Cyber Space: Cyber War or Cyber Space Peace Treaties

Hasan L. Al-Saedy
British Institute of Technology and E-Commerce
258-266 Romford Road, London E7 9HZ, UK
Email: hasan {at} bite.ac.uk

***Abstract*— In this research paper the author investigates the major significant development of the cyber space and related technologies. Main security threats to cyber space security are also discussed. Significant amendments to the security of cyber space are highlighted. The national necessary preparation for cyber war is demonstrated. Also the advantages of having cyber space peace treaties over the cyber war option are discussed.**

***Keywords*- (*Cyber Space, Cyber Security, Privacy, Cyber War and international Security*)**

I. INTRODUCTION

E-Commerce, E-Government and E-Bank are significant achievements of the twenty and twenty first centuries. The easy access to communications media gave significant advantages for the new millennium citizen compared with the available facilities available during the nineteenth century. The economy and everyday live ,now days, are independent on the posted letters, paper application forms and alike. The cyber space becomes mature enough to accommodate all types of transactions processing and handling procedures. However, the main limitation of the cyber space is the security and privacy problem in general and the identification and verification problem in particular. In spite of the fact that the need for the identification and verification mechanism in commercial transaction processing were used by societies for more than thirty centuries, the identification and verification today is a significant defect of the cyber space. On one hand people in Babylon used fingerprints biometric to sign their identity on clay on the other hand a major defect of the recently developed internet is the identification and verification. TCP/IP protocols accept the initiation of communications without identification and verification [1]. This defect in designing of the internet subjected the communicated data to significant threats and attacks. The internet is not the exception; other elements of the cyber space were designed with the same defect.

In the following sections, the author discusses the major development in cyber space technology; defects of cyber space, security threats, recent media reported privacy violation cases, preparation for the cyber war, and the alternative to cyber war.

II. MAJOR ACHIEVEMENTS IN CYBER SPACE TECHNOLOGY

Historical references indicate that the basic concepts and idea of telephone were around as early as 1832, however, the invention of the first practical telephone is credited to Alexander Graham Bell (March 3 1847 – August 2 1922). The development of the telephone communications had a significant impact on the performance of the world economy in general and the stock exchange in particular. It gave the facility to the stock exchange dealer and investor to trade from a distance [2].

Another significant achievement is the development of telegraph communications system and Morse Code in particular in 1836 [4]. The telegram system used the same communication lines used in telephone with a major advantage that as an individual you do not need to be the owner of the telephone line to use the telegraph; in fact you buy your share of time from the post office. The amount of money you pay is very much dependent on the number of words in your telegram. In Morse code, the early concepts of information theory were introduced. A high frequency character in language was assigned the shortest code; the low frequency character in language was assigned the longest code. This is to say that Morse code maximize the amount of information and minimise the size of the code.

To facilitate the communications system worldwide and to establish a wired communication the submarine communications cable is established in 1850[5]. Another significant achievement was the establishing of the radio wireless transmission in 1918 [7].

The first electronics encrypted system was developed by Gilbert Vernam in 1918[6]. This is the development of stream cipher encryption system or what is called the one time pad.

The German encryption mechanical electronics encryption machine is Enigma. Enigma was developed in 1920 and used by the German army during the Second World War. The cryptanalyses of Enigma was credited to Allan Turing [7].

Claude Shannon developed the concept of information theory and coding system in 1950, In fact Shannon code theory was the generalization of the coding concepts used in Morse code [8]

A significant achievement was the development of the electronic computer during and after the Second World War. Universities in Swiss land, the United Kingdom and United

States developed a university research computer. Low cost military electronic scarab offered in Tottenham court road electronic shops in London was used to develop the first generation research computer. However, the first commercially available first generation computer was made available in 1951 is Univac 1 [9].

A major breakthrough in developing the high level language occurred in 1955. This is the breakthrough of parsing the mathematical expression and the development of FORTRAN language [9]

Another achievement in communication was the development of the cell phone in 1960 and the development of the Satellite communication systems [10].

The first military network came to existence was the ARPANET 1963. This network is expanded to US universities in 1969 and to be the current internet in 1970 [11].

The IBM computer company developed the Data Encryption Standard (DES) in 1970, DES was the first block cipher symmetric algorithm[11]. The Global Positioning System (GPS) is developed in 1973 [12].

A major achievement happened in the middle of 1975, this is the development of the large scale interaction and utilizing this in developing the third generation computers and Personal Computer. Third generation computers consume less power and generate less heat compared with the first and second generation computers [13].

The Open System Interconnection Networking developed as a European network in 1977. Open System Interconnection network is a seven layer network.

Key management and distribution was a major problem before 1977. The development of public key encryption in Massachusetts Institute of Technology was another significant achievement in cryptography and data security[11].

Another significant achievement was the development of the World Wide Web by Sir Tim Berners-Lee (Web Technology) 1989 and the development of web commerce and social network applications [14]

Figure 1 shows that the major achievements were developed over 200 years, 70 percent of the significant achievements occurred between 1950 and 2000.

III. MAJOR PROBLEMS IN CYBER SPACE SECURITY

A major problem in internet security is the problem of identification and verification. In spite of the fact that the use of identification and verification technique being used by the legal institutions for centuries. The internet was designed without taking in consideration the requirement of identification and verification. The main protocols used in TCP/IP lack security measure of identification and verification. An example is the three handshake protocol and Address resolution protocol. The lack of security in the two protocols was the reason behind the majority of successful network attacks. The diagram of the three handshake protocol is given below.

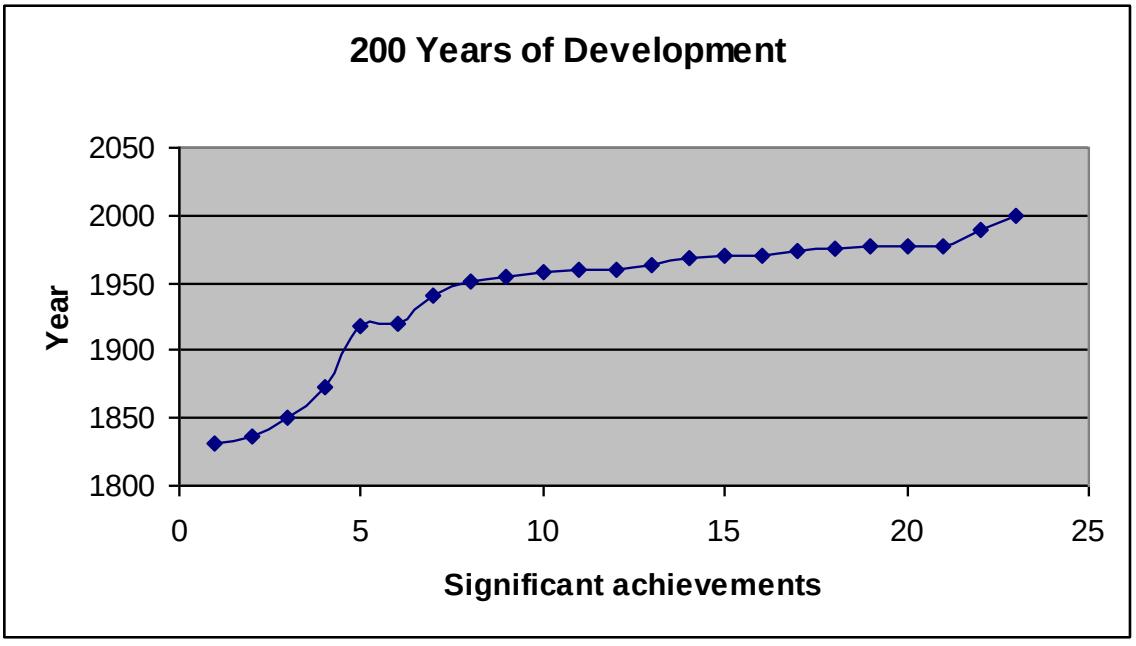

Figure 1: 200 Years of Cyber Space Developments

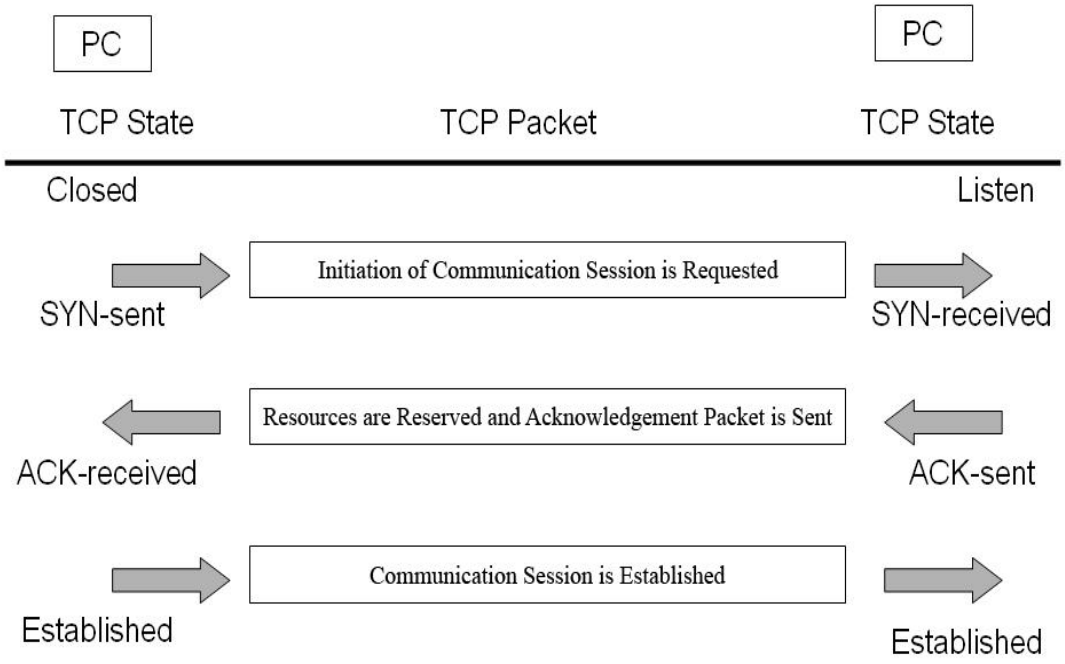

Figure 2: TCP/IP Three Hand Shake Protocol

The mobile phone is a necessity now days and used by everybody, the mobile security is not an exceptional case. Interception software is commercially available and internet down loadable. The features available in this software are interception of live calls, short messages (SMS) and social network application. Also, it retrieves pictures, videos, audios and contacts.

It is important to give a comparison at this stage between network traffic interception and cell phone live calls and short messages traffic.

Media Access Control (MAC) card view all LAN traffic and pass on to the client only the Packets addressed to the client's IP address. Subscriber Identification Module (SIM) card view all the live calls, short messages within the cell and trigger the cell phone for only calls and messages address to its cell phone.

The widely used GSM communication system is designed with security and privacy problems. The algorithms are used. These are A3, A5 and A8.

A3 is the authentication algorithm; cell phone authenticates itself to Mobile Station. Algorithm A8 is the key generation algorithm. It generates 64 bits as the encryption key.

Algorithm A5 is a stream cipher algorithm. Three Linear Feedback Shift Registers (LFSR) are used in the algorithm. Lengths of shift registers are 19, 22, and 23. The complexity of the algorithm is 2^{64}. The last 10 bits of the key is set to 0s. This reduced the complexity of the brute force attack to 2^{54}. Recently reported dived and conquer attack was 2^{40} [15].

IV. SECURITY THREATS MITIGATION

Three major techniques were developed during the last twenty years to reduce the risk of security threat mitigation, these are the TSL/SSL, Pretty Good privacy and the zero knowledge protocol calculator.

TSL/SSL was developed in 1993 by Netscape. Four types of algorithms were deployed in TSL/SSL; they are the Public Key Encryption, Block Cipher Encryption, Compression / Decompress and Error Detection Algorithm.

Pretty Good Privacy was developed by Phil Zimmermann in 1991. It addresses the problem of identification and verification by deploying the Public Key Algorithm [11].

The most recent development is the zero knowledge protocol calculators. The use of the calculator will reduce the number of phishing attack drastically on bank accounts. It is expected to save huge amount of money by preventing phishing type of attacks.

V. SIGNIFICANT MEDIA REPORTED VIOLATION CASES

Media often reports security and privacy violation on cyber space. However, significant attacks reported during the last five years are the Wikileak, cyber attack on the Iranian atomic

energy project, the Iranian attack on the US financial enterprises, the US attack on the French president's residence, the allegation about the wiretapping of the telephone communication of the German Head of State, the US violation of citizen privacy and Mandiant Intelligence Report:

Wikileak
International diplomatic emails are regularly intercepted by the United State Security Agencies, Intercepted emails regularly save on a computer system. Bradley Manning is a US army officer, Bradley Manning leaked emails to Mr Julian Assange, and Julian Assange published the leaked emails on the Wikileak web site.[16]

Cyber Attack on the Iranian Atomic Energy Project
The Siemens industrial controller devices are used to control the spinning of the centrifuge spinner used to enrich the uranium in Iran atomic energy project.
Stuxnet is a worm developed jointly by the US and Israel viral experts. Stuxnet modifies the control program of the spinners to destruct them. [17]
Flame malware also known as skywiper, it attacks Microsoft Windows operating Systems, it was deployed in the middle east. MAHER the Iranian centre of Computer Emergency Response Team discovered Flame in 2010.[18].

Iranian attacks on the US financial enterprises
Iranian denial of service attacks on the US financial enterprises were reported by Wall Street media. Wall Street media admitted that the Iranians are a viable cyber enemy of the US. The size of damage inflection is not reported yet by Wall Street media.[19]

US attack on the French president's residence
Credible French media reported a cyber attack on the French President's Residence during the last French election.[20].

Wiretapping of the telephone communication of the German Head of State
A wide spread allegation about the wiretapping of telephone communication of the German head of state Angela Merkel is reported. The US president Barak Obama was aware of the incident. [20].

US violation of citizens' privacy
Edward Snowden is a young computer science graduate formerly worked with the Central Intelligence Agency and the National Security Agency. Mr Snowden disclosed classified documents to the media. Disclosed documents show that US security agencies violate the privacy of US citizens on regular bases. [21]

Mandiant Intelligence Report
A group of Chinese hackers who are part of the Chinese military have been conducting attacks on American interests over the last seven years. [22].

Dishfire
Dishfire is a national Security Agency database; data is collected and analyzed for extracting intelligence information. Sources of the collection are SMS messages, GPS rooming, financial transactions and missed calls.[23]

VI. PREPERATION FOR CYBER WAR

A year length of practical training of average C programmers is sufficient enough preparation. The Programme covers the following:

- TCP/IP programming
- Web Programming
- Communications interception and analyses tools.
- Detection of Cyber Attacks
- Engineering of Cyber Attacks
- Capturing and Analyses of Cyber Viruses
- Engineering of Cyber Viruses

VII. CYBER SPACE TREATIES AS ALTERNATIVE

The US government is the biggest investor in cyber space, the economy of the US is very much dependent of the utilization on the cyber space commercially this is on one hand; on the other hand developing a national security team is within the budget of any country. The nearest history shows that a country with a reasonable average financial resource could be a rival to a nation like the US and could inflict a high financial damage on the US economy. China is the technological emerging power and attacking of the US economy is within its technical capabilities. Therefore, it is in the interest of the US government to come to terms with other nations like Iran and China. Therefore, cyber space treaties are viable action. This is also the opinion of a top US security technology expert [24].

VIII. DISCUSSION AND CONCLUSIONS

Figure 1 shows that the major achievements were developed over 200 years, 70 percent of the significant achievements occurred between 1950 and 2000. A major defect in cyber space is the security and privacy problem. Leading nations like US and Chine take the advantage of the weak security and privacy of the cyber space, more nations will join, like Israel, Nigeria and Iran. Investing in cyber war is within the budget of nations like Iran in the Middle East and Cuba in Latin America. It is in the interest of a country with big investment in cyber space like US to come to terms with developing nations like Iran, China and Cuba.

REFERENCES

1. Snader J. C.,(1994) Effective TCP/IP Programming, Addison –Wesley.
2. Coe, Lewis(1995), The Telephone and Its Several Inventors: A History, Jefferson, North Carolina, McFarland & Co., Inc. ISBN:07864-0139-9.

3. Pesonen, L. (1999) GSM Interception, http://www.tml.tkk.fi/Opinnot/Tik-110.501/1999/papers/gsminterception/netsec.html
4. Burns, R. W.(2004), Communications: An International History of the Formative Years, Institute of Electrical Engineering, ISBN: 0-86341327-7.
5. Headrick, D.R., & Griset, P. (2001). Submarine telegraph cables: business and politics, 1838-1939. The Business History Review, 75(3), 543-578.
6. Thomas Beth and Fred Piper(1984), The Stop-and-Go Generator. EUROCRYPT.
7. Sungook Hong(2001), Wireless: From Marconi's Black-box to the Audion, MIT Press. Bauer, F. L. (2000). Decrypted Secrets (2 ed.). Springer. ISBN 3-540-66871-3.
8. Shannon, C. E. (1948): A Mathematical Theory of Communication, Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656.
9. Goldstine, H. H. (1972). The Computer: from Pascal to von Neumann. Princeton, New Jersey: Princeton University Press. ISBN 0-691-02367-0.
10. Gordon A. G., Richard K. S. (2006) Mobile and Wireless Communications: An Introduction, McGraw-Hill International, ISBN 0-335-21761-3.
11. Stalling W.(2011), Cryptography and Network Security, Fifth Edition , Pearson.Hoffman-Wellenhof, B., H. Lichtenegger and J. (2001) Collins.Global positioning system: theory and practice. New York, Springer-Verlag.
12. Hoffman-Wellenhof B, Herbert Lichtenegger, James Collines, Global Positioning System: Theory and Practice, Springer- Verlag(1997).
13. Freiberger, Paul; Swaine, Michael (2000) Fire in the Valley: The Making of the Personal Computer (2nd edition ed.). New York: McGraw-Hill. ISBN 0-07-135892-7.
14. Tim Berners-Lee. (2010) "Frequently asked questions". World Wide Web Consortium. Retrieved.
15. Pesonen L., GSM interception, in http://www.di.unisa.it/professori/ads/corso-security/www/CORSO-9900/a5/Netsec/netsec.html
16. Channing, Joseph (2007). "Wikileaks Releases Secret Report on Military Equipment". The New York Sun. Archived from the original on 2012-05-26.
17. Langner, Ralph (2011). "Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon". TED. TED Conferences, LLC.
18. Lee, Dave (2012). "Flame: Massive Cyber-Attack Discovered, Researchers Say". BBC News.Archived from the original on 30 May 2012.
19. Sanger, David E. (2012). "Obama Order Sped Up Wave of Cyberattacks Against Iran". The New York Times.
20. The White House, Office of the Press Secretary(2013), "President Barack Obama's State of the Union Address," February 12, 2013;http://www.whitehouse.gov/the-press-office/2013/02/12/president-barack-obamas-state-union-address.
21. Dilanian, Ken.(2013) "A spy world reshaped by Edward Snowden". Los Angeles Times. December 22.
22. Gorman, Siobhan (2009). "Electricity Grid in U.S. Penetrated By Spies". The Wall Street Journal. Retrieved November 2, 2010.
23. Radnedge, Aidan (2014), "Did Uncle Sam use your iphone as a spyphone?, Metro , Friday, January 17, 2014.
24. Schneier B.(2012), Cyber War or Peace Treaties, https://www.schneier.com/blog/archives/2012/06/cyberwar_treati.html