VOLUME - 11, ISSUE - 04, APRIL - 2022 • PRINT ISSN No. 2277 - 8160 • DOI : 10.36106/gjra

Original Research Paper | Computer Science

CYBER AUTONOMY AND IT'S ROLE IN INDIA'S CYBER SECURITY

Sruthi Nair* Amity Institute of Defence and Strategic Studies, AUUP, India. *Corresponding Author

Oza Sakshi Ravi Amity Institute of Defence and Strategic Studies, AUUP, India.

ABSTRACT The globe has entered the era of hybrid wars and to be on the winning side, securing and protecting data remains a high priority for every nation. As hackers continue to explore and exploit, safeguarding systems and networks become even more difficult. Due to the pervasive deployment of cyber-physical systems and IOT devices, the need to defend the number and complexity of the systems increases rapidly. This is where cyber autonomy comes to our rescue. Cyber autonomy can help a system to identify attacks, patch vulnerabilities and if required, counterattack without the help of an IT specialist. Taking a cue from above, this paper aims to suggest multiple prospects cyber autonomy can bring to India's cyber security framework and its potential consequences, as digital India remains the aim of every Indian.

KEYWORDS : Cyber Autonomy, Cyber Security, India's Cyber Security Framework, Digital India

INTRODUCTION

India is a powerful developing country in South Asia and aspires to become a world leader. To make this dream a reality, India needs to develop in defense, economy, and technology. The Indian government has put forth various initiatives, such as Atmanirbhar Bharat, Make in India to help boost the country's economy and reach the $5 trillion economic milestones by 2025.

The government provides incentives and perks to investors and manufacturing companies to increase the country's production and become an exporter of defense-related products manufactured in the country. In the field of technology, the Indian government cooperates with IIT and IISC to bring newer technologies to society and promote innovation by young people. India lacks a well-structured cyber security framework to protect the government's confidential data as well as citizen's data.

After the Cold War, cyber security has become as important as military security. Today, it has accelerated and become more complex due to globalization and increasing reliance on information and communication technology. With the start towards digitalization, cyber security threat has also increased with all the information stored in computers and electronic devices, data remains most vulnerable to being exploited.

According to the world's leading security experts and analysts, the next war will be a battle for data. Today, data has become the most important asset possessed by any country/region. Countries such as America, China, Canada, Australia, Japan, Russia, Israel, and many more have well-structured cyber security policies and budgets to protect their network systems and confidential information from being exploited. India faces an important need to secure critical institutions such as satellites, power grids and thermal power plants from attacks. As per a report released by security software-maker Symantec, four out of ten attacks in 2014 were done on non-traditional service industries like business, hospitality, and personal. India must develop an effective cyber crisis management plan to deal with these challenges.

HISTORY OF INDIA'S CYBER SECURITY

Digital India, the globe's largest ICT initiative aims at transforming India into a digital country. However, in India the cyber security domain is neglected. Even though the computer and IT sector flourished in the country in the 1960s and '70s, India did not have a security plan to protect its newly established Information and communication industry. It was not until after the 1998 hacking of the BARC website by Pakistani hackers, Indian Prime Minister Atal B. Vajpayee decided to create a national task force for IT and software development. This was the first-time cyber security was mentioned as an objective in the Information and Communications (ICT) policy of India.

This very objective was used as a framework to create the Information Technology act of 2000 which extended security regulations of telegraph and telegram to the internet under the concept of cyber security. After the easy availability of the internet to the masses, cybercrimes and cyber-attacks were at an all-time high. In 2004, The Indian government established Computer Emergency Response Team CERT-IN, making it a single authority in-country to block individual websites as a countermeasure to threats. CERT-IN targeted websites that promoted violence and terrorism, pornography, hate speech, slandering, racism, and gambling.

After the 26/11 Mumbai attacks, where the internet and social media were found to have played a major role in the planning and execution of the attacks, the Indian government further decided to amend the IT act of 2002 which gave CERT-IN more power to execute cyber security functions such as collection and analysis of information on cyber incidents, emergency countermeasures against cyber-attacks, issuing of guidelines for prevention and reporting of cyber incidents and more.

With the continuous rise in the number of cyber-attacks in the country, the government decided to formulate a National Cyber security policy (NCP) in 2013 before this India had no policy which solely focused on the issues related to cyber security domain. The aim of NCP was to create robust cyberspace for its citizen, the government, and businesses with a strong vision for critical cyber infrastructure. Some of the key objectives of the policy were to create information assurance, protect national infrastructure, and build indigenous security technologies, and a large cyber security workforce by 2017.

After the NCP in 2013, National Critical Information Infrastructure Protection Centre (NCIIPC) was established in 2014 which was responsible to protect Indian cyberspace from cyber-attacks. Two agencies in India are working to counter both internal threats as well as external threats. In 2019, Cyber Swachhta Kendra was established under CERT-IN with the purpose of analyzing BOTs and malwares and to create awareness among the public regarding the importance of cyber security. Although the administration has taken few efforts, there has not been any major reform in India's cyber security policy which requires a comprehensive strategy to act against cybercrimes and cyber-attacks.

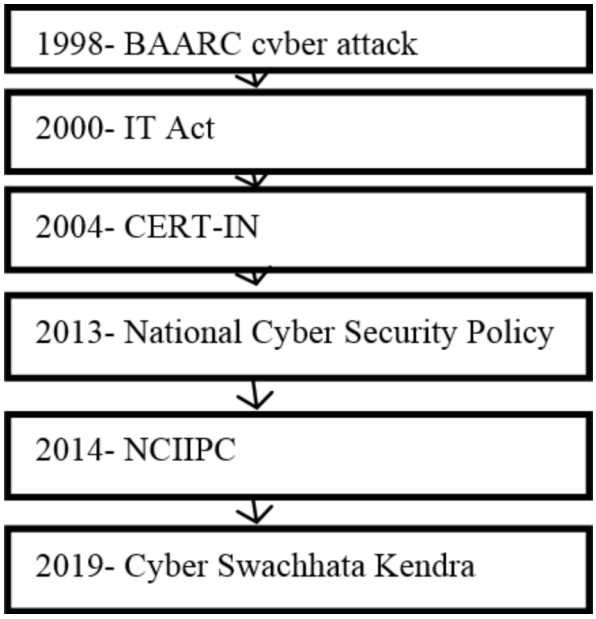

Fig.1. Flow Chart Of Cyber Reforms In India.

LITERATURE REVIEW AND GAP ANALYSIS

Cyber autonomy is a new topic and is highly experimental in terms of usage. Penetration testing and vulnerability assessment tools are the most used with implications in public and private industries. Ryan Ko in his paper published after the Cyber Grand Challenge has described in detail about automating cyber defense tools. The paper talks about the several gaps in the cyber security industry and about how cyber autonomy is the need of the hour. It proposes four steps through which complete autonomy can be achieved. But the paper neither proposes a plan to incorporate autonomy into national security nor does it mention how to go from phase 2 to phase 3. The paper by David Brumley talks about the future of Cyber Autonomy. It talks about various software and their vulnerabilities and the Cyber grand challenge. It goes into detail about mayhem, a tool that examines vulnerabilities. The paper goes into detail about the various rounds of the contest and how mayhem faced them all. But this paper also lacks the exact aspect of the self-adapting tools and merely proposes the scalability of these programs.

Analysts and security experts around the world have been reiterating the importance of a well-functioning and well-structured cyber security system. In the age of globalization and new technologies, with easy access to electronic devices, cyber-attacks are the main problem that should be taken care of without creating more problems.

Author Sushma Devi Parmar looks at the importance of cyber security from an Indian perspective. The paper studies the Indian cyber security fields related to energy, defense, finance, and telecommunications, and focuses on its vulnerabilities. Although the focus is on India's cyber security, the paper does not detail the future aspects of India's cyber security, nor does it make or suggest any decision-making recommendations to address existing security vulnerabilities. Similarly, the author Ramesh Subramanian has been concerned about cyber security before and after colonization in India and has studied the evolution of cyber security. In his analysis, the author confirmed that even after India became independent in 1947, it continued to abide by pre-colonial laws and failed to formulate and implement a comprehensive cyber security policy. The document is also dedicated to India's cyber security, without mentioning the future of cyber security, nor does it propose a method to formulate and implement a comprehensive cyber security policy.

CYBER AUTONOMY

The meaning of cyber autonomy lies in the term itself, autonomy of cyber field. The ability of security systems to become fully independent in terms of detecting and patching vulnerabilities is cyber autonomy. It entails detecting and locating new vulnerabilities, repairing those vulnerabilities and if need be, rewrite source codes to prevent and strengthen them. If a user despite not having any technical background is able to protect against cyber-attacks, therein lies the success of cyber autonomy.

We may be using a software with exploitable bug, but due to lack of technical knowledge, we may not know it. If we were able to make computer do what hacker do, we would need a hacker to discover and identify vulnerabilities. On a fundamental level, it involves enabling computers to take a software binary and independently find a security vulnerability in it. This is the future, one where computers can fix itself.

The basis of cyber autonomy involves software that can automatically discover vulnerabilities. It can also include tools that can repair itself and counterattack. The success of this technology lies in the fact that it can quickly explore the various options and decide the next step bereft of any human involvement. Now, there can be various difficulties that could arise with a technology like this especially during the execution phase. But the fact that this technology is cost effective and time saving holds a huge advantage over potential problems that might arise from its usage.

Now cyber autonomy does not mean complete removal of human involvement. It is only the availability of tools that combine the mind of man with the speed and execution skill of Artificial Intelligence.

To give a working example of cyber autonomy, we can look at a tool called Mayhem. It was built with a system that analysis software, based on formal analysis of a program, unlike fuzzing. Unlike humans, who can work only on source codes, this tool can work on binary codes, which eliminates the creator of the code being analyzed. When the tool detects a vulnerability, it starts generating a working exploit, like a hacker would do, but the tool does it with greater efficiency within a lesser time frame. Now to patch these vulnerabilities data flow analysis was used to understand the said code followed by hardening the binary and finally patching the discovered vulnerabilities.

According to Ryan Ko of University of Queensland there are four levels to achieving cyber autonomy. The first level is Data Fusion, followed by Cyber Security workflow Automation, followed by Operational Cyber Autonomy and finally Strategic Cyber Autonomy. What this essentially means is that, from the first level to the fourth level, there is a transition from reactive to proactive software along with the increasing autonomy. This is the future.

CYBER AUTONOMY IN INDIA

We face several challenges in the cyber security field in India and it will probably increase in the age of IOT. Weak devices will provide entry points for attackers.

Cyberspace is widely used in India. However, we rely heavily on the capabilities of antivirus software and tools to ensure our safety. But they are not fully able to detect and prevent vulnerabilities. So, India must work harder to safeguard itself in the cyber space. In the era of intelligent malware, we require appropriate intelligent malware detection system. It has become a necessity for us to use technologies that combine the power of machine learning with AI. These will have the ability to defend our systems with minimal effort and cost.

Hence investing in such software is essential. India also needs to rectify its lack of spending in cyber-R&D. If we can encourage and boost research and find solutions, then our dependence on transfer of technology would decrease making us an overall powerful nation digitally. India must promote both the basic research and the application of these research results by essentially converting them to practical problems. If government and institutions interact with each other, a comprehensive method can be achieved to introduce and practice cyber autonomy in our nation.

No country can ever be fully safe from threats. But adequate measures can be taken to minimize the possibility of an attack. India needs to investigate its cyber security strategy as prevention is always better than cure.

CONCLUSIONS

It is becoming more and more challenging to defend networks and computer systems. The increasing complexity of systems due to the pervasive deployment of Internet of Things and cyber physical stems implies that human effort alone does not scale as software are being released at a faster pace than we can examine. Brute force is required to tackle this, and machines have this. This brute force is necessary to detect, analyze, exploit, and patch various software and applications so leveraging it is smart. Implementing cyber autonomy can tackle multiple security issues, which otherwise would make us vulnerable.

In case of India over the years various policies have been implemented to tackle its cyber security issue. But lack of a comprehensive framework makes it harder to safeguard its cyberspace. Today, India ranks among top 5 countries in the world most affected by cybercrime. As per the data released by CERT-IN, cyber-attacks in 2020 increased by 300%, a significant jump as compared to 2019. Four major cyber-attacks targeted Indian banking and government institutions in past 5 years. As reliance on online banking and growing technology increases, these numbers are expected to surge in future as hackers keep exploring different ways to exploit loopholes within the system, and for this very reason implementation of cyber autonomy within India's cyber security strategy becomes the need of the hour. Accommodating cyber autonomy into its framework can greatly increase the safety of its critical infrastructure. If we look at India's cyber security through the lens of cyber autonomy, India will be able counter the ongoing asymmetry where solutions are outweighed by the diverse attacks just to achieve parity between attacks and solutions. India needs to revise its cyber security strategy by keeping up with the emerging trends, and cyber autonomy is the latest trend.

REFERENCES

[1] Ko, R. K. L, "Cyber Autonomy: Automating the Hacker- Self-healing, self-adaptive, automatic cyber defense systems and their impact to the industry, society and national security," ArXiv.Org 2018.

[2] Brumley, D., 2018. The Cyber Grand Challenge and the Future of Cyber-Autonomy. USENIX

[3] Crispan, C. et al., 1998. Stackguard: Automatic adaptive detection and prevention of buffer-overflow attacks. USENIX Security Symposium

[4] Liivoja, R., Naagel, M. & Väljataga, A., 2019. Autonomous Cyber Capabilities under International Law, Talinn, Estonia: NATO.

[5] Mezic, A. (2019, November 3). Why Autonomous AI is Needed in Cybersecurity. Security Boulevard.

[6] Kumar, V. (2019, October 11). Autonomous Cyber AI: A New Defence System in Cybersecurity. Analytics Insight.

[7] C. (2019, October 9). Autonomous Cyber AI is Revolutionizing Cyber Defense. CISOMAG | Cyber Security Magazine.

[8] Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture. (2018, May 1). IEEE Conference Publication | IEEE Xplore.

[9] A. Kott, L. V. Mancini, P. Theron, M. Drašar, H. Günther, M. Kont, et al., "Initial Reference Architecture of an Intelligent Autonomous Agent for Cyber Defense", US Army Research Laboratory ARL-TR-8337, March 2018.

[10] M. R. Stytz, D. E. Lichtblau and S. B. Banks, "Toward using intelligent agents to detect assess and counter cyber attacks in a network-centric environment", Institute For Defense Analyses Alexandria VA, 2005.

[11] R. Rasch, A. Kott and K. D. Forbus, "Incorporating AI into military decision making: an experiment", IEEE Intelligent Systems, vol. 18, no. 4, pp. 18-26, 2003.

[12] R. Rasch, A. Kott and K. D. Forbus, "AI on the battlefield: An experimental exploration", AAAI/IAAI, 2002.

[13] Ali Mirza, Qublai K., Irfan Awan, and Muhammad Younas. "CloudIntell: An Intelligent Malware Detection System." Future Generation Computer Systems 86 (2018): 1042-053. Print.

[14] Subramanian, R. (2020). Historical Consciousness of Cyber Security in India. IEEE Annals of the History of Computing, 42(4), 71–93.

[15] Parmar, S. D. Cybersecurity in India: An Evolving Concern for National Security.