SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 5, NO. 6
ISSN: 2054 -7420

The Dark Side of the China: The Government, Society and the Great Cannon

Arif Sari, Zakria Abdul Qayyum and Onder Onursal
Faculty of Business, Department of Management Information Systems,
Girne American University, Kyrenia, Cyprus;
arifsari@gau.edu.tr; zakria_mughal@yahoo.com; onder.onursal@gmail.com

ABSTRACT

The main purpose of this research is to understand the concept of one of the main firewall technology developed within the scope of Golden Shield Project called "Great Cannon" and "Great Firewall" and elaborates the details of this tool in China. The proposed technology deployed in China has claimed to enhance the public safety and country wide national cyber security however there were many other circumstances raised from the legal, ethical and moral issues due to censorship and surveillance of this deployment. The research also elaborates and outlines the effects and technical issues of this deployment since this paper highlights the existing research trends in network security and exposing the current state of the Golden Shield project for the China with its censorship policy.

Keywords: Quantum Insert, Golden Shield, Censorship, Government, China, Great Cannon, Great Firewall, National Firewall

1 Introduction

The In digital age, it is important to understand information technology, information security, and the challenges an interconnected world face. Military capabilities of a country are usually underestimated or not fully understood by population, which is also caused by a not always correct perspective the media suggests. Thinking about evolution of warfare, we understand that not only military strategies have changed, but the tools to carry out the mission are evolving rapidly.

The wars in future would not necessarily require the opponents to even meet each other face to face physically, instead, the resolution of conflicts will take place in cyberspace.

The boundaries will be crossed digitally, not kinetically. That is the victims of cyber war will not be combatants, but civilians – every man, woman, child that are located in the country under attack. Instead of physical damage, the cyber-attacks will be infrastructure based, targeting military systems, financial systems, and security systems [2].

The countries with the most powerful armies in the world - the United States of America, the United Kingdom, Russian Federation, China [1] – have developed and continue upgrading mechanisms to not only provide cyber security within their countries, but also the tools to attack other countries for accomplishing their political, economic and patriotic wishes.

DOI: 10.14738/tnc.56.4062
Publication Date: 5th December 2017
URL: http://dx.doi.org/10.14738/tnc.56.4062

In this report we discuss security and attack tools considered as one of the most powerful in current cyber space, which were created by People's Republic of China in the Golden Shield Project. China's intention is to use information warfare in the cyber realm. This is well implemented by the "Blue Army" – a unit that carries out cyber warfare - which conducts both offensive and defensive cyber missions to protect the infrastructure of China from foreign cyber threats. It is widely reported that the Chinese supposedly use the public Internet and World Wide Web to exploit weaknesses of foreign countries including the United States, England, Canada, Australia, France, Japan, Taiwan, India, Pakistan, South Korea and Vietnam. It is also stated that the Chinese allegedly intrude countries via the Internet to exfiltrate data, and consequently to gain competitive economic advantages [2].

The following section of the report will describe history of the Chinese Golden Shield Project creation, and mechanism and tools designed for cyber security, existing network technologies, its circumvention and cyber-attacks.

2 History of the Internet in China & Creation of Golden Shield Project

The beginning of the use of the Internet in China occurred in 1987, by sending an email with a title "Crossing the Great Wall to Join the World". Up until 1994, the steps have been taken to make the Internet available to the Chinese population. In September 1994, a Sino-American Internet agreement was signed by China Telecom and U.S. Secretary of Commerce, under which China Telecom is to open two 64K dedicated circuits in Beijing and Shanghai through Sprint Corporation of the United States [3].

The initial steps to control the Internet use were taken by the State Council in 1996. The first Internet censorship was called the "Temporary Regulation for the Management of Computer Information Network International Connection", and stated that "No units or individuals are allowed to establish direct international connection by themselves" and "All direct linkage with the Internet must go through ChinaNet, GBNet, CERNET or CSTNET. A license is required for anyone to provide Internet access to users" [2]. In 1997, the Ministry of Public Security announced a number of policies for the Internet users in China, which were approved by the State Council. A few of the listed regulations state that any unit or individual is prohibited to use the Internet to create, replicate, retrieve, or transmit information that incites to resist or breaks the Constitution, law, or administrative regulations; incites division of the country, hatred or discrimination among nationalities; the truth, spreads rumors, or destroys social order; or provides sexually suggestive material or encourages gambling, violence, or murder, terrorism or other criminal activity. In 1998, the project of the Internet content blocking and filtering was started by the Chinese Government, but was not implemented. The project was named the "Golden Shield Project", also widely known as the "Great Firewall of China" [2][4]. The project provides China with Internet censorship at the Internet backbone and internet provider level, and aims to control the information movement between the Internet in China and the global Internet. The initial design planner of the "Golden Shield" and its architect is known to be the President of the Beijing University of Posts and Telecommunications, Fang Binxing. He stated that the creation of the project took five years and was launched in 2003. Another key figure in "Golden Shield" project is Mr. Li Run sen, the Head of the Commission of Science and Technology of the Ministry of Public Security of China, and since 1996 the group leader and chief technical advisor of Golden Shield Project. As Technology Director at MPS, in 2002, he announced the "Information Technology for China's Public Security" to a national audience of Chinese law enforcement, four-day inaugural "Comprehensive Exhibition on Chinese Information System" in Beijing [2].

3 Golden Shield Project and Great Firewall of China

The Ministry of Public Security of China operates censorship and Internet surveillance initiative. The main purpose of the Golden Shield Project, further referred as the Great Firewall of China (GFW) is blocking and restricting access to unauthorized, forbidden content to Chinese Internet users and anyone else within Chinese borders. Some examples of prohibited or blocked keywords are “Dalai Lama”, “human rights”, “democracy” [2]; most of the widely used social network websites like facebook.com, twitter.com, instagram.com, search engines like Google, media - The New York Times, The Wall Street Journal, Youtube, many pages of Wikipedia [6].

The Great Firewall does not allow the access to sites that have specific keywords estimated as threats to public security and safety by blocking IP addresses, TCP ports, HTTP requests, DNS requests [5]. Generally, firewalls are in-pass barriers between the networks through which the traffic from one network flows to another. Yet the Chinese project is called “Great Firewall”, it operates as an on-pass system which eavesdrops on traffic flowing between China and other countries. On-path systems are good for censorship and provide more scalability but less flexible than in-path systems as attack tools, due to inability to control packets that were already sent from server to reach their destination [7][8]. The Great Firewall observes the connections and decides whether their packets should be blocked by reassembling them which provide better blocking accuracy but require additional computational resources [7].

According to [13], Intrusion Detection System (IDS) devices of the Great Firewall of China are placed for keyword filtering at Autonomous Systems (ASes) and router level. There are 24 border ASes and most of them belong to backbone. The majority of internal ASes (87.0%) are within direct reach of border (belonging to the backbone) ASes. The best vantage points for efficient content filtering are in the border/backbone ASes since they can easily serve as choke points, given that IDS devices have enough power and the censors do not intend to monitor domestic traffic. Two of Chinese IPSs – CHINANET and CNCGROUP have the majority (63.9%) of China’s total peerings with other countries and are the major filtering ISP’s. They have different approaches placing their filtering devices. CHINANET, instead of filtering strictly along the border, offloads the burden to its provincial network. While, CNCGROUP has most of its filtering devices in the backbone rather than provincial network, and all its filtering is done within very few hops into China’s address space.

3.1 GOLDEN Shield Project and Great Firewall of China

The Great Firewall performs via three types of content blocking technology, which are DNS Poisoning, IP Address blocking, and filtering URLs and TCP packets for sensitive keywords via deep packet inspection [8][10].

3.1.1 IP blocking (packet dropping)

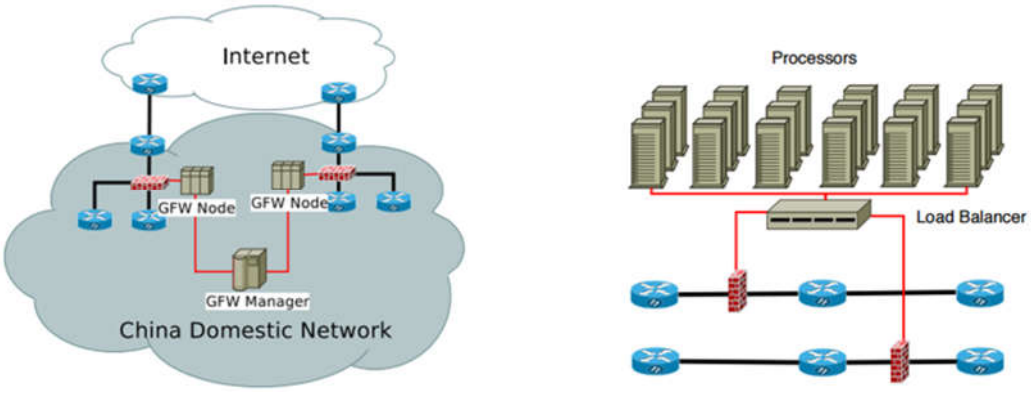
IP blocking is done in case if the access to a certain IP address with potentially sensitive data should be denied [2]. Great Firewall relies on null routing, i.e. dropping or ignoring packets without informing the source that the data did not reach its intended recipient, rather than forwarding them. GFW peers with the gateway routers of all Internet Service Providers in China, and hijacks all traffic to blocked websites by injecting routing information into BGP (Border Gateway Protocol) – routing protocol of global Internet. This way through GFW, the Chinese government maintains the blacklist. Null routing does not add performance impact on gateway routers of ISPs, also there are no special devices needed for

implementing null routing [11]. However, this packet dropping scheme have two main problems: first, the list of IP addresses must be kept up-to-date; second, if a few websites share hosting server with a blacklisted website, all of the websites on the same server will be blocked [2] [16]. IP blocking mechanism is not difficult to circumvent. It can be done by setting up a proxy outside of China or by moving the website to another IP address [11].

3.1.2 DNS (Domain Name System) injection

DNS poisoning of responses for certain domains is one of the primary filtering methods that the Great Firewall of China. The GFW has load-balanced architecture, where on each physical link the reassembly and censorship is done in multiple parallel processes (Figure 1). It performs DNS-based censorship at China's borders, using a blacklist of around 15,000 keywords. GFW nodes operate in clusters of several hundred processes which inject censored responses at a rate of about 2,800 per second [9].

With DNS poisoning method, requested domain names are not resolved, but instead incorrect IP addresses are returned to a requester [2]. Once a DNS request is sent from a user located in China to a certain domain outside of the country, the GFW checks the request and if it finds patterns that match censored content, it sends a poisoned DNS response to the requesting DNS resolver, which due to its position in the network, reaches the DNS resolver faster than the DNS server. The requesting DNS resolver catches the poisoned DNS response from the GFW, and ignores a legitimate response sent by DNS server [9][12].



(a) Overall GFW Architecture (b) Structure of a single GFW node

Figure 1. The architecture of GFW according to [9]

Some of the GFW DNS poisoning studies claim, that if the first DNS response is ignored, then the legitimate response can be received [14]. In another [12], on contrary, it was found that despite of expectations that after the poisoned response sent by GFW, the DNS server sends the correct response to DNS resolver, that was not always the case. In many occasions both the legitimate and the poisoned DNS responses were incorrect. The GFW returns poisoned responses from a small set of incorrect IP addresses. The same IP addresses are used as responses of legitimate DNS responses. These IP addresses are registered in different locations around the world without a clear pattern. If to try accessing these IP addresses, no response package is sent from them. This could mean that either there is no host located at these IP addresses, or that even if there is a host, the responses are filtered either by an outbound firewall or at the network interface. Even if a particular DNS request is not poisoned by GFW, the result will still be unavailable to a user. As it appears, DNS servers within China are poisoned themselves, that is why widely

proposed methods of avoiding DNS poisoning, such as ignoring the first received DNS response or identify and ignore poisoned responses [14], would not always work. As a solution, users should configure their local DNS resolver to point to DNS servers which are outside of the influence of the GFW and not poisoned [12]. Findings show that the main use of the GFW's DNS poisoning is actually to corrupt the cache of DNS servers, but not to poison DNS requests of users [9].

Users outside of China can also be affected by DNS poisoning mechanism of Great Firewall. Collateral damage happens when DNS resolvers outside of China contact authoritative servers located in or at the end of paths that transit China, that is, Chinese censorship is being applied to non-Chinese requests as well [15].

3.1.3 TCP Reset/Keyword blocking

The Great Firewall of China also blocks content by filtering URLs and TCP packets. If a user requests a URL with a banned keyword, or a webpage that contains a keyword, the GFW drops packets by closing the connection between the two points [10]. The keyword-based blocking occurs within the routers that maintain connections between China and the rest of the world [16]. Intrusion detection system (IDS) devices are attached to routers and determine whether the content of packets matches filtering rules. If it does, then the router sends TCP reset packets (TCP RES) to both client and server (Figure 2) [13].

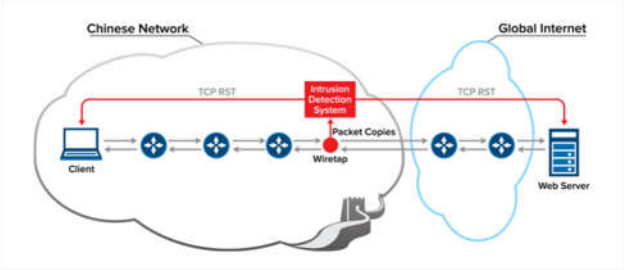


Figure 2. Blockage of sensitive content by injecting forged TCP resets [17].

However, blocking of packets is done not during TCP connection establishment phase, but after the first HTTP GET request. HTTP GET requests are allowed to proceed as normal but the router censors the request and sends a spoofed TCP RST packet (Figure 3) [18]. After TCP resets are sent, further attempts by the same client to request access to the same resource will be disabled for a period from a few minutes to an hour by injecting additional reset packages. However, if the endpoints entirely ignore the TCP resets, they will not have any effect on the client's TCP/IP stack, so the client will have an access to requested web page. IDS systems might also add a discard rule to the main router, rather than issuing resets. There is another occasionally used strategy observed. The GFW sends a fake SYN/ACK packet to some pairs of endpoints with random, invalid sequence numbers. If the SYN/ACK packet generated by the GFW reaches the client before the real SYN/ACK then the connection fails. The client then records the incorrect sequence number from the misleading SYN/ACK and returns the value to the server which is considered as an incorrect ACK value. This occasion triggers a reset packet and the client closes [16].

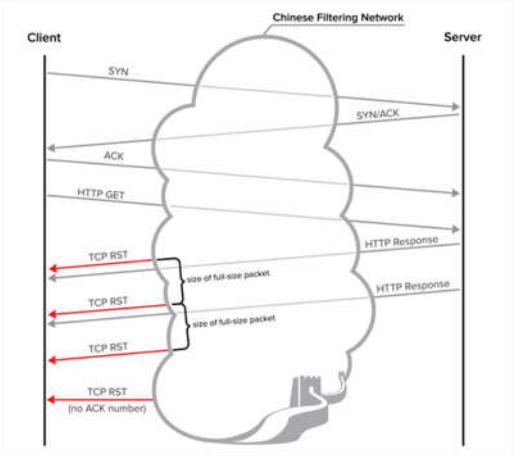


Figure 3. ACK-GET TCP Handshake through the GFW [17]

One of circumvention methods applied through monitoring of keywords by using HTTPS which encrypts content that is potentially to be blocked and thus makes the keyword unreadable in the packet. Another method is to avoid the use of URL so that the keywords cannot be read in plain text. In cases with popular websites, the GFW blocks the access to the entire website by using aforementioned IP address blocking mechanism [10].

3.2 Circumvention methods

There are around 688 million Internet users in China [22], 1-3% (app. 20 million Internet users) of which regularly try to access the open Internet by circumventing the Great firewall [23]. The main anti-censorship tools used by Chinese population and people within the borders of China include proxy servers, VPN (virtual private network) services and Tor.

Proxy servers. Using proxy servers to bypass the GFW can be done by finding some proxy nodes and encrypting the traffic. Proxy servers operate through browsers, connecting a Chinese user's machine with a server located outside the country, and masking the user's IP address with the server's IP address [10]. Popular and free proxy services used in China are FreeGate, Ultrasurf, and Psiphon (version 3). They depend on a range of proxy servers outside China and encrypt all the HTTP traffic in SSL (Secure Sockets Layer) tunnels to these servers. Using proxy is usually does not cost anything to the users, however VPN provides better performance at least in terms of speed and stability [11].

VPN services. VPN and Secure Shell (SSH) services are considered the most powerful and stable tools for bypassing censorship. They work in a similar way to proxy servers, but depend on a virtual, private host or an account outside China.

Users connect their computers to VPN, which encrypts the users' requests and sends them to a foreign server, which processes the actual request. The request is able to bypass the Firewall because it is encrypted [10]. A private encrypted invisible for the GFW channel is created to connect users to a server outside of China. VPN services are usually not free and requite technical professionals for configuration. Usually popular commercial or public VPN services are be blocked by IP address and/or "vpn." domain names, such as vpn.com, vpn. net, vpn.org, vpn.info, etc. [11].

Tor. Tor is a famous anonymous communication and circumvention tool against Internet censorship. It achieves anonymity by re-routing through a series of proxy servers. The complicated encrypted SSL-based

protocols and thousands of proxies make Tor an ideal tool for bypassing the blocking and surveillance of GFW [24]. In order to create a private network pathway with Tor, a client needs to build a circuit of relays (encrypted connections through proxy nodes) on the Tor network. The pathway is built incrementally, by adding one hop at a time, so each relay along the way knows only the two nodes that are one hop before and after it. A separate set of encryption keys is used for each hop along the circuit, except for the last hop to the destination server [25]. However, the global public list of relays is Tor's biggest weakness. Chinese censors download the lists and add each IP address to a blacklist. In response to the blocking of its relays, the operators of the Tor network began to reserve a portion of new relays as secret, non-public "bridges" [26].

3.3 Active probing

The operators in charge of Chinese censorship infrastructure continue to innovate methods to detect and block the circumvention methods. Because the encrypted traffic is more difficult to analyze, so that deep packet inspection might not be able to understand what is in the traffic and whether it should be blocked. Yet during deep packet inspection the operators can look at specific set up of TLS such as port number, type of encryption, handshake parameters or flow information, this information is usually not enough to be sure that this is something that needs to be blocked. In order to exclude uncertainty and collateral damage, and response to enhanced circumvention systems, the method called "Active probing" started being used by the censors of the GFW. This probing works by passively monitoring the network for suspicious traffic, then actively probing the corresponding servers, and blocking any that are determined to run circumvention servers such as Tor (Figure 4). Once the connection between Chinese server and a server in a foreign country is established, the Great Firewall initially closely looks at TLS connection handshake, and if it considers the connection suspicious, it next launches a probe that connects to the same server in that country and tries to speak the protocol of the connection they suspected (e.g. Tor). The foreign server will terminate the connection, if the guess of the GFW was not correct, but if the Firewall is right, the server will answer with a handshake, so in that case the GFW is sure that the connection is undesirable and can block it. This is a two stage inspection, where in the first stage deep packet inspection is done on a lot of traffic, and a portion of the traffic that is suspicions is selected; in the second stage, the active probing is used to understand what this portion of traffic really is. The system can detect the servers of at least five circumvention protocols and is upgraded regularly and operates in real time.

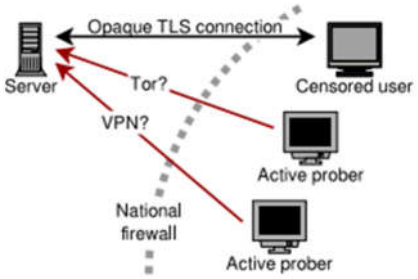


Figure 4. Simplified schema of Great Firewall's active probing

4 Great Cannon

In March 2015, two services designed to circumvent Chinese censorship - GreatFire.org and two GitHub pages run by GreatFire.org – were stroke by a Distributed Denial of Service (DDoS) attack with 2.6 billion requests per hour sent (at peak) [21][19]. The implemented mechanism allowed the attackers to manipulate a part of the legitimate traffic from inside and outside China to launch and steer Denial of Service attacks against the anti censorship project [20]. It was later reported that the source of the attack was a malicious Javascript returned by Baidu servers. This recent event showed that the Golden Shield Project has evolved from just blocking foreign content from coming into the country to attacking foreign websites. The offensive system is called “Great Cannon” (GC), and considered separate from the Great Firewall, with different design and capabilities. This distinct attack tool hijacks traffic to (or presumably from) individual IP addresses and can randomly replace unencrypted content as a man-in-the-middle. The Great Cannon is known to use traffic of systems outside of China by infecting the users’ browsers with malicious programs to create a massive DDoS attack. Observations show that the design of the Great Cannon is not well-suited for traffic censorship, compared to mechanisms used by the Great Firewall. That is, it cannot censor any traffic not already censorable by the GFW. This indicates that that the role of the GC is to inject traffic under specific targeted circumstances, not to censor traffic. However, there are some mutual features that the Great Cannon and the Great Firewall have, such as the same specific TTL side-channel, and that they might share some common code (Figure 3). Great Cannon acts on traffic on the same link as the Great Firewall, which is the evidence that the GC appears to be co-located with the GFW. However, the content analysis of the GC is more primitive and easily manipulated, but offers big performance advantages as it does not need to deal with complex state concerning connection status and packets reassembly, as GFW does. The Great Cannon discovers the target’s IP address and identify a suitable exploit. When the GC decides to inject a reply, unlike the GFW, it only examines the first data packet of a connection. It uses a flow cache (with capacity up to 16,000 entries for a single sending IP address) to remember recent connections it has estimated no longer requiring examination. The GC is then tasked to intercept traffic from the target’s IP address, and replace certain responses with malicious content. Figure 4 shows the decision flow of the Great Cannon. Any user who has ever made a single request to a server inside China not employing encryption is a potential target for GC’s malicious code. The users of some websites that are located outside of China but use some sources from Chinese servers would not even realize that their computers were communicating with Chinese servers and were a target for attacks. The Great Cannon is noticed to have similar capabilities as the NSA’s QUANTUM system. The DDoS attacks launched by the GC so far are aligned with political concerns of the Chinese government. The attacked websites, GreatFire and GitHub, provided services, like proxies, and technologies for users to circumvent Chinese government censorship [19].

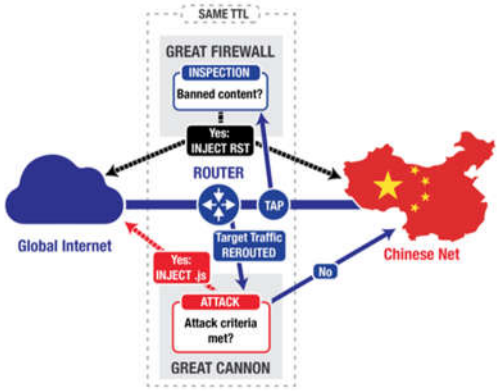


Figure 5. Simplified logical topology of the Great Cannon and Great Firewall

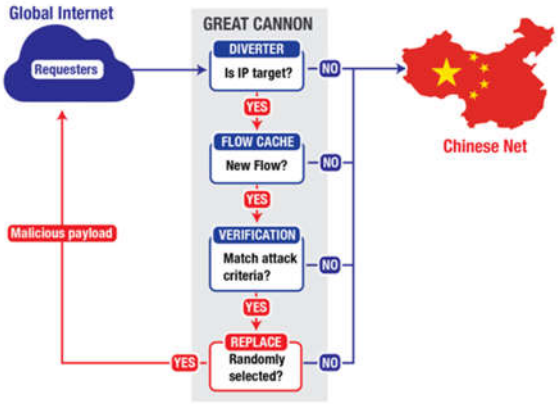


Figure 6. The Great Cannon's decision flow [19]

The Great Cannon is a big shift in tactics of the political implication of Chinese government. The reasons for deploying the GC are not mentioned explicitly. However, analyzing the attack to GreatFire website, we can state that the Chinese government's aims were both to try blocking the operations of an undesirable resource and to show other organizations that the outcomes can be costly. Yet, we do not know the full power of the Great Cannon, thus the way China decides to use this tool is not know the full power of the Great Cannon, thus the way China decides to use this tool is unpredictable and probably future attacks can reach the entire country level. What is seen from already implemented attacks should be a notice to the countries with not advanced cyber security mechanisms to take serious actions towards improving their situation in cyberspace.

Societies facing lot of challenges due to governmental limitations and protection based restrictions. The strict regulations lead distrust in the public against government services and virtualization become necessary. However some countries exaggerated the meaning of security and public safety through censorship policy [25-26].

The researchers focused on developing variety of different technologies in order to enhance secure communication environments [27-33]. The security proposals targeted to reach maximum security without leading and collision and censorship during providing secure communication environment for public. Both organizations and governments spend effort on spreading and deploying these emerging technologies to propose a secure environment and protect user/customer data [34-40].

Providing countrywide security is a serious issue that requires considering lightweight communication infrastructure, scalability and flexible fault tolerance systems. The existing mechanism that was deployed within China focused on censoring by detecting anomalies on the network in existing communication infrastructure through restriction policies [35-46]. The existing technologies focused on enhancing supremacy of the government on public and nations through modifications and restrictions of current communication infrastructure.

As described above, blockchains have the potential to revolutionize the world of technology and communication. At the very least, it is very likely to disrupt the financial industry and turn it on its head. The technology also has the potential to disrupt other markets such as the entertainment industry, the energy industry and even electoral processes. The group of researchers has described as how the blockchain can cause disintermediation in the entertainment industry [31]. Essentially, artists would be

able to earn more because they would be able to sell their content directly to consumers using smart contracts. The various levels of middlemen would be eliminated and artists would be able to regulate content consumption and sale via smart contracts; programmable bits on a blockchain. In the energy sector, a scenario is described where independent generators of energy via renewable sources such as solar, are selling energy to one another via blockchains [30]. The large utility firms across the world are taking note of the trend and quite a few in countries such as Austria and Germany have started experimenting with blockchain technology. A comparison of the applications of blockchain technology in the financial services, entertainment and utilities industries generates a clear theme: disintermediation. The decentralized, distributed, transparent, programmable and anonymous nature of the blockchain is a death knell for middlemen. Smart and proactive companies are taking note and embracing the technology in a bid to remain relevant with time.

5 Conclusion

Since the beginning of the Golden Shield Project in 1998, there have been many improvements made in both censorship mechanisms and attack tools. Implementation of censorship mechanisms under the Golden Shield Project has both advantages and disadvantages and can be considered from a few perspectives: the Chinese government, businesses, and regular users (both within Chinese borders and outside of China). The Golden Shield Project is implemented from the approval of the Chinese government; consequently, its design was done in the way to benefit the government at the first place. So, having such a powerful mechanism for censorship as the Great Firewall and an attack tool as the Great Cannon, gives China great political, social and economic advantages against other nations. They control the information flow to the country, that is, the population is educated and aware of the countries and the world's concerns and problems, in the way which is preferable to the government. Because China has their own search engines, social networks, mail services, they have access to any private information of user of the Chinese Internet, what gives them an opportunity to control the population and use them as a resource for operations in cyberspace against foreign businesses or countries. The disadvantage of having such strict censorship is the dissatisfaction of the population whose human rights and freedom of speech are violated. For businesses in China, a big advantage is they are protected from western influences and businesses, where it would be more difficult to compete and achieve success. Censorship is disadvantageous for international businesses, as it makes the communication with outside countries more difficult, as for reaching out potential consumers, supplies or services, thus it decreases profit the companies could have made. Advantages of the censorship for the users of the Chinese Internet include: safer environment by blocking offensive material available on racist and pornographic websites and reduction of internet crime. The major disadvantage is an obvious violation of human rights. It prevents people from sharing their opinion, especially on topics such as religion and politics. The users of foreign countries are affected by collateral damage caused by implementation of the Great Firewall's censorship mechanisms.

REFERENCES

[1] Mizokami, K., (November 9, 2014). The 5 Most Powerful Armies on Planet Earth. Retrieved from http://nationalinterest.org/feature/the-5-most-powerful-armies-planet-earth-11632?page=show

[2] Hagestad, W. T. (2012). 21st Century Chinese Cyberwarfare : An Examination of the Chinese Cyberthreat From Fundamentals of Communist Policy Regarding Information Warfare Through the Broad Range of Military, Civilian and Commercially Supported Cyberattack Threat Vectors. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing.

[3] Evolution of Internet in China. (January 1, 2001). Retrieved from http://www.edu.cn/introduction_1378/20060323/t20060323_4285.shtml

[4] The Golden Shield Project. Retrieved from: http://gutenberg.us/articles/golden_shield_project

[5] Ensafi, R., Winter P., Mueen A., and Crandall R. A. (2015). Analyzing the Great Firewall of China Over Space and Time. Proceedings on Privacy Enhancing Technologies. Volume (1), pp. 61–76

[6] Carson, B. (July 23, 2015).9 incredibly popular websites that are still blocked in China. Retrieved from http://www.businessinsider.com/websites-blocked-in-china-2015-7/#google-including-gmail-1 An Analysis of China's "Great Cannon".

[7] Khattak, S., Javed, M., Anderson, P.D., Paxson, V. (2013) Towards Illuminating a Censorship Monitor's Model to Facilitate Evasion. Retrieved from https://www.usenix.org/conference/foci13/workshop-program/presentation/Khattak

[8] Anonymous. Towards a Comprehensive Picture of the Great Firewall's DNS Censorship. In 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14) (San Diego, CA, Aug. 2014), USENIX Association.

[9] Fan, L. (December 12, 2012). Understanding and Circumventing The Great Firewall of China. Retrieved from http://www.cs.tufts.edu/comp/116/archive/fall2015/lfan.pdf

[10] Anderson, D., (November 30, 2012). Splinternet Behind the Great Firewall of China. Retrieved from http://queue.acm.org/detail.cfm?id=2405036

[11] Farnan, O., Darer, A., Wright, J. (October 24, 2016). Poisoning the Well: Exploring the Great Firewall's Poisoned DNS Responses. Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Socie. Vienna, Austria

[12] Xu, X., Mao Z. M., and Halderman A. J (2011).Internet Censorship in China: Where Does the Filtering Occur? Retrieved from http://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf

[13] G. Lowe, P. Winters, and M. L. Marcus. The great DNS wall of China. MS, New York University. Accessed December, 21, 2007.

[14] Anonymous (2012). The Collateral Damage of Internet Censorship by DNS Injection. ACM SIGCOMM Computer Communication Review. Volume 42, Number 3

[15] Clayton, R., Murdoch, S., Watson, R.: Ignoring the Great Firewall of China. In: Danezis, G., Golle, P. (eds.) PET 2006. LNCS, vol. 4258, pp. 20–35. Springer, Heidelberg (2006)

[16] Xu, Y. (March 8, 2016) Deconstructing the Great Firewall of China. Retrieved from https://blog.thousandeyes.com/deconstructing-great-firewall-china/

[17] Verkamp, J.P. and Gupt, M, (2012). Inferring Mechanics of Web Censorship Around the World. Retrieved from https://www.usenix.org/conference/foci12/workshop-program/presentation/Verkamp [19] Marczak, B., Weaver, N., Dalek, J. (April 10, 2015). China's Great Cannon. Retrieved from https://citizenlab.org/2015/04/chinas-great-cannon/

[18] Using Baidu 百度 to steer millions of computers to launch denial of service attacks, (March 25, 2015). Retrieved from https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1

[19] Xu, Y. (March 14, 2016). The Emergence of China's New Weapon: the Great Cannon. Retrieved from https://blog.thousandeyes.com/chinas-new-weapon-great-cannon/

[20] [Lee, M. (January 25, 2016). China's Nearly 700 Million Internet Users Are Hot For Online Finance. Retrieved from http://www.forbes.com/sites/melanieleest/2016/01/25/chinas-nearly-700-million-internet-users-are-hot-for-online-finance/#100192b01391

[21] The Chian Great War, http://edition.cnn.com/2015/10/25/asia/china-war-internet-great-firewall/

[22] Xu, Y. (May 11, 2016). The Ongoing War Between China's Great Firewall and Circumvention Tools Retrieved from https://blog.thousandeyes.com/the-war-between-chinas-great-firewall-and-circumvention-tools/

[23] Tor: Overview. Retrieved from https://www.torproject.org/about/overview

[24] Ensafi, R., Winter P., Mueen A., and Crandall R. A. (2015). Examining How the Great Firewall Discovers Hidden Circumvention Servers. Proceedings of the 2015 ACM Conference on Internet Measurement Conference

[25] Sari, A. (2016); "E-Government Attempts in Small Island Developing States: The Rate of Corruption with Virtualization", Science and Engineering Ethcis, Springer , pp.XX. ISSN-O: 1353-3452, DOI: 10.1007/s11948-016-9848-0.

[26] Sari, A., Akkaya, M., Abdalla B., (2017) "Assessing e-Government systems success in Jordan (e-JC): A validation of TAM and IS Success model". International Journal of Computer Science and Information Security, Vol.15, No.2, pp.277-304, ISSN:1947-5500.

[27] Alzubi, A., Sari, A., (2016) "Deployment of Elliptic Curve Cryptography (ECC) to Enhance Message Integrity in Wireless Body Area Network". International Journal of Computer Science and Information Security, Vol.14, No.11, pp.1146-1153, ISSN:1947-5500.

[28] Alzubi, A. and Sari, A. (2016) Deployment of Hash Function to Enhance Message Integrity in Wireless Body Area Network (WBAN). Int. J. Communications, Network and System Sciences, Vol.9,No.12, pp. 613-621. http://dx.doi.org/10.4236/ijcns.2016.912047

[29] Sari, A., Rahnama, B., Eweoya, I., Agdelen, Z. (2016) Energizing the Advanced Encryption Standard (AES) for Better Performance. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp.992-1000, ISSN 2229-5518.

[30] Rahnama, B., Sari, A., & Ghafour, M. Y. (2016). Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation. In D. G., M. Singh, & M. Jayanthi (Eds.)

Network Security Attacks and Countermeasures (pp. 270-312). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8761-5.ch012

[31] Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks. Int. J. Communications, Network and System Sciences, Vol.8, No.13, pp. 567-577. Doi: http://dx.doi.org/10.4236/ijcns.2015.813051.

[32] Sari, A. and Karay, M. (2015) Comparative Analysis of Wireless Security Protocols: WEP vs WPA. International Journal of Communications, Network and System Sciences, Vol. 8, No.12, pp. 483-491. doi: http://10.4236/ijcns.2015.812043.

[33] Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Net-works (VANET). Int. J. Communications, Network and System Sciences, Vol. 8, No.13, pp. 552-566. http://dx.doi.org/10.4236/ijcns.2015.813050 .

[34] Cambazoglu, Ş. and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. Int. J. Communications, Network and System Sciences, Vol.8, No.13, pp. 533-542. http://dx.doi.org/10.4236/ijcns.2015.813048.

[35] Kirencigil, B.Z., Yilmaz, O., Sari, A., (2016) Unified 3-tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 1001-1011, ISSN 2229-5518.

[36] Sari, A. (2015) "Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite". International Journal of Communications", Network and System Sciences, Vol.8, No.3, pp. 29-42. doi: http://dx.doi.org/10.4236/ijcns.2015.83004.

[37] Yilmaz, O., Kirencigil, B.Z., Sari, A., (2016) VAN Based theoretical EDI Framework to enhance organizational data security for B2B transactions and comparison of B2B cryptographic application models.International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 1012-1020, ISSN 2229-5518.

[38] Sari, A., (2015), "Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks", New Threats and Countermeasures in Digital Crime and Cyber Terrorism, (pp. 66-94). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7. April 2015.

[39] Sari, A. (2015) "Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks". International Journal of Communications, Network and System Sciences, Vol. 8, No.3, pp. 19-28. doi: http://dx.doi.org/10.4236/ijcns.2015.83003.

[40] Sari, A. and Akkaya, M. (2015) Fault Tolerance Mechanisms in Distributed Systems. International Journal of Communications, Network and System Sciences, Vol.8, No.12, pp. 471-482. doi: http://10.4236/ijcns.2015.812042.

[41] Sari, A. (2015) "A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. Journal of Information Security", Vol.6, No.2, pp. 142-154. doi: http://dx.doi.org/10.4236/jis.2015.62015.

[42] Sari, A. (2014); “Security Approaches in IEEE 802.11 MANET – Performance Evaluation of USM and RAS”, International Journal of Communications, Network, and System Sciences, Vol.7, No.9, pp. 365-372, ISSN: 1913-3723; ISSN-P: 1913-3715, DOI: http://dx.doi.org/10.4236/ijcns.2014.79038.

[43] Rahnama, B.; Sari, A.; Makvandi, R., "Countering PCIe Gen. 3 data transfer rate imperfection using serial data interconnect," Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013 International Conference on , vol., no., pp.579,582, 9-11 May 2013 doi: http://doi.acm.org/10.1109/TAEECE.2013.6557339.

[44] Sari, A.; Rahnama, B., (2013) "Simulation of 802.11 Physical Layer Attacks in MANET," Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on , vol., no., pp.334,337, 5-7 June 2013, http://dx.doi.org/10.1109/CICSYN.2013.79 .

[45] Sari, A., Rahnama, B (2013). “Addressing security challenges in WiMAX environment”. In Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13). ACM, New York, NY, USA, 454-456. DOI=10.1145/2523514.2523586 http://doi.acm.org/10.1145/2523514.2523586

[46] Sari, A. (2014); “Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks”, Transactions on Networks & Communications, Society for Science and Education, United Kingdom, Vol.2, No.5, pp. 1-6, ISSN: 2054-7420, DOI: http://dx.doi.org/10.14738/tnc.25.431.

