices" and "will have serious consequences for Russian-Turkish relations" [10].

As shown in Fig. 3, the second wave of an attack engaged thirty days after the Russian aircraft was dropped. The second wave of an attack was felt massively by the community since these attacks were organized consciously, and they intensively hit commonly used services throughout the country.

b) The hacker group called Anonymous was not involved in the attacks that would negatively affect the normal lives of civilians; instead, they organized attacks for propaganda purposes.

However, Anonymous's video, which was prepared and published before the December 2015 attack, included the speech that claimed an attack on civilian airports [7]. For example, the cyber-attack in June 2015 at a Polish airfield affected civilians through chaos as a result of unnoticed changes made to flights during the cyber-attack [11]. Additionally, this high-volume country-wide attack led to a significant aftermath toward the public both financially and morally. At the same time, the attack did not affect politicians and governments.

c) The hacker group Anonymous had eleven on-going cyber-attack operations [7]. However, no major states were targeted by Anonymous in these Middle Eastern operations except for an event in Thailand and some occurrences in small states in the Middle East. Moreover, the attacks on the violation of freedom of expression and human and animal rights were presented as the general justification for the operations by Anonymous.

The general justification for the ongoing cyber-attack operations of Anonymous was that of being against the violation of freedom of expression and human and animal rights. It was the first time that this group had threatened to harm civilians of a country like Turkey.

d) The fact that none of the banks that were attacked were Russian-owned and that the first news of the attack spread from news centers to those close to Russia, it can be ascertained that this attack might have been instigated by Russia under the name of "Anonymous."

The attack hit the major national Turkish banks such as Garanti Bank, Akbank, Is Bank, and Ziraat Bank: none of these banks were Russian-owned [12].

e) The attack did not resemble any of the familiar attack dimensions that Anonymous has been credited for in terms of volume and strategy.

The previous attacks by Anonymous were around 2.5 Gbps and at least one attack reached up to 220 Gbps on December 2015. Similar to the December 2015 attack, large-scale volumetric attacks require substantive infrastructure support such as powerful servers and an Internet service provider. Anonymous is a hacker group that does not have any leader, central coordinator, or manager, and they do not receive any known-financial support. At the same time, their profitability motive is questionable since they have the infrastructural support and to perform such high volume attacks. Due to these reasons, the reality of one hacker group to organize such a professionally planned attack to be carried out in two stages (December 14, 2015 – December 24, 2015) and to intensely target online public services such as the ".tr" extension websites, e-government services, and national Turkish banks is problematic.

f) The duration of an attack also emerges as another important factor since it could not have been carried out by amateur attackers (Lamers or Newbies) without an effective attacking engine.

It is not possible for an attack to be carried out over a 2 day period and to affect the Internet traffic country-wide and the critical public services by amateur hackers or simple botnets. Such large-scale high-volume attacks require the hiring of advanced servers to form stronger botnets, which would require a backer with strong financial incentives.

4. National cyber firewall projects

The national Cyber Firewall projects were organized in developed countries due to the volume and impact of cyber-attacks increasing rapidly over the last decade. In this section, the development of cyber-technologies, national cyber firewall projects, and weapons in countries such as Russia, China and the U.S.A. are investigated. The Fig. 4 below illustrates the classification of countries with corresponding cyber technology.

In the following sections, each corresponding country's national cyber security technologies is investigated in detail to expose the impact and importance of these technologies in cyberspace.

4.1. NSA the quantum insert (QI) – USA

The Office of Tailored Access Operations (TAO) is a cyber-warfare intelligence-gathering unit of the National Security Agency (NSA) which was established in 1998 [13]. The role of TAO is to identify, monitor, and gather intelligence from computer networks and systems belonging to these networks and that are used by foreign entities of the United States [14]. The previous documents were leaked by NSA contractors who stated that the TAO engineers have special software templates that were used to break into commonly used network components such as routers, switches, and firewalls belonging to multiple product vendor lines [14].

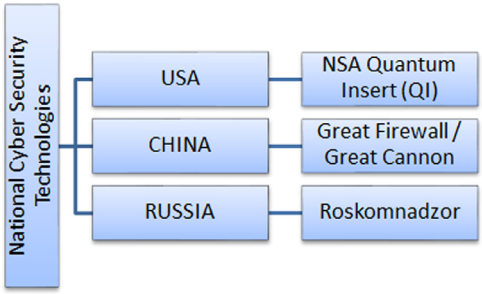

Fig. 4. Developed countries with cyber technologies.

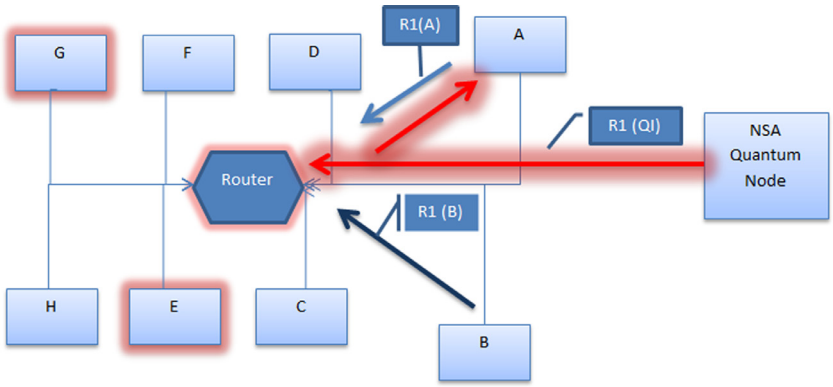

Fig. 5. Sample quantum attack scenario.

TAO has developed an attack suite called “QUANTUM Insert” (QI) that relies on comprisable network components such as routers and that then duplicates Internet traffic by typically sending “QUANTUM” requests and delivering these requests before a legitimate request arrives to the intended target. During this time, the malware is also loaded [15]. The “QUANTUM” architecture suite was developed on the basis of the Man-On-The-Side Attack Principle whereby the attacker has limited access to the communication channel that allows the attacker to read the content and insert new messages but not to modify or delete any messages sent by the other participant. The global surveillance disclosures reveal that by using the tools developed by TAO, NSA’s compromises reached industrial scale exploitation in 2013. It was exposed in 2013 that NSA’s “QUANTUM” infected 50,000 computer system controls and used them temporarily during certain periods of cyber-attacks [15]. It was also proven that NSA spied on U.S.A. citizens through “QUANTUM” and tracked hundreds of thousands of Americans phone calls [16]. Even the British Intelligence service GCHQ has used the “QUANTUM” insert to set up fake LinkedIn web pages and spied on the Belgian mobile phone giant “Belgacom” [17]. The targeted victims, who were high-level employees of the company, had “authorization” to the Belgacom infrastructure and when accessed, they were redirected to fake websites that contained malware. The Fig. 5 below illustrates the “QUANTUM” architecture based on the Man-On-The-Side Principle.

Node (B) sends legitimate HTTP requests to node (A) in order to communicate with node (A). Meanwhile, NSA Quantum Node sends its fake request (R1(QI)) that is delivered to node (A) before the legitimate request of node (B) (R1(B)) is delivered to the router and due to the router has been compromised by NSA Quantum node request. Node (A) responds to a Quantum Node Request and is redirected through the HTTP request to the site which will infect its system. The Quantum Node does not interfere with the communication between node (A) and node (B); however, it infects node (A) and communicates with node (A) based on the intended purpose.

Likewise, as in the scenario explained above, the node (E) and node (G) are the compromised and infected nodes on the network that communicated with the QI Node previously. The controls of the infected nodes belong to NSA, and they may be used for different cyber-attack purposes such as forming an anonymous botnet to generate high-volume large-scale DDoS attacks. Fig. 6 below illustrates an anonymous network that was organized from infected nodes and compromised routers of separate networks controlled by NSA through QI, which can perform high-volume large-scale DDoS attacks against an intended target.

As shown in Fig. 6 above, a network formed from a combination of infected nodes from different networks generates high volumes of network traffic through compromised routers. The consideration of more numbers of compromised routers and infected nodes increases the volume of traffic flow significantly. This high volume of network traffic of compromised nodes may flow through compromised routers to any NSA intended target which may lead to exhaustion of the targeted

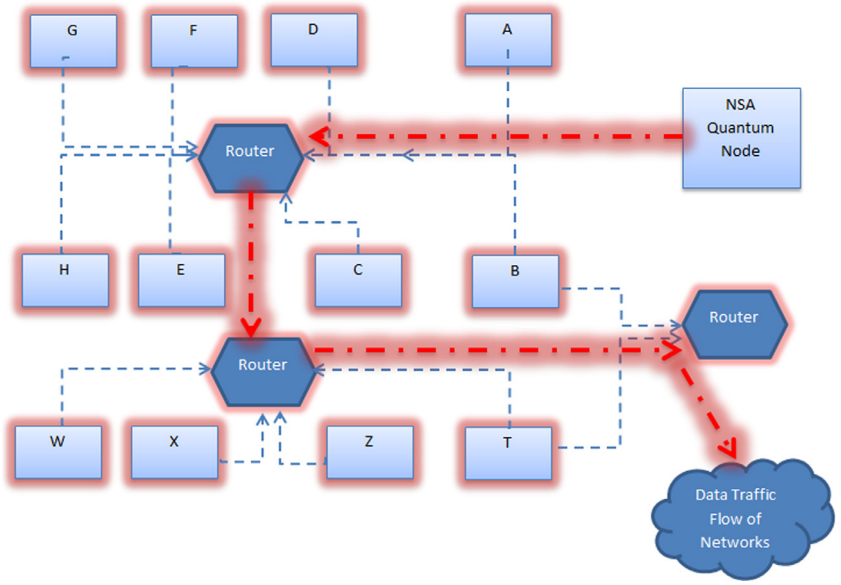

Fig. 6. Anonymous Botnet formed by NSA through QI.

system. Even if such volumetric attacks were organized by the NSA through this strategy, it cannot be proven since the compromised nodes and routers belong to different distributed and independent networks.

4.2. Great Firewall/Great Cannon – China

The Great Firewall and Great Cannon were developed by the Chinese Ministry of Defense within the scope of the Golden Shield Project in China. These cyber weapons were exposed as a result of a massive DDoS attack on Amazon servers in the United States in March 2015 [18]. China launched a massive DDoS attack on the servers of GitHub and GreatFire.org websites on March 16, 2015. These sites were hosting various tools to provide full-accessibility to the Internet which was against the country-wide censorship applied by the Chinese government. The massive attack led to sites being out of service for 2 days after the attack and caused massive financial losses for companies.

Fig. 7 below illustrates the architecture of China's Great Firewall and Great Cannon. As shown in the figure, the Great Firewall works as an on-path system that monitors the complete network traffic flow through a network tap (TAP) between China and the outside world. The network traffic flow is filtered based on the Chinese censorship policy and is interrupted by injecting the TCP Reset (RST) package into the communication between end points in case of any violation of policy [19].

The Great Cannon works as an in-path system that directly injects and suppresses the traffic flow. The Great Cannon examines individual packets based on the selected flow of traffic generated between targets or sets of addresses and this decreases the amount of traffic and helps to avoid the computational cost of TCP byte stream reassembly. The Great Cannon intercepted the incoming network traffic to the servers of the Chinese national search engine "Baidu.com's", which hosts commonly used social and advertising scripts and receives massive amounts of requests daily. The individuals send requests to one of the Baidu servers associated with certain javascript file requests with a variety of queries [19].

The Great Cannon intercepts the transmission of the incoming request address enlisted as a target and it drops the request before it reaches the Baidu servers; and instead, it sends a malicious script back to the requesting user as a response. The aim of the Great Cannon is to re-route the targeted traffic to any intended destination. The malicious script received by the requesting user, which is outside of the Chinese network, becomes a part of an "anonymous botnet" that unintentionally participates in a DDoS attack to any intended target determined by China.

The Great Cannon has the authority to interfere and re-route the traffic flow of local Internet service providers that connect to the Great Firewall country-wide. This opportunity is an advantage for the Great Cannon to operate based on high-volume traffic and the Man-In-the-Middle Principle. The Chinese Censorship policy forces the Chinese population to use the national search engine "Baidu" massively, which leads to the creation of a high-volume of network traffic flow within the country and it also creates a sufficient capacity to flood any network and carry out a serious DDoS attack.

As a result, The Great Firewall and Great Cannon are two independent systems with different functionalities, yet they have similar characteristics and a significant structural relationship. The National Firewall developed by China filters all incoming network flow to China and interferes with the incoming network flow through the TCP (RST) package injections based on the Chinese Censorship Policy before it gets into the country's internal network. In addition to this, the Great Cannon monitors traffic from services such as national service providers, national search engines, and national data centers,

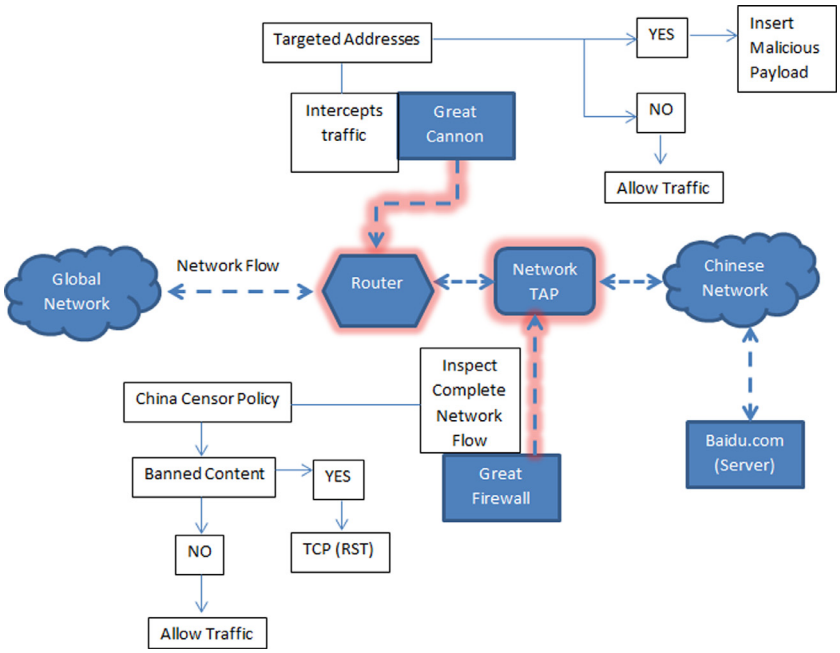

Fig. 7. Architecture of China's Great Firewall and Great Cannon.

and it may re-route this massive flow of traffic to any desired destination. The consideration of Internet usage by the Chinese population and their services makes the Great Cannon a serious cyber-threat against other countries.

4.3. Roskomnadzor – Russia

The Federal Service for Supervision in the Sphere of Telecom, Information Technologies, and Mass Communications (Roskomnadzor) was established by Russia pursuant to Decree No. 1715 on December 3, 2008 [20].

Russia regulates the national cyber-security policy of the hardware devices that are used to provide the Internet, and they claims that the physical network infrastructure must be subject to control of the sovereign country. The social networking sites were forced to obey the data storage law of the country which makes them route their traffic to the Russian telecommunication system and host their servers in Russia. Popular sites such as LinkedIn have been blocked for violating the national data storage law after a court ruling approved by Putin in 2014 [21]. The country's national cyber-security policy requires strict control on domestic Internet security in order to provide national security. For that reason, Russia has started to develop its own infrastructure to establish a national security with specialized cyber-weapons similar to China.

In order to establish a control over the complete network flow of the country, it is compulsory to connect all network infrastructure components to each other within the country. Russia established the national social network "Vkontakte" in October 2006 [22], the national search engine "Yandex" in 2000 [23], and thus partially established the national Internet. However, it is also necessary to establish national data centers within the country where citizens will deploy their personal data in order to establish a firewall like China's. The Fig. 8 below represents the existing network infrastructure and components deployed by Russia in order to establish national cyber security.

As shown in Fig. 8, it is important to organize all internet traffic interfaces under a single national Internet framework and to control a whole country's Internet traffic through a single national cyber firewall.

However, due to lack of infrastructural facilities, it is a long and difficult process to create a restrictive national cyber firewall project similar to that of China. This project requires the deployment of large-scale data centers that will require major changes in the entire infrastructure and architecture of the entire Russia information system industry. In addition to this, a possible decrease in service quality will cause service providers to lose a great deal of control over the Internet traffic.

Meanwhile, it is known that China has employed 2 million people for monitoring online activities within the country's network. In the context of a national cyber-security policy, many countries, including Russia, do not have the human power at these numbers. Even though a similar formation could take place based on a population percentage, the figure for Russia would be around 200,000. Although figures in this amount are possible on a population basis, the possibility is beyond the material feasibility of Russia. Russia does not appear to be economically ready to pay the economic cost of blocking or filtering a large portion of the country-wide Internet.

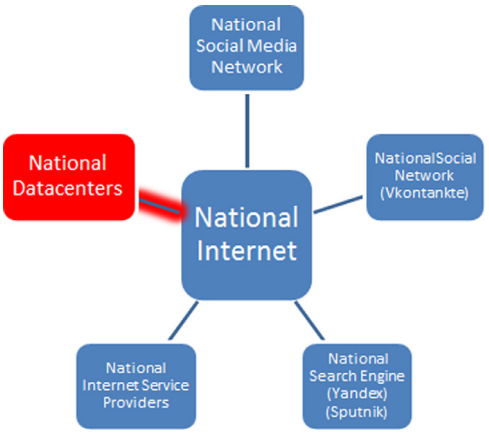

Fig. 8. Russian National Security Infrastructure Components.

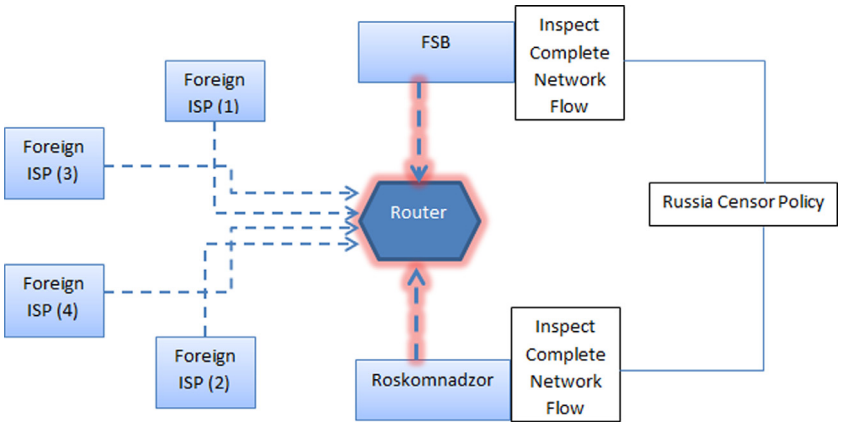

Fig. 9. Two-tier Architecture of Russian Censor Policy.

Because of the circumstances stated above, Russia could not switch to a national cyber firewall system or use a two-tier Internet control mechanism based on a country censorship policy. Fig. 9 illustrates the two-tier architecture of the Russian censorship policy used by Roskomnadzor.

In the first tier, all foreign Internet service providers operating in Russia are obliged to direct their network flow of all personal data to the platforms and routers under the control of the FSB (Russian Intelligence Service). In addition to this, Roskomnadzor administers and controls the servers that maintain the social media content in Russia. In the second tier, the contents of the traffic flow are analyzed by the FSB and/or Roskomnadzor, whereby inappropriate contents are intercepted and censorship is applied based on the national censorship policy.

5. Background of the study and related work

The use of machine learning methodologies such as Naive Bayes [24], k-means [25], C4.5 decision tree [26], SVM [27] and KNN [28] has become popular among researchers to use in traffic classification while proposing intrusion detection systems. Researchers have proposed neural network architectures for intrusion detection to achieve high efficiency and low costs [24]. Different types of proposals developed such as backpropogation, neural network (multilayer perceptron) [25]. The neural network provides opportunity to develop algorithms that can be used to model complex networks or attack patterns and predict problems. It is trained to identify users based on what commands they use during a given day. In a system of 10 users and a data set collected for 12 days, the neural network was 96% accurate in detecting anomalous behavior with a false alarm of 7%.

A similar neural network system has been used to develop an adaptive intrusion detection system for TCP/IP networks. The system was trained based on previous well-known intrusion data so intrusion is detected from an analysis of predetermined models for both normal and intrusion actions learnt from training data set. Researchers have achieved 95% of performance using two-hidden multi-layer perceptron neural networks and the error backpropogation training algorithm [26].

The K-nearest Neighbor Classifier (KNNC) has been used by DARPA to evaluate 1998 DARPA data through a simulator of an Air Force Local Area Network. The developed system provides an excellent detection rate. The system detection rate is excellent but it is computationally expensive for real-time implementation due an increase in simultaneous processes requiring more processing power to compute and analyze the detection process [28]. This was one of the main disadvantages of the KNN since the performance is severely affected by a small size of training data which cannot accurately represent the traffic classes but use of huge number of data costly and requires processing. Apart from this, the KNNC clustering technique has a significant disadvantage, since it is based on the calculation of a numeric distance between observations.

A network service flow can have many features to detect anomalies or there may be co-related features which affect each other to expose anomalies; however, the clustering methods are unable to capture the relationship between different features of a single record, which degrades the accuracy of the attack detection.

Naïve Bayes classifiers were used by researchers for intrusion detection that resulted in an increase of an Bayesian Network due to increase of an number of attacks and features modeled by a Bayesian network, so increased the complexity of the deployment. [24]. Data mining approaches were also deployed to provide intrusion detection based on specific features of symbolic data and form of incoming packages of network service flow. Researchers have used Radial Basis Function and statistical features to detect intrusions and anomalies. The KDD CUP 99 data has been used for training; however, due to small number of descriptors used to train the system, the entire system could not successfully function in large scale networks [28].

A combination of neural network and hybrid fuzzy logic is used by researchers to develop intrusion detection systems. The developed model has been used with KDD CUP 99 data to train their system. It provides attack detection for a specific number of network flows that uses 10% of the KDD CUP data [28].

Machine learning (ML) framework is introduced by the researchers to propose intrusion detection. The proposed system classifies attack types by using KDD CUP 99 dataset. The proposed approach provides better results than the existing ML based intrusion detection solutions [26].

Genetic Algorithm is used by researchers to propose a new intrusion detection system that has used 10% of KDD CUP 99 data to train their system. However the system rules were not updated with the new data which leads corresponding system rules to be outdated and expose lack of detection [26].

Researchers have compared the performance of naïve Bayes with the C4.5 decision tree algorithms. The results indicate that the naïve Bayes algorithm has a better performance with respect to existing best performance metrics perform on KDD CUP 99 data [24].

The research has focused on input-based triggering and event-based control for leader-following problems to prevent network failure or central coordinator problems [28]. It is clearly shown in this section that very little effort has been spent on the development of an intrusion detection system based on RBF-NN through the analysis of the KDD CUP 99 intrusion dataset.

6. Seddulbahir - Turkey

The meaning of the word “Seddulbahir” is "a set in front of the sea." The cyber-attacks generated from the overseas countries represent the majority of cyber-attacks against Turkey. The national cyber-firewall Seddulbahir will respond to overseas cyber-attacks and filter incoming network traffic flow. The majority of cyber-attacks in Turkey were generated from Malaysia, Switzerland, Russia, and the U.S.A. in 2015; worldwide in 2016, the greatest numbers of attacks were generated from South Korea, the U.S.A., and China [29].

It is difficult to determine the origin of an attack or to predict which country is behind the attack due to the inexistence of boundaries of developing Internet technology in cyberspace. Governments are obliged to ensure the public safety of citizens in cyberspace, and due this reason they deploy strict cyber policies which have conflicted with the freedom of expression over the Internet. National cyber-policies and national technologies developed by governments, such as the national censorship policies, national communication infrastructure with national public services to monitor and control the incoming/outgoing flow of network traffic within the country.

Appropriate analysis of incoming/outgoing flow of network traffic within the country is a key factor for accurate detection and prevention of cyber-attacks. The diversification of package types and services in an incoming/outgoing network flow requires the development of an adaptive, low-cost intrusion detection system to differentiate, detect, and prevent cyber-attacks.

In order to propose a flexible, reliable, low-cost, and adaptive intrusion detection system, an artificial neural network algorithm is deployed on the proposed system and tested using previously collected intrusion datasets proposed by DARPA.

The KDD CUP 99 intrusion dataset has been used to train and test proposed systems. The KDD CUP 99 intrusion full data set contains the TCP-dump raw data of about five million connections collected from seven weeks of network traffic records of the training sets. In addition to this, two weeks’ worth of test data set records, having around two million network traffic records, was collected [30].

The dataset contains 21 different attacks (categorized as probing, DoS, U2R, and R2L) and 66 different network service flows based on three communication protocols (TCP, UDP, and ICMP). This dataset has been used by researchers in the literature for analysis and development of intrusion detection systems. It has been provided by the Massachusetts Institute of Technology (MIT) Lincoln labs has a different classification of intrusions, network service flows, and novel communication

Table 1
Number of attack types and categories in training KDD CUP 99 dataset.

Normal	Probing	DOS	R2L	U2R
Normal (97,277)	Nmap (231)	Land (21)	Spy(2)	Buffer_overflow(30)
	Portsweep (1040)	Pod (264)	Phf(4)	Rootkit(10)
	Ipsweep (1247)	Teardrop (979)	Multihop (7)	Loadmodule (9)
	Satan (1589)	Back (2203)	ftp_write (8)	Perl(3)
		Neptune (107,201)	Imap(12)	
		Smurf (280,790)	Warezmaster(20)	
			Guess_ passwd (53)	

Table 2
Selected features as input parameters from KDD CUP 99 intrusion dataset.

INPUT		
Feature name	*Description*	*Feature number*
protocol_type	type of the protocol, e.g. tcp, udp, and icmp (3 protocol types)	1
service	Network service on the destination, e.g., http, telnet, smtp etc. (66 service types)	2
flag	Normal or error status of the connection. Possible status are SF, S0, S1, S2, S3, OTH, REJ, RSTO, RSTOSO, SH, RSTRH, SHR	3
src_bytes	number of data bytes from source to destination	4
dst_bytes	number of data bytes from destination to source	5
wrong_fragment	number of "wrong" fragments	6
hot	number of "hot" indicators	7
num_failed_logins	number of failed login attempts	8
logged_in	1 if successfully logged in; 0 otherwise	9
num_failed_logins	number of failed login attempts	10

protocols in the military networking environment. The dataset contains a variety of TCP/IP connection features such as duration, type of protocol, dst_hst_service_count, etc.; the data set also contains different types of attacks such as warezmaster, pod, perl, smurf, satan, etc. and different network service flows such as http443, http, netbios_ns, netstat, pop_3, smtp, etc. [30]. Table 1 indicates the number of attack types and categories from the KDD CUP 99 intrusion data set.

10% of the entire KDD CUP 99 intrusion data set has been used to prepare the proposed system based on RBF-NN. A normalization process is conducted due to the complexity and redundancy of the records in the dataset.

In the first stage, the proposed system differentiates between normal and malicious incoming/outgoing flow of network traffic within the country. Later, the system distinguishes the type of attack that is generated through the clustering and classification stage. In order to complete the classification process, we have used a specific number of features from the KDD CUP 99 intrusion dataset. We chose 10 input parameters as shown in Table 2 below. Since some of these features and sub-features were not numeric, a specific feature number has been assigned for each feature and its service category as a result of mapping progress.

As mentioned above, 10% of the selected KDD 99 CUP intrusion data is normalized, classified, and mapped. The mapping progress is done by numbering the features using numbers 1–12 to represent the possible statuses. For example, in the attack types, the "Normal" class is mapped to the number 1. Likewise the "Probe", "DoS", "U2R", "R2L" are mapped to numbers 2–5 respectively. The other sub-categories such as services and flags are also mapped respectively.

The proposed model design was based on RBF-NN. The ANN is an adaptive parallel distributed information processing model which consists of a set of simple processing units called "neurons, a set of synapses, the network architecture, and a learning process used to train the networks. The RBF is constructing global approximations of functions using combinations of basic functions centered on weight vectors. It is used for discrimination and classification tasks and also for binary pattern classification. RBF networks include three layers which are the input layer, one hidden layer, and an output layer [30].

The transformation from input space to output space is nonlinear and the transformation from the hidden unit space to the output space is linear, the set of Basis functions $\{0, (x)|i = 1, 2, \ldots, M\}$ is defined as follows;

$$(I)i(x) = G(\|x - t_i\|) = \exp(-\|x - t_i\|), i = 1, 2, 3, \ldots M \tag{1}$$

Where $[t_i|i = 1, 2, \ldots, M\}$ is the set of M centers to be determined and x is one of the training (input) data in a set $\{x_i = 1, 2, \ldots, N\}$ of size N. Typically, the number of basis functions, M is less than the number of data points. Our aim is to find the suitable w values in order to minimize the Euclidean Norm.

$$\|d - Gw\|^2, \text{ where } d = [d_1, d_2, \ldots, d_N] \tag{2}$$

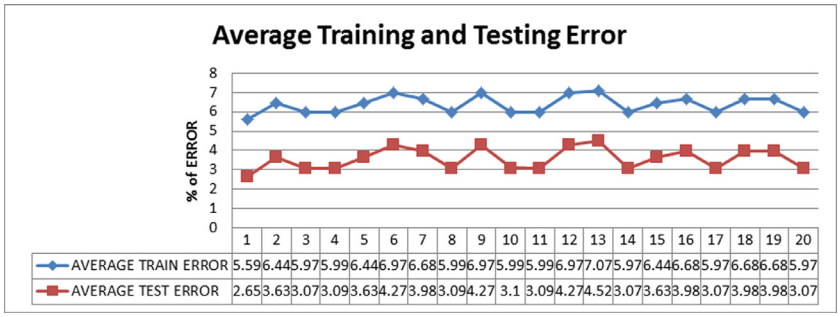

Fig. 10. Average test and train error of proposed RBF-NN algorithm on KDD CUP 99 data.

$$G = \begin{bmatrix} G(x_1 - t_1) & G(x_1 - t_2) & \cdots & G(x_1 - t_M) \\ G(x_2 - t_1) & G(x_2 - t_2) & \cdots & G(x_2 - t_M) \\ \vdots & \vdots & & \vdots \\ G(x_N - t_1) & G(x_N - t_2) & \cdots & G(x_N - t_M) \end{bmatrix} \tag{3}$$

$$w = [w_1,\ w_2, \ldots w_M]^T$$

The vector d is an N-dimensional desired response vector, the matrix G is an N x M matrix of Green's function and the vector w is M-by-1 wt vector for the linear transformation from the hidden unit space to the output space. The minimum norm solution to the over determined least squares data fitting problem can be given as follows:

$$W = \left(G^T G\right)^{-1}{}_{G^T d} \tag{4}$$

The set of centers $\{t_i | i = 1, 2, \ldots, M\}$can be selected randomly from the set of data points and can be selected using the clustering techniques to find the suitable centers or can be selected using the gradient descent algorithm. In this study, we used random selection to find the set of centers for the Radial Basis Functions. The proposed algorithm for the cyber-firewall designed and deployed is shown below (Algorithm 1).

The results obtained from the experiment are illustrated in Fig. 10. In this experiment, a normalized, classified, and mapped data set is divided into training data (90%) and test data (10%). We used a different number of centers and a different number of neuron values for the experiment, as 2, 4, 6, 8, to train the system and collect the best-trained values. The proposed model trained is based on 90% of the classified dataset. In the testing phase, only the first 10 input groups of 10% of the data were entered into the system in order to observe a possible set of outputs and error rates. This output group, which is generated by the system, is compared with the actual output group which was not inputted or processed by the system and it was observed that the proposed system approached the actual output within the percentage error margin.

Fig. 10 above indicates the average training error and average test error of the proposed system based on the actual system data. The system has an average test error ranging from 2.65% to 4.52% with an average of 3.57%, and an average training error ranging from 5.58% to 7.07% with an average of 6.37%.

Algorithm 1
Proposed algorithm.

S1: START
S2: DEFINE #of_attack
S3: DEFINE #of_iteration
S4: DEFINE #of_input
S5: DEFINE #of_output
S6: LOAD RawG [#of_attack] [#of_input + #of_output]
S7: G [#of_attack] [#of_input + #of_output]∈←NORMALIZE(RawG [#of_attack] [#of_input + #of_output])
S8: SET center {ti|i = 1,2,3,…..,M}
S9: RBFDATA[#of_attack] [#of_input + #of_output]←randomize([attack order])
S10: Calculate Weight_of_each_input, $W = (G^T G)^{-1} G T^d$.
S11: CALCULATE training_error
S12: CALCULATE testing_error
S13: IF (iteration > #of_iteration), go to S9
S14: IF (training_error > %8 || testing_error > %8), go to S8
S15: IF (error < %8), record avg(training_error), avg(testing_error)
S16: STOP

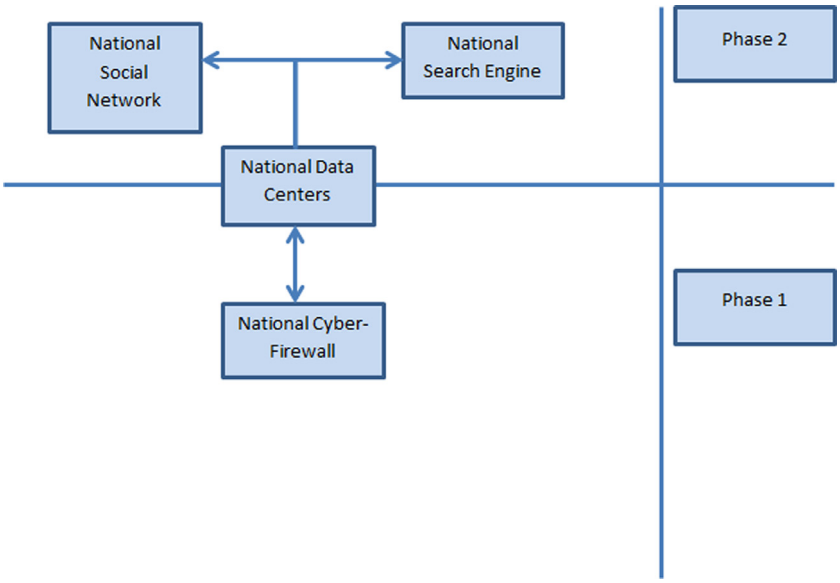

Fig. 11. Seddulbahir project phases.

As it is clear from Fig. 10, the proposed system functions effectively and learns 94% of the attack patterns successfully and it is also shows that the trained system will make a correct prediction of at least 97.99% according to the results of the average testing error.

This proposed model is deployed as a first of its kind that uses the RBF-NN algorithm for training and testing through the KDD CUP 99 intrusion dataset. The proposed systems achieved the best results for the detection and classification of attacks in contrast to similar proposals. The work proposed by researchers is focused on the nearest neighbors based density peaks approach to intrusion detection by using the KDD CUP 99 intrusion dataset [30]. The proposal achieved successful detection of probe attacks with 20% efficiency while other attack clusters were not considered. The back propagation neural networks applied to the anomaly and network intrusion detection by the researchers using the KDD CUP 99 intrusion data [30]. The proposal did not expose the training and testing results of the proposed architecture. The proposal made by researchers for detecting DDoS attacks against the data center was conducted with a correlation analysis. The K-nearest neighbor's traffic classification, with a correlation analysis, is deployed for detecting DDoS attacks against data centers. However, the distribution of the data is one of the main concerns for the proposed approach since it conducts polar clustering while our proposed approach uses rectangular clustering which is not affected by the distribution of data. In polar clustering mechanisms, specific calculations are required to measure the area that will be narrowed down to where the data is distributed. Our proposal does not rely on the existence of KDD CUP 99 intrusion dataset since once the system is trained it uses the new anomaly results detected in the system as an input for the next decision. So the system does not function based on static data and updates itself through its self-training functionality. The successful completion of "Countrywide-Security" with the Seddulbahir project consists of 2 stages as shown in the architecture of the Seddulbahir project phases in Fig. 11 below.

The Seddülbahir project consists of two phases. The second phase of the project entails the modeling of a national search engine and the design of a National Social Network whereby these two components will be integrated. Also, the establishment of the National Data Center services will need to host the data generated by these two services. The National Data Center will be responsible for providing the infrastructure for the extended services and will provide data storage services countrywide. The completion of the project will be finalized after the completion of the design and deployment of the National Cyber-Firewall which will be integrated with the entire system.

The primary goal of Seddulbahir is to legitimately defend the public and governmental systems of the country against cyber-threats which may arise from inside or outside of the country. For this reason, the national cyber-firewall, national search engine, and national social network services are within the scope of this project.

In contrast to other cyber-firewall systems, Seddulbahir will be designed not to interfere with the rights and freedoms of the public in cyberspace or within the country but to protect them based on the basis of the citizens' rights and freedoms.

The Seddulbahir project design is being developed based on a combination of cyber-firewall systems from China, Russia, and the U.S.A. that have proven security and access control through the integration of communication systems and network infrastructures within their respective countries. The project will function with the integration of 5 basic components that would work together as shown on Fig. 12 below.

First class priority should be given to the development of the national search engine which is used as a public source to ensure national cyber security.

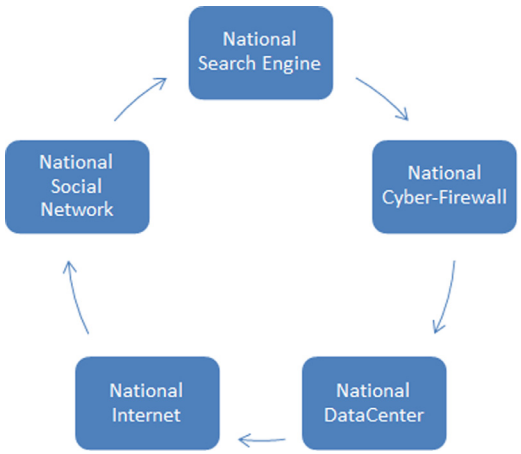

Fig. 12. Seddulbahir National Cyber-Firewall System Components.

Table 3
Technological infrastructures of countries in cyber-space.

Country	National search engine	National social network	National internet	National datacenters	National cyber-firewall – cyber-weapon
USA	Google.com Yahoo.com	Facebook-Twitter-Instagram-Snapchat- LinkedIn – Youtube – Skype	Available	Available	NSA Quantum System
Russia	Yandex – Sputnik	Vkontankte - Odnoklassniki	Available	Not Available	Not Available
China	Baidu – Sogou – Youdao	Tencent,Weibo,Renren, PengYou, QQ, Douban, Youku, Diandian	Available	Available	Great Firewall/Great Cannon
Turkey	Not Available	Not Available	Available	Not Available	Not Available

Table 4
Available search engines in Turkey.

Abacho	Arama	Netbul
Abaragambi	Asiaminor	TurkArama
Altanvista	Baybul	Indexturkiye
Arabul	Mynet	Rehber

It is well-known that Russia (Yandex), the U.S.A. (Google), and China (Baidu) have gathered intelligence by using OSINT (Open Source Intelligence) technology through national search engines that they developed in order to prevent variety of possible threats and attacks in advance. In addition to this, in the past, these search engines have been used in high-volume large-scale cyber-attacks generated by these countries. The desired national search engine intended to be developed by Turkey will provide both intelligence and countrywide national search engine services for the public.

Based on the 2010 Arab Spring and 2013 Turkey Gezi Park Events, we see how an effective use of social networks (Facebook, Twitter, Instagram) can be used to manipulate the perception of the public against governmental authorities. Turkey experienced a lack of control over social media and faced serious social media manipulation issues during the Taksim Square protests, and they therefore blocked social media channels during the events.

Developed countries such as Russia, China, and the U.S.A. established their own national social networks and special attention has been given for the monitoring of these services based on strict national censorship and cyber-crime policies to prevent social manipulations within their countries.

Table 3 below illustrates the technological infrastructures of developed countries in cyber-space. As mentioned previously, the majority of the technologies required for Turkey to deploy the proposed National Firewall System are not available yet.

Table 4 below shows the search engines available in Turkey. The existing search engines possess significantly negative performance rates in terms of design, speed, accuracy, and reliability compared to other search engines developed by other countries.

The possibility of widespread usage of the National Social Network is quite low since the national cyber-security policy does not address any restrictions for foreign social networking sites operating within the country. In addition to this, applications that are categorized under the “National Social Networking” applications category that are not containing the national design but the names are foreign and are demanding to be domestic.

Table 5
National Social Network examples of Turkey.

http://freelyshout.com	http://www.peplr.com
http://www.raamy.com	http://www.curbaa.com
http://www.hocam.com	http://www.inploid.com/
http://friendplans.com	http://www.takiplen.com

Another important aspect of the establishment of the National Social Networks is to prevent the trend towards the widespread fondness of foreign admiration rising within Turkey. This will also lead the public to communicate and think in their languages and trigger a transfer of specified moral values of the public within the society. The following Table 5 illustrates the national social networks in Turkey. However, none of the following examples contain any desirable national social network features.

At the 25th meeting of the Supreme Council for Science and Technology (BTYK), it was decided to establish a legal, technical and administrative model for the consolidation of the data centers and the public institutions and the establishment of the Public Integrated Data Center of Turkey. The Prime Ministry, the Ministry of Development, the Scientific and Technological Research Council of Turkey (TUBITAK), and TÜRKSAT would be active stakeholders in the project.

It is known that while the development of the system is in progress and continuing throughout the country, the integration of the national banks to e-government systems across the country has been completed. This integration was one of the reasons for the countrywide domino effect during the December 14th and 24th, 2015 attacks that affected integrated institutions and organizations.

7. Conclusion

The current global cyber security situation indicates that the principal of the World Wide Web could be misleading for end users. Thinking that the web is open to all and provides unrestricted access may not be the case as a result of the continued development in national cyber technologies, national cyber-policies, and the continuous cyber-warfare among countries. For example, previously developed cyber-weapons and cyber-firewall technologies isolated Turkey's global internet possibilities and created various limitations in the country's web environment. The current research indicates that we may see the majority of the global networks turning into small intranets that are controlled through strict cyber-policies and monitored through cyber-technologies.

In Turkey, the proposed cyber-firewall system Seddulbahir has been used by the Artificial Neural Network Radial Basis Function algorithm to detect 21 different attack types through 66 different network service flows under different categories. The Artificial Neural Network Radial Basis Function approach was used for the first time with the KDD CUP 99 intrusion dataset for an accurate classification of 21 different attacks (Probing, Denial of Service, User-to-Root, and Remote-to-Local) through the analysis of 66 different network service flows based on three communication protocols (TCP, UDP and ICMP) against different types of cyber-attacks.

Future research could address deploying artificial intelligence oriented and automated mitigation techniques on the proposed Seddulbahir system to enhance and strengthen country-wide networks. In the proposed architecture of the National Cyber-Firewall, Seddulbahir can be deployed on the National Internet and will function similarly to the Great Cannon used by China, and it will be able to monitor the incoming flow of network traffic from the National Social Network, National Search Engine, and National Datacenter. This architecture will also be able to provide protection against cyber-attacks by allowing Turkey to isolate the Internet traffic and to pass all Internet traffic through the National Cyber-Firewall servers.

References

[1] "The most hacker-active countries", InfoSec Institute, 5 August 2015, Accessible at: resources.infosecinstitute. com/the-most- hacker-active-countries-part-i/.
[2] Hekim Hakan, Başıbüyük Oğuzhan. Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. (Cyber Crimes and Turkey's Cyber Security Policies). Uluslararası Güvenlik ve Terörizm Dergisi 2013;4(2):135–58 2013.
[3] Turkey General Directorate of Security, Department of combating cyber crimes, Accessible at: http://www.siber.pol.tr/Sayfalar/hakkimizda.aspx.
[4] Information technologies and communication authority, Accessible at: http://www.btk.gov.tr.
[5] Bicakci S, Ergun FD, Celikpala M. The cyber security scene in Turkey. Center Econ Foreign Policy Stud 2013. Accessible at http://edam.org.tr/document/cybernuclear/edam_cyber_security_ch2.pdf.
[6] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi Güvenliği Derneği (Republic of Turkey Ministry of Transport, Maritime Affairs and Communication, Information Security Foundation), (2012, June), "Ulusal Siber Güvenlik Stratejisi: 2023'ün siber uzayında güçlü ve önder bir Türkiye için" (National Cyber Security Strategy: For a strong and leading Turkey in 2023's cyber space) Accessible at: www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf.
[7] Howell Kellan. Anonymous declares cyberwar against Turkey over alleged ISIS support. Washington Times 2015. Accessible at http://www.washingtontimes.com/news/2015/dec/23/anonymous-declares-cyberwar-against-turkey-over-al/ .
[8] Stock exchange istanbul (BIST) index and daily trading Volume, electronic data delivery system, Central Bank of the Republic of Turkey, Accessible at: http://evds.tcmb.gov.tr/.
[9] Chang Lulu. Anonymous is behind those massive cyber-attacks in Turkey. Digital Trends Comput 2015. Accessible at http://www.digitaltrends.com/computing/anonymous-behind-turkey-cyberattakcs/#ixzz4SNfuFVqI.
[10] Chance Matthew, Martinez Michael. 5 things you need to know about Russian jet shot down by Turkey. CNN MiddleEast 2015. Accessible at http://edition.cnn.com/2015/11/24/middleeast/russia-turkey-jet-downed-syria/.
[11] Wiktor Szary and Eric Auchard, June 22, 2015. "Polish airline, hit by cyber attack, says all carriers are at risk", Reuters Technology News, Accessible at: http://www.reuters.com/article/us-poland-lot-cybercrime-idUSKBN0P21DC20150622.

[12] BirGun, December 25, 2015, “Bankalara ve internet altyapısına saldırıları Redhack üstlendi” Online News, Accessible at: http://www.birgun.net/haber-detay/bankalara-ve-internet-altyapisina-saldirilari-redhack-ustlendi-98913.html.
[13] Aid, Matthew M. (8 June 2010). The secret sentry: the untold history of the National Security Agency. Bloomsbury USA. p. 311. ISBN 978-1-60819-096-6.
[14] Tailored access operations, secret bases, Retrieved: 10/12/2016, Accessible at: http://www.secret-bases.co.uk/wiki/Tailored_Access_Operations.
[15] Floor Boon, Steven Derix and HuibModderkolk. NSA infected 50,000 computer networks with malicious software Accessible at. Handelsblad. Retrieved November 23 http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/).NRC.
[16] Leslie Cauley (5/11/2006). "NSA has massive database of Americans' phone calls" (Accessible at: http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm) . USA Today. Retrieved: December 12, 2016.
[17] Tony Paterson. “GCHQ used 'Quantum Insert' technique to set up fake LinkedIn pages and spy on mobile phone giants” (Accessible at: http://www.independent.co.uk/news/uk/home-news/gchq-used-quantum-insert-technique-to-set-up-fake-linkedin-pagesand-spy-on-mobile-phone-giants-8931528.html). The Independent. Retrieved November 10, 2016.
[18] GreatFire. Cyberspace administration of China, using Baidu 百度 to steer millions of computers to launch denial of service attacks. How the Great Fire Anti-Censorship Project and Amazon’s Cloud Front are under Denial of Service attack. 25th March 2015, Accessible at: https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1.
[19] Bill Marczak, Jakub Dalek, John Scott-Railton, Reports and Briefings, Ron Deibert, Sarah McKune. ‘China’s Great Cannon’. Citizen Lab, munk school of global affairs, University of Toronto, April 2015. Accessebile at: https://citizenlab.org/2015/04/chinas-great-cannon/.
[20] The federal service for supervision of communications, information technology and mass media, December 12, 2016, Accessible at: https://eng.rkn.gov.ru/.
[21] Maria Tsvetkova and Andrew Osborn, November 17, 2016, “Russia starts blocking LinkedIn website after court ruling”, Technology News, Reuters, Accessible at: http://www.reuters.com/article/us-russia-linkedin-idUSKBN13C0RN.
[22] Vkontakte Accessible at https://vk.com/about.
[23] Yandex, December 12, 2016, Accessible at: https://yandex.ru/.
[24] Moore AndrewW, Zuev Denis. Internet traffic classification using Bayesian analysis techniques. In: ACM SIGMETRICS performance evaluation Review, 33. ACM; 2005. p. 50–60.
[25] Erman J, Arlitt MF, Mahanti A. Traffic classification using clustering algorithms. In: Proceedings of the 2006 SIGCOMM Workshop on Mining Network Data; 2006. p. 281–6.
[26] Taboada HeidiA, Baheranwala Fatema, Coit DavidW, Wattanapongsakorn Naruemon. Practical solutions for multi-objective optimization: an application to system reliability design problems. Reliabil Eng Syst Safe 2007;92(3):314–22 ISSN 0951-8320.
[27] Este A, Gringoli F, Salgarelli L. Support vector machines for TCP traffic classification. Comp Netw Intern J Comp Telecomm Network 2009;53(14):2476–90 September.
[28] Roughan Matthew, Sen Subhabrata, Spatscheck Oliver, Duffield Nick. Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification. In: Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement; 2004. p. 135–48.
[29] Lippmann R, Cunningham RK. Improving intrusion detection performance using keyword selection and neural networks. Comp Netw 1999(34):597–603.
[30] Gavrilis Dimitris, Dermatas Evangelos. Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features. Comp Netw 2005;48(2):235–45. ISSN 1389-1286 https://doi.org/10.1016/j.comnet.2004.08.014.

Arif Sari is a chairman of the department of Management Information Systems at Girne American University, Canterbury, United Kingdom. He received his BS degree - in Computer Information Systems and MBA degree - (2008 and 2010) at European University of Lefke, and Ph.D. degree (2013) in Management Information Systems at Girne American University.