DOI: https://doi.org/10.53486/sstc2024.v2.10
CZU: 004.056.5

A NEW FUTURE FOR CYBER SECURITY

BRADU Nichita, Bachelor Cyber Security Student
IU International University of Applied Sciences
Berlin, Germany
Telephone: + 49 152 07701335
Email: bradunichita.cs@gmail.com

Abstract: *The article discusses the main trends in cybersecurity and the rise of artificial intelligence. It analyzes the landscape of cyber security that will be projected to see significant advancements and changes in the future.*
Keywords: *threats, cybersecurity, hacker, artificial intelligence, security measures, cyber criminals*

JEL CLASSIFICATION: C82, D74, D84

INTRODUCTION

To some individuals, AI is the creation of artificial life forms that are capable of outsmarting human intelligence, while to others, it is any form of data processing technology that can be referred to as AI. Cyber security protects the personal information of users online by keeping it secret; for example, password information, financial information, and personal emails. If not well protected, it is very easy for hackers and other cyber criminals to access and misuse this information in fraudulent deals. This can be done by improving our cyber security so we will not victims of cyber-attacks and hence protecting our digital identities.

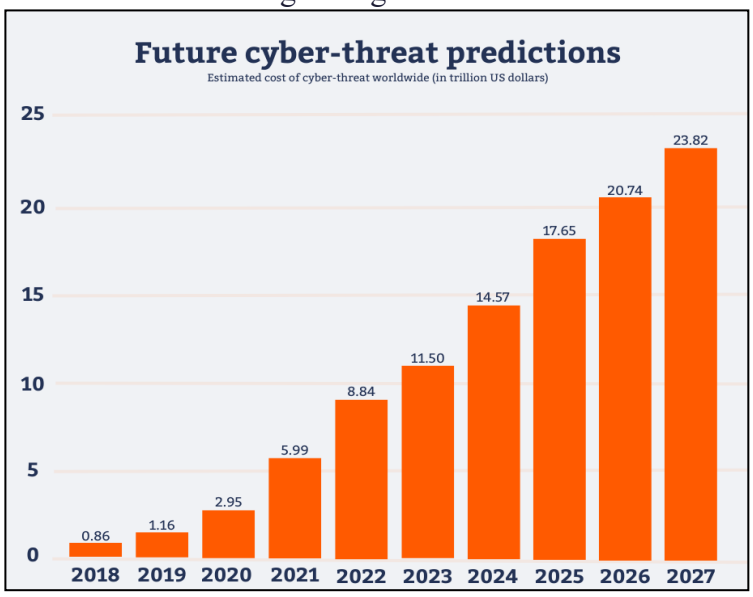
AI in Cyber Security: Impact. AI turned the world upside down last year. Today we are therefore faced with the all-important question: Who will use the new technologies and behavioral psychological principles more effectively to their advantage in 2024 - we or the cybercriminals? The answer is both. We're not ready for cyber-attacks yet. That's the simple truth. Yet, many organizations still don't meet this low threshold of protection and safety. Professionalization in cybercrime continued to progress, reaching a whole new peak in 2024 with the increase in AI and innovative technologies. This is because this will be the period when organizations invest in their security, considering that in the near future, the methods of cybercriminals are likely to perfect.

Battling Cyber Threats in 2024: The Role of AI and the Future of Security Measures. Professionalization of cybercrime, combined with artificial intelligence, enables cybercriminals to construct complex social engineering attacks that are scarily and convincingly realistic. Ralf Schneider said, Allianz Senior Fellow, Head of Cyber Security and NextGenIT Think Tank that bad guys need less and less and less organizational power in order to drive a really good attack. In the end, this will present us with a quantity problem. With AI on our side, too, we can offer better, more efficient solutions that are adaptive to any emerging threat in the year 2024. Artificial intelligence on our side will continuously perform better in detecting and responding to cyber threats in real time by leveraging machine learning algorithms to identify and neutralize malicious activity with greater speed. This will further allow more sophisticated authentication methods such as biometric identification and behavioral analytics to enhance security measures against unauthorized access. On the other hand, from a hacker's perspective, artificial intelligence can be used to further develop and increase the complexity of cyber threats, thus making the job of traditional cybersecurity measures even harder. Also, AI algorithms can become extremely complicated; their decision-making processes are not always understandable by humans. It is this lack of transparency that complicates the process of discovering and resolving certain vulnerabilities in AI systems.

What are cybersecurity trends in 2024? The future of cybersecurity looks bright, with several exciting trends on the horizon. A few predictions for 2024:

- Increased Automation & Artificial Intelligence
- Improved Collaboration & Cyber Security Analytics
- The Rise of Machine Learning
- Cloud Security Gets a Boost
- Greater Focus on User Education & Awareness

The trends in cybersecurity in 2024 will include data protection from unethical means, such as hackers, with the support of the latest technological advancement. These include RaaS, AI & Automation, Cloud Security, Cyber Threat Intelligence, IoT, and many others. Moreover, access to technology has facilitated us with more data compared to any other era. However, greater convenience implies greater risk due to cyber-attacks along with other security vulnerabilities. This is where it becomes very significant to be updated on new trends in cybersecurity, so that it can catch up with this threat, which does seem to be growing.



Source: Statista AZTECH

We need to act now. For the first time in history, cyber-attacks are accelerating faster than our defenses can keep up, and we cannot afford to wait longer. Malicious activity targeting all the world through cyberspace continues unabated at an unprecedented rate, with cybercriminals and state-based or state-sponsored actors routinely targeting our networks and data. The industrialization of cybercrime has made it easier than ever for malign actors to steal valuable data, disrupt our systems, etc. The criminals and states are not only seeking to exploit vulnerabilities in our devices and people but also disrupt critical infrastructure and government systems.

CONCLUSION

Cyber security will continue to be of increasing importance in 2024 due to the rapid evolution of technology and thus constant changes in threats. Not less crucially, organizations need to invest significantly in robust security measures, train their people in best practices, and stay up to date with the latest threats that might compromise sensitive data or systems. Since individual, corporate, and government dynamics are at play in that very space, cybersecurity challenges call for everyone's best effort and consideration to keep up and provide a secure online environment for one and all. By being more aware and taking conscious steps, we can minimize cyber threats and build a robust digital atmosphere both now and for the times to come.

REFERENCES:

1. Michael Houghton. 13 Top Strategic Cyber Security Trends to Watch Out For in 2024. 2023.
2. MacdonnelUlsch. CYBER THREAT! How to Manage the Growing Risk of Cyber Attacks. 2014.
3. Australian Guvernament. 2023-2030 Australian Cyber Security Strategy. 2023.
4. Tushar Bhardwaj, Himanshu Upadhyay, Tarun Kumar Sharma, Steven Lawrence Fernandes. Artificial Intelligence in Cyber Security: Theories and Applications, 2023.
5. Yuri Diogenes, Dr. Erdal Ozkaya. Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, Second Edition. 2019.
6. Alessandro Parisi. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. 2019.
7. Charles J. Brooks, Christopher Grow. Cybersecurity Essentials: An accessible introduction to cybersecurity concepts and practices. 2018.
8. Metroway: What is your Cyber Security strategy? 2023.
9. Tomaž Klobučar, Ramanpreet Kaur - Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. 2023.

Coordonator ştiinţific: OHRIMENCO Serghei, dr.hab., prof.univ.
Academia de Studii Economice din Moldova
Republica Moldova, mun.Chișinău
str. Bănulescu Bodoni 61,
Telephone: + 373 79359405
E-mail: osa@ase.md