EasyChair Preprint

№ 3952

Cybersecurity and National Security - a Brief History and Exploration of the Growing Political Concern for Country Resilience in Cyberspace

Tabitha Bilaniwskyj-Zarins

July 26, 2020

Cybersecurity and National Security
A Brief History and Exploration of the Growing Concern For Country Resilience in Cyberspace.

Tabitha Bilaniwskyj-Zarins

Abstract

This review of Cybersecurity and National Security includes a brief history of cyberspace and how it became a politicised reality. Several significant cyberattacks are identified including the Morris Worm and Stutnex, the first attempt at Cyberwarfare. An International approach convened by the Council of Europe was established to encourage a united approach to cyber safety. Discussion of central eastern Europe Militarisation of Cybersecurity concludes this review.

1 Introduction

This paper will discuss a brief history and explore the concept, development, and the reality of an unseen planet known as Cyberspace. A concept of countries laying stakes to their portions of the virtual landscape. Cyberspace started as a sci-fi novel story that becomes a reality which enables governments to attack in the realm of computer connectedness (Dunn Calvety 2005). Significant cyberattacks, such as the Morris Worm and Stutnex, created the need for an antivurus protection industry (Orman 2003). Advanced Artificial Intelligence (AI) is now at the forefront of cybersecurity (Li 2018). A new treaty by the Council of Europe was formed to tame the Cyberspace Frontier, challenging Governments to implement policy. Governments were tasked with assigning its Ministries to set policies for Cybersecurity (Council of Europe 2020). A brief span around the globe, paying attention to central eastern and eastern Europe, will highlight the countries that have greater reliance on cybersecurity for securing classified and personal intelligence. The greater the wealth of economies, the more complex a nation's system, the greater the need for a higher authority of policy development for Cybersecurity (Dunn Calvety 2005).

2 A Brief History of Cyberspace

Nearly forty years ago the first imagined concept of cyberspace was by William Gibson in his science fiction novel 'Neuromancer'. (Dunn Calvety 2005) The Guardian newspaper article on William Gibson describes Gibson's Cyberspace being a "consensual hallucination created by millions of connected computers" (Cumming 2014). The story continues with a character known as 'Case' who plays the role of a junkie hacker, that manages to "jack" into this futuristic system of a major corporation. (Dunn Calvety 2005) The first concept of cyberspace was born.

In 1990 the concept of cyberspace was politicised by John Perry Barlow, a political activist, who adopted the phrase 'cyberspace' for his foundation the "Electronic Frontier Foundation (EFF) a non-profit organization for defending digital privacy, free speech and innovation" (Electronic Frontier Foundation n.d). He related the concept cyberspace as the new frontier, giving now the Internet as sense of place. (Dunn Calvety 2005) The EFF believed the Internet and World Wide Web (WWW) should be an unlegislated place. It is still an active organisation today. Cyberspace was now a political place.

3 The Developing Reality of Cyberspace and Cyberattack.

Sci-fi concepts continued to develop the unseen new world of Cyberspace, introducing biological words such as virus, worms and bugs. A trend developed by computer scientists (Dunn Calvety 2005)

The first attack on the internet was the Morris Worm created by Robert Tappan Morris, a graduate computer scientist, in 1988. (Dunn Calvety 2005) Computer security in 1988 was not even considered at that time and the Morris Worm was to change the landscape of how users, administrators, and researchers viewed the internet and its use. A need for internet security was born, and the new industries of firewalls and antivirus protection emerged as a result. (Orman 2003)

In 2001, the Council of Europe (COE) convened in Budapest for a convention on Cybercrime and to encourage many member states to sign a treaty. "The main objective was to pursue a common criminal policy aimed at the protection of society against cybercrime, adopting appropriate legislation and fostering international co-operation" (Council of Europe 2020).

In 2007 Estonia, the northern most Baltic country bordering with Russia, was cyberattacked continuously for three weeks by Russia in retaliation for the removal of a Soviet Era War Memorial in Tallinn; disabling Estonia's Parliament, Ministries, banks and media (Traynor 2007).

Fast track to 2010 to the first cyber warfare attack known as Stuxnet where malware became a weapon in Cyberspace (Dunn Calvety 2005). The Stutnex attack was a vastly different and significant malicious attack devised by the US and Israeli Governments to physically destroy a military target on Iranian Soil. (Langer 2011)

4 Cyberspace Frontier Lands need Smart Security.

The Oxford's Definition of Cybersecurity - "the state of being protected against the criminal or unauthorised use of electronic data or the measures taken to achieve this" (Lexico 2020). In some countries cybersecurity is still viewed as science fiction and the need for policy is of a civil concern, that is for business, banking, and internet service provider's responsibility to report cyberattacks to Government. Countries view this as a general risk. (Tumkevic 2016) There are various approaches to Cybersecurity, countries with a military approach to National Security are countries with advanced technologies storing large amounts of its population's data, security intelligence and highly classified data, and are therefore, requiring strong and secure, and impenetrable protective cyber infrastructure. (Tumkevic 2016).

Firewalls and traditional antivirus software, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) are not enough protection from Advanced Persistent Threats (APTs), like those against Estonia in 2007, by malicious technicians from rogue states. (Li 2018) Artificial Intelligent (AI) technology is becoming more important in combating APTs. Machine Learning (ML) AI needs to be programmed to detect threats. Advanced Deep Learning (DL) technology is becoming increasingly important in identifying and combating cyberthreats. (Li 2018)

5 Militarisation of Cyberspace

In 2008, Estonia was one of the first countries in the world to adopt a national cybersecurity strategy because of a persistent attack from Russia in 2007. Estonia established an Interagency between its Ministry of Defense (MOD) and Ministry of Economic Affairs and Communications; and the Cyber Security Council 2011. (Tumkevic 2016)

Latvia, another Baltic country, adopted the Cyber Security Strategy 2014-2018, based on cyber-attack incidents and for the likely increase in cybersecurity risks. This was an integrated approach between government and civil defense. Latvia has a National Information Technology Security Council which is responsible for National Cybersecurity Policies, coordinating policy development between the public and private sectors, and the Ministry of Defense sets the policies. Latvia is seen to be a leader in Cybersecurity policy development for the whole of Europe. (Tumkevic 2016)

Lithuania, the third state in the Baltic region has not approved a National Cybersecurity strategy, although has approved a National Security strategy. (Tumkevic 2016)

In Poland, Cybersecurity became an integral part of Poland's national security policies throughout many of its Ministries. (Tumkevic 2016)

Other countries following similar paths in adopting strong National Cybersecurity Policies include The Czech Republic, placing strong emphasis on prioritizing cybersecurity; and Slovakia and Hungary have National Cybersecurity Strategy's establishing Cybersecurity councils. (Tumkevic 2016)

Ukraine's Digital Agenda for 2020, in comparison, is compromised. The National Cybersecurity strategy is needed to combat

information leaks, intellectual property protection and corruption. (Digital Agenda for Ukraine 2020)

Interestingly, President Putin announced it has passed a new "Russian Internet Law to disconnect Russia from the world wide web". (Forbes 2020)

6 Conclusion

Cyberspace, as discussed within this paper, started as a concept born from a novel by William Gibson in 1984, followed by the politicisation of the concept by John Perry Barlow. The need for cybersecurity became a reality after the first known worm attack in cyberspace through the internet in 1988. New antivirus and firewall industries emerged as a result. Cyber war increased via the World Wide Web and so did the urgency to establish a unified international approach coordinated by the Council of Europe. After three weeks of continued cyber-attack on its banks, businesses and industries, Estonia developed the most comprehensive National Cybersecurity Policies within its Ministry of Defense. Throughout countries of central eastern and eastern Europe this paper highlights the reliance on cybersecurity for securing classified and personal intelligence. This paper identifies the greater the wealth of economies, and the more complex a nation's system, the greater the need for a higher authority of policy development for Cybersecurity and the role that Artificial Intelligence will inevitably have.

References

Dunn Cavelty, M From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, *International Studies Review*, Volume 15, Issue 1, March 2013, Pages 105–122, https://doi.org/10.1111/misr.12023

Langner, R, "Stuxnet: Dissecting a Cyberwarfare Weapon, in *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49-51, May-June 2011. https://ieeexplore.ieee.org/document/5772960

Li, J. Cyber security meets artificial intelligence: a survey. *Frontiers Inf Technol Electronic Eng* **19,** 1462–1474 (2018). https://doi.org/10.1631/FITEE.1800573 https://link.springer.com/article/10.1631%2FFITEE.1800573#citeas

Orman, H, "The Morris worm: a fifteen-year perspective, in *IEEE Security & Privacy*, vol. 1, no. 5, pp. 35-43, Sept.-Oct. 2003. https://ieeexplore.ieee.org/document/1236233/citations#citations

R. Sabillon, V. Cavaller, J. Cano and J. Serra-Ruiz, "Cybercriminals, cyberattacks and cybercrime," 2016 *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, 2016, pp. 1-9. https://ieeexplore.ieee.org/document/7740434

TumkevičA. (2017) "Cybersecurity in central eastern Europe: from identifying risks to countering threats", *Baltic Journal of Political Science*, 0(5), pp. 73-88. doi: 10.15388/BJPS.2016.5.10337. https://www.journals.vu.lt/BJPS/article/view/10337

Council of Europe 2020, *Convention on Cybercrime*, France, viewed 18 March 2020. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Cumming, E, 28 July 2014, Guardian News and Media Limited or its affiliated companies 2020, *William Gibson:the man who saw tomorrow*, Australia, viewed 18 March 2020. https://www.theguardian.com/books/2014/jul/28/william-gibson-neuromancer-cyberpunk-books

Doffman, Z, 1 May 2019, Forbes Media LCC 2020, *Putin signs 'Russian Internet Law' To Disconnect Russia from the World Wide Web,* viewed 18 March 2020. https://www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/#3bc7a4dc1bf1

Electronic Frontier Foundation n.d, USA, viewed 18 March 2020. https://www.eff.org/

Lexico.com 2020, viewed 16 March 2020. https://www.lexico.com/en/definition/cybersecurity

Minitch, L, 2020, *Digital Agenda for Ukraine,* Lviv, viewed 17 March 2020. http://www.e-ukraine.org.ua/media/Lviv_Minich_2.pdf

Traynor, I, 17 May 2007, Guardian News and Media Limited or its affiliated companies 2020, *Russia accused of unleashing cyberwar to disable Estonia*, Brussels, viewed 16 March 2020. https://www.theguardian.com/world/2007/may/17/topstories3.russia