Claudia-Alecsandra GABRIAN
Babeș-Bolyai University, Romania

RANSOMWARE IN THE AGE OF AI: NAVIGATING CYBERSECURITY CHALLENGES IN HYBRID WARFARE

Abstract:	*While the volume of ransomware threats continues to escalate around the world, AI revolutionizes the landscape of cyber offense and defense. Ransomware now evolves into an even more flexible and complex weapon, enabled through AI, morphing into a tool to attack critical infrastructure by state-sponsored opponents. Attackers leverage automation, adaptive encryption, and advanced phishing, whereas defenders employ AI-driven predictive algorithms, behavioral analysis capabilities, and real-time anomaly detection. On the one hand, AI for defense is limited by the vulnerability to adversarial attacks and rapid evolution of malware-both very serious challenges.* *The case studies will present the ransomware's role in hybrid warfare heighten national security risks and geopolitics. Argument: AI has transformed ransomware from a simple form of cyber extortion into an effective weapon for destabilizing the key infrastructures of a nation. Why it matters: Resilient knowledge of this evolution will be the knowledge that is needed for developing resilient cybersecurity strategies. Main question: What constitutes ransomware as a feasible hybrid tool of war? Objective: Identify and evaluate the challenges AI-driven ransomware presents for cybersecurity in hybrid warfare. Literature Review: A review of recent studies on the application of AI within the context of ransomware and hybrid warfare, reports on ransomware attacks and groups of cybercriminals. Data Analysis: Reviewed trends in the evolution of ransomware, AI development, and hybrid warfare strategies.*
Keywords:	**Cybercriminal groups; ransomware; artificial intelligence; critical infrastructure; AI tools**
Contact details of the authors:	E-mail: claudia.gabrian@ubbcluj.ro
Institutional affiliation of the authors:	**Babeș-Bolyai University, Doctoral School of International Relations and Security Studies**
Institutions address:	Mihail Kogalniceanu, no. 1 Street 400084, Cluj-Napoca, România; Tel: +40 264 405 300; Fax: +40 264 591 906, https://www.ubbcluj.ro/en/

Introduction

The nature of conflict, in these times of AI-driven warfare, has grown beyond physical battlegrounds into cyberspace where digital tools along with AI are being used to disrupt, disable, or manipulate adversaries. Hybrid conflicts combine conventional military operations with cyberattacks, disinformation, and economic sabotage. Thus, it becomes a dominant strategy both for state and non-state actors. Hybrid war applies to the use of classic military actions in addition to asymmetric activities, like cyberattacks, to destabilize and destroy a target. Cybermeasures, including ransomware attacks, increasingly form part of this. Most importantly, AI transforms ransomware and other cyber tactics, making such attacks faster, targeted, and adaptable. The new code Rust in russian is the modernization of ransomware-a new challenge to critical infrastructure protection and national security in an AI-driven cyber landscape.

The evolving threat of ransomware is one of the major challenges in this conflict landscape. Ransomware attacks are some of the persistent cybersecurity attacks, where malicious actors encrypt important information until a requested ransom is paid for access. These attacks exploit weaknesses in communication networks and critical infrastructure, and lately, they have been using advanced AI algorithms that help them

identify targets of high-risk systems. In AI-powered ransomware campaigns, automation in scaling phishing attacks, optimization in malware delivery, and evasion of traditional cybersecurity defenses are realized.

Ransomware now can be used in hybrid warfare to disrupt societies and critical sectors, such as healthcare, finance, and government. Leveraging AI, an adversary could go on to render any ransomware attack more precise, at scale, and with strategic and psychological consequences on both civilian and military targets. Moreover, AI-powered automation allows cybercriminals to orchestrate an attack against global networks faster and on a wider scale. The same multiplies the challenge of cybersecurity defense. The combination of AI-driven warfare and ransomware creates an increasingly dangerous setting in which the security of the world would face a serious threat. As more communications technologies are put to military and civilian use, the establishment and enforcement of superior cybersecurity controls become quite vital as a counterbalance to these AI-enabled threats. It would have to involve reaping the support of governments, corporations, and international security agencies in developing AI-based defenses against the continuing ransomware threat in hybrid conflict scenarios.

In the literature review, there are a lot of studies that include AI applications in cybersecurity, focusing on both offensive and defensive strategies. Some articles that are relevant to this topic show that using AI, cyberattacks have become increasingly frequent, impactful, and sophisticated. Nowadays, the dual-edged nature of AI is used for the benefit of organizations and cyber criminals, this means that defensive AI uses machine learning (ML) and other AI techniques to improve the security and resilience of computer systems and networks against cyber-attacks. Conversely, offensive AI takes advantage of the abuse of AI for malicious activities. Some examples include creating new cyberattacks or automating the exploitation of existing vulnerabilities. Also, a third part is correlated with adversarial AI or abuse of AI systems. That can be defined as attacks that might exploit vulnerabilities in AI systems to cause them to make incorrect predictions with either manipulation over the input data feeds to the AI system or poisoning up the training data on which the respective AI system was trained[1].

In support of such expert analysis, many forms of cyber defense systems have been designed in support and collaboration with experts. This is important in ensuring privacy and the integrity of information are secure and accessible through cybersecurity systems from internal and external threats. Therefore, the general purpose of cybersecurity systems is to combat security threats emanating from online sources, even including ransomware. Consequently, there has been a need for the more dependable cybersecurity infrastructure that encompasses both the defensive and offensive approaches through the employment of advanced methods for the discovery of previously unknown cyber intrusions and techniques. In general, defensive approaches use reactive strategies that are focused on prevention, detection, and responses. This is the more a traditional method to keep networks safe from the cybercriminal and requires a thorough understanding of the system to be secured. Understanding of the system and various weak points gives rise to the development of preventive measures. The offensive approaches, on the other hand, are a counterpoint to the defensive methods and proactively predict and remove threats in the system using various ethical hacking techniques. As a vast volume of data is accessible and cyber criminals attempt to get illegal access to cyber-infrastructures, various techniques of Artificial Intelligence and Machine Learning have been explored. This is because ML-based cybersecurity solutions, both offensive and defensive, have been able to handle and analyze large volumes of data and complex detection logic that were tough to handle using traditional methods[2].

One important and dynamic theme that this article shows within the transformative potential of AI in countering emerging cyber threats is the adaptability of defense strategies set within cybersecurity. The key to this adaptability is AI-driven models, which are able to learn dynamically and change in real-time. This responsiveness is so important given that cybercriminal actors have adapted their strategies on a moment-by-moment basis to affect their attack. Having a background in machine learning algorithms and pattern recognition, Artificial Intelligence can check new attack patterns rather swiftly that could be evading conventional static defenses. This is the ability that will let cybersecurity professionals stay ahead of the

[1] Masike Malatji, Alaa Tolah, *Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI*, Springer, February 2024, https://link.springer.com/article/10.1007/s43681-024-00427-4#citeas (23.11.2024)

[2] Jennifer Tang, Tiffany Saade, Steve Kelly, *The Implications of Artificial Intelligence in Cybersecurity*, Virtual Library Reports, October 2024, https://securityandtechnology.org/virtual-library/reports/the-implications-of-artificial-intelligence-in-cybersecurity/ (23.11.2024)

evolving threats and provide rapid development of countermeasures. The situational awareness gained allows for quicker, more informed decisions to be made, thus enabling pro-active responses to take place on all kinds of possible threats. Basically, it implies a complete paradigm shift in cybersecurity-that adaptability is now extended to AI-powered defense strategies. It does this by incorporating machine learning on top of dynamic threat modeling, thus going beyond rule-based traditional approaches. This ensures powerful defense that can rapidly counter and neutralize newly emerging cyber threats in today's rapidly shifting digital landscape[1].

The most notorious use of AI is the negative use of the technology by malicious actors for harm against the automated industry with the very methods that were designed for protecting the system. Being modular, AI can be shaped for threat and destruction rather than just safety and reliability. Besides, the vulnerabilities in the AI methods raise much more security concerns and threaten exploitation where attackers can manipulate the algorithms, invoke unnormal behaviors in the mechanism, and launch attacks such as adversarial attacks. The cyber criminals often divert the legitimacy of AI for this purpose to gain some personal benefits. AI incorporated attacks can be challenging to the security of the system as it can adapt to the security measures to evade detection, prevention, and mitigation techniques[2].

Defining ransomware and hybrid warfare

The typical lifecycle that defines ransomware includes infiltration, encryption, a demand for ransom, and possible decryption or destruction of data. Initially, ransomware was more opportunistic, often affecting individuals and small businesses. However, it has grown into a sophisticated tool that is well used against large organizations and vital infrastructures, causing unparalleled disruption. The evolution has further led to even more sophisticated versions like Ransomware-as-a-Service that allows even none-tech-savvy cybercriminals to conduct ransomware attacks[3].

Hybrid warfare integrates all these traditional military objectives with cyber, information, and psychological operations directed at an enemy to force strategic accomplishment of goals without resorting to conventional fighting. The form of war would also include the use of cyberattacks, such as ransomware, to disrupt basic services, create socioeconomic turmoil, and even further weaken the economy of an adversary. As such, where cyber capabilities have been used for the defeat of essential infrastructure as part of hybrid war techniques, state and state-sponsor actors are able to influence pressure in politically sensitive regions without necessarily resorting to conflict. When it strikes vital services in energy, health, and others, ransomware can be included as part of hybrid warfare, acting as a geopolitical instrument of influence and coercion[4].

AI is playing a increasingly bigger role in ransomware, amplifying their effectiveness, adaptability, and stealth. Attackers use AI-powered techniques to automate ransomware delivery, enhance social engineering, and evade detection-all factors that complicate defense efforts. In the context of hybrid warfare, AI-enhanced ransomware is a low-cost, high-impact tool that state-sponsored actors can use to disrupt essential services relatively anonymously. Since AI enables adaptable and evasive attacks, it will be more challenging to identify the origin of ransomware as coming from a particular group or nation, making diplomatic responses difficult and adding additional complications to national security. Tools that are used:

Automation of Ransomware Delivery and Execution: AI algorithms are making it easier to deploy ransomware across a large network because they can automate the tasks involved in deploying ransomware, such as scanning for vulnerabilities, moving laterally within a network, and encrypting files, as has been seen in attacks like WannaCry and NotPetya.

Advanced Social Engineering Techniques: Using machine learning algorithms that analyze current social media information, patterns in people's email use, and other public information, highly convincing

---

[1]Badria Sulaiman Alfurhood, Dattatreya Mankame, Meenakshi Dwivedi, *Artificial Intelligence and Cybersecurity: Innovations, Threats, and Defense Strategies*, https://www.researchgate.net/publication/376375202_Artificial_Intelligence_and_Cybersecurity_Innovations_Threats_and_Defense_Strategies (23.11.2024)

[2]Rafy Fazley, *Artificial Intelligence in Cyber Security*, https://www.researchgate.net/publication/377235308_Artificial_Intelligence_in_Cyber_Security (23.11.2024)

[3]Cybersecurity and Infrastructure Security Agency (CISA), *Ransomware Guide*, Stop Ransomware, https://www.cisa.gov/stopransomware/ransomware-guide (01.11.2024)

[4]Broadcom, *Symantec Internet Security Threat Report*, Symantec, Vol. 3, January 2023, https://docs.broadcom.com/doc/istr-03-jan-en (01.11.2024)

phishing messages can be built targeted against a specific individual or organization; Adaptation to Detection and Evasion: Most of the traditional cybersecurity tools use known patterns or signature-based detection of malware for their detection. Artificial intelligence uses deep learning and machine learning models and enables ransomware to evade these defenses by adapting in real time[1].

Analyzing reports on ransomware attacks shows that ransomware is considered one of the most widespread attack vectors in the modern world, also through the Ransomware-as-a-service model. The ransomware ecosystem has visibly evolved during the first half of 2024, were notable changes in the methodologies of attack, victimology, and tactics of cybercriminals. The team from Rapid7 identified 21 new ransomware groups coming onto the scene in the first six months of 2024, some of them are brand new, while others have been rebranded as previously known groups.

The use of encryption algorithms such as AES, RC4, and especially ChaCha underlines a strategic decision taken by ransomware groups to optimize performance and security evasion. Such evolution of infection techniques is part of the more general trend for cybercriminals to focus on increasingly sophisticated tools and upgrading the effectiveness of their attacks.[2] Also, is important to analyze the next six months for 2024, to see if these cybercriminal groups can reestablish and adapt their techniques to launch cyberattacks using AI methods.

The evolution of ransomware with AI capabilities

Ransomware attacks moved during the 2010s from targeting individual users to big organizations and critical infrastructures. Although RaaS platforms had given an opportunity for less technical criminals to commit such attacks, a series of highly visible ransomware attacks, such as WannaCry and NotPetya, showed how much disruption ransomware could cause. Further, throughout the 2020s, artificial intelligence accelerated this evolution by making ransomware a lot more automated, adaptive, and persistent[3]. AI technologies transformed ransomware into a more sophisticated, evasive, and effective weapon. The main AI-powered improvements include:

Automation and Scaling: AI makes it possible for ransomware attackers to automate every step of the attack, from initial compromise all the way to lateral movement. AI-driven automated tools can identify and exploit weaknesses much faster and at higher scales than would be possible manually. Attackers use machine learning in refining their targeting precision by selecting victims based on industry, network vulnerability, or payment potential that improves the overall success rate of ransomware[4].

Adaptive Encryption and Behavior: Traditional ransomware encrypted files in a predictable and, therefore, detectable pattern. AI makes it possible for ransomware to adapt to various encryption algorithms, changing dynamic behavior and becoming more evasive to traditional static defense mechanisms. The adaptive encryption allows ransomware to selectively encrypt important files, many times waiting to evade initial scans before launching a full attack-a ploy that gives attackers an upper hand over traditional detection models which might not identify altered encryption patterns[5]. Advanced Social Engineering/Phishing Techniques: Traditionally, phishing has always been one of the popular delivery methods of ransomware, but it is now

---

[1] Gavin Hull, John Henna, Arief Budi, *How to improve cybercrime investigations: A review of the digital forensic literature in the wake of recent technological advancements*, "Crime Science", Vol. 8, No. 9, September 2019, https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-019-0097-9 (01.11.2024)

[2] Rapid7, *2024 Ransomware Radar Report*, October 2024, https://www.rapid7.com/globalassets/_pdfs/2024-rapid7-ransomware-radar-report-final.pdf (23.11.2024)

[3] CSO, *A history of ransomware: The motives and methods behind these evolving attacks*, July 2020, https://www.csoonline.com/article/569617/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html (01.11.2024)

[4] Benjamin Jensen, Yasir Atalan, Jose Macias, *Algorithmic Stability: How AI Could Shape the Future of Deterrence*, Center for Strategic and International Studies, June 2024, https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-deterrence (01.11.2024)

[5] Microsoft Corporation, *Microsoft Digital Defense Report 2024*, Microsoft Security Insider, 2024, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 (01.11.2024)

more effective because of AI. Through machine learning algorithms, it can analyze an enormous amount of data with the ability to create highly personalized phishing emails around possible targets[1].

AI-Driven capabilities enhancing ransomware in hybrid warfare

Hybrid warfare will continue to evolve with advances in technology and will shift the geopolitical environment. In as much as state and non-state actors will continue to leverage cyber-capabilities in the immediate future, the integration of digital warfare is very much a cornerstone of hybrid strategies. This evolution increases the complexity of conflict and further blurs the lines between traditional and unconventional military engagements[2].

For instance, emerging technologies using artificial intelligence will accelerate the speed of decisions and increase the accuracy of operations. They will advance intelligence collection and disrupt adversary communications, underlining the need for agile and creative countermeasures. Automation of ransomware in hybrid warfare enables state-sponsored groups to conduct large-scale attacks with unprecedented velocity and accuracy, often overwhelming traditional defenses. They can strike many critical systems, crippling energy, transportation, and healthcare sectors with more operations. AI-driven adaptive encryption increases the evasive capabilities of ransomware. While older ransomware relies on static encryption methods, AI-enhanced ransomware can dynamically switch to different keys or algorithms to thwart decryption or forensic analysis. Adaptive encryption provides the ransomware with the intelligence to adaptively adjust to the specific defensive layouts of a target-such as switching to a different encryption algorithm if the previous one was detected as vulnerable, thereby keeping the data locked. Ransomware can be adaptive in that it changes its code to evade traditional antivirus detection, especially with polymorphic ransomware. In hybrid warfare, adaptive encryption can be strategically targeted at critical infrastructure, with data recovery, being difficult, especially for high-value targets such as government agencies and defense organizations[3].

One of the most potent contributions AI has made to ransomware is its capability for personalized attack through custom targeting. The attackers will apply machine learning algorithms to aggregate multiple volumes of data on individuals and organizations, tailoring the methods of delivery for the ransomware in hopes of increasing the potential success rate of an attack. Examples involve AI-powered tools that monitor communication patterns of a target, their social media usage, and network activity; this provides insight into the ways to infiltrate the network most effectively through things like highly customized phishing emails or crafted malware downloads[4].

In hybrid warfare, ransomware strikes, tailored for specific targets, are allowed on selected victims by state-sponsored actors based on their political, economic, or military importance. Examples target critical infrastructure, such as power grids and telecommunications systems, to create maximum disruption. Furthermore, malware can also be tailored for specific languages, cultures, and sectors, which will make sure that the ransomware really resonates and spreads effectively in the targeted environment. The evasiveness of ransomware during the compromise of critical systems for extended durations presents difficult countermeasures, particularly in high-value environments such as defense networks, government agencies, and financial institutions[5]. AI greatly enhances the efficiency of spear-phishing and social engineering tactics, which usually serve as entry points for ransomware. Conventional phishing emails have generic messages and broad targeting, hence being much easier to identify as suspicion prone. With AI, immense personal and organizational data can be analyzed to send tailor-fit phishing emails that look quite legitimate. Machine

[1] CrowdStrike, *Types of Social Engineering Attacks*, https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/ (01.11.2024)

[2] Total Military Insight, *Historical Examples of Hybrid Warfare*, July 2024, https://totalmilitaryinsight.com/historical-examples-of-hybrid-warfare/ (23.11.2024)

[3] SentinelOne, *What is Polymorphic Malware?,* https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-polymorphic-malware/ (02.11.2024)

[4] Microsoft Corporation, *Audience Targeting*, https://about.ads.microsoft.com/en/tools/performance/audience-targeting (02.11.2024)

[5]Frank Hoffman, Matt Neumeyer, Benjamin Jensen, *The Future of Hybrid Warfare*, Center for Strategic and International Studies, July 2024, https://www.csis.org/analysis/future-hybrid-warfare (02.11.2024)

learning algorithms will tune messages based on a target's recently observed social media activity and professional contacts[1].

AI-Driven defense mechanisms against ransomware

AI-powered predictive models are changing the face of ransomware defense through swift identification of precursors to potential threats before they enter a system. Predictive models, by analyzing big data sets inclusive of attack patterns, vulnerabilities, and system configurations, compute the environments that are at greater risk and predict when and where the ransomware attacks will take place. AI-powered threat intelligence solutions aggregate feeds in real time, analyze the information, and present insights to the security teams for timely awareness of the latest emerging threats and how ransomware patterns are trending. Most of them are designed on machine learning models that have been trained on previous attacks and computer signals to identify early warning signals that will enable the organization to patch the vulnerabilities as well as change firewall settings, among other preventive measures, to avoid infiltration[2].

Predictive algorithms represent early warnings of highly organized ransomware campaigns in hybrid contexts of war, allowing governments and critical sectors to prepare their defenses in anticipation of possible state-orchestrated cyberattacks. This is of great essence in securing critical infrastructure, where the stakes for a ransomware breach could be as high as national security and public safety[3]. This would be the most important capability in a hybrid war scenario to strike back ransomware against critical infrastructure, as behavioral analysis tools can detect and mitigate ransomware threats aimed at basic infrastructure-like power grids, healthcare, and communications systems of any type in a way that would really lessen possible disruption[4].

Anomaly Detection Systems have improved response times by real-time alerts to security teams, the automatic responses include system isolation and blocking suspicious traffic. AI is not only helpful at the stage of detecting ransomware but also in coordinating rapid response and recovery. AI-driven automated incident response systems can triage security alerts, prioritize incidents down to those that need attention, and can even take containment steps such as disconnecting the affected device from the network[5]. AI can further reinforce such recovery efforts by locating and restoring critical files from backups and isolating encrypted files to stop further proliferation[6]. AI is changing the face of ransomware defense by having predictive, responsive, and adaptive capabilities that normally are not achievable with conventional cybersecurity means. Tools of modern AI-driven ransomware defense include:

Predictive algorithms: These algorithms analyze past ransomware attack data for patterns that can help in predicting future threats. Such algorithms evaluate the extra vulnerabilities an attack may cause in a network and provide proactive defense mechanisms to cybersecurity teams, which would alert them about areas of high risks or recommend proactive defenses.[7]; Behavioral Analysis and Anomaly Detection: AI-driven behavioral analytics solutions identify patterns of activity operating out of the ordinary, which, in this context, could mean an imminent ransomware attack. Anomaly detection provides additional security in that it will include all those minor and minute variations that perhaps the static defense mechanisms would not be able to detect[8].

The qualitative analysis revealed that to assess the effectiveness of AI-driven defense mechanisms is important to develop robust intrusion detection systems for cyberthreats, such as ransomware, because is important to understand malware behavior. Machine learning stands at the forefront of automating behavior

[1] Trend Micro, *Spear Phishing*, http://www.trendmicro.com/vinfo/us/security/definition/spear-phishing (02.11.2024)
[2]World Economic Forum*, AI and Cybersecurity: How to Navigate the Risks and Opportunities*, https://www.weforum.org/stories/2024/02/ai-cybersecurity-how-to-navigate-the-risks-and-opportunities/ (02.11.2024)
[3]Microsoft Corporation, *What is Behavioral Analytics?,* https://www.microsoft.com/en-us/dynamics-365/topics/ai/customer-insights/what-is-behavioral-analytics, (02.11.2024)
[4] Fortinet, *Network Traffic,* https://www.fortinet.com/resources/cyberglossary/network-traffic (02.11.2024)
[5]Broadcom, *Symantec Ransomware Threat Landscape 2024,* https://www.symantec.broadcom.com/hubfs/Symantec_Ransomware_Threat_Landscape_2024.pdf?hsCtaTracking=767be7a3-c8a1-4cd1-8387-7ec8ac770b3c|e27274de-c76f-4496-ac64-e943054afaa8 (02.11.2024)
[6] IBM, *AI Cybersecurity*, https://www.ibm.com/ai-cybersecurity (02.11.2024)
[7] IBM, *Predictive Analytics*, https://www.ibm.com/topics/predictive-analytics (02.11.2024)
[8]CrowdStrike, *AI-Powered Behavioral Analysis*, https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/ai-powered-behavioral-analysis/ (02.11.2024)

analysis through informative feature extraction from network packets and paving the way for developing sophisticated intrusion detection systems. Deep learning (DL) defense mechanisms are increasingly deployed to automate the identification of cyber threats and with these systems continuously evolving can enhance effectiveness over time. The primary themes are related to regular updates for DL to maintain effectiveness[1], and various mitigation strategies against different types of AI-driven cyberattacks for empirically assessing effectiveness.

AI-empowered and real-time network traffic analysis extends aptitudes for more detection and neutralize potential threats. Furthermore, AI-powered threat intelligence uses global threat landscapes and historical data to predict and to respond proactively to new threats. Automation is one of the most important aspects of artificial intelligence in the process of threat mitigation through the coordination of responses. By putting threat data in context and discerning the real from the false, context-aware AI systems reduce the chance of missing a security incident and [2]AI-based models can repair cybersecurity bugs in a code[3].

AI technology integrated with human expertise in cybersecurity improves the efficiency of threat detection mechanisms. Conclusively, AI technology has revolutionized cybersecurity incident response by introducing automation that augments efficiency and effectiveness within cybersecurity defense strategies respecting threat detection and mitigation.[4] AI models will learn a pattern and behaviors found in previously collected data; this is potentially less effective in malware detection for sophisticated ransomware operating. This reliance on historical data creates a blind spot concerning zero-day ransomware attacks-new subtypes that take advantage of unknown security vulnerabilities[5].

Case studies

In 2017, ransomware attack known as WannaCry used exploits against unpatched systems to rapidly spread across networks. Whereas during the time this attack occurred, several organizations' defenses were using AI-based defenses, none of these systems identified the propagation strategy used by WannaCry-a limitation pointing to a gap in training AI models on pre-existing attack behaviors. The inability to detect WannaCry, in this respect, underlines fully the risks of relying solely on machine learning models that cannot adapt to new, previously unknown forms of attack. This incident, thus, puts into focus the importance of having updated patches along with system defenses in addition to the solutions provided by AI[6].

As a short analysis, WannaCry, sometimes also called WCry or WanaCryptor was a ransomware malware. The virus that was associated with ransomware had worm functionality since it is able to spread itself within infected networks. Following the completion of encryption, a ransom note was displayed to the user, in which the attackers ask for $300 to be paid in a 3-day time span. The ransom amount increases to $600 if the victim resists, which is to be paid in 7 days. In that attack in 2017, an EternalBlue exploit was used, believed to have been developed by the American NSA and which had previously been leaked by a cybergang known under the alias “The Shadow Brokers”. This exploit affects the Windows operating system, for which the company provided a patch to fix in a rush. Unfortunately, many individuals and organizations that did not update computers were targeted in this attack, more than 200,000 computers worldwide were infected with WannaCry within a few days when the attack. A fix of the EternalBlue exploit, along with finding the “kill switch” that allowed stopping the execution of the malware, were the two main contributions helpful in

---

[1] Aya Salem, Saffa Azzam, *Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques*, “Journal of Big Data”, Vol. 11, No. 105, August 2024, https://doi.org/10.1186/s40537-024-00957-y (23.11.2024)

[2]Masike Malatji, Alaa Tolah, *Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI,* “*AI and Ethics”*, February 2024, https://doi.org/10.1007/s43681-024-00427-4 (23.11.2024)

[3]Irshaad Jada, Thembekile Mayayise, *The impact of artificial intelligence on organizational cybersecurity: An outcome of a systematic literature review*, “*Data and Information Management”*, June 2024, https://doi.org/10.1016/j.dim.2023.100063 (23.11.2024)

[4]HacknJill, *Can Cybersecurity Be Replaced by AI?*, https://hacknjill.com/cybersecurity/advanced-cybersecurity/can-cybersecurity-be-replaced-by-ai/ (23.11.2024)

[5] Jannatul Ferdous, et.all., *AI-Based Ransomware Detection: A Comprehensive Review*, “IEEE Xplore”, Vol. 12, September 2024, https://ieeexplore.ieee.org/document/10681072 (03.11.2024

[6] CSO, *WannaCry Explained: A Perfect Ransomware Storm*, https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html (03.11.2024)

slowing down this malicious campaign. By the time it was finished, though, total damage had reached into the billions, with victims in over 150 countries having been affected. A campaign of such scale raised international investigation of the highest level aimed to find out who was behind the outbreak and was find out that ransom notes were most likely written by hand, with the writers seemingly fluent in Chinese[1].

The DarkSide Ransomware Attack on Colonial Pipeline 2021 was another ransomware attack, representing one of the more significant ransomware attacks that had been publicly disclosed to take place against critical infrastructure in the U.S. During the attack, while the pipeline's operational technology systems responsible for physically moving the oil were not directly compromised, they shut down 5,550 miles of pipe. After stealing the data, the hackers infected ransomware in the "IT Network" of Colonial Pipeline, which later spread the attack to many work computers necessary for billing and accounting[2].

The Colonial Pipeline company was responsible for nearly half the fuel supply and is one of the most important pipeline operators in the United States. It carries nearly 45% of fuel for the East Coast: gasoline, diesel fuel, heating oil, jet fuel, and of fuel that military forces use. The company suffered so severely after the attack and after that it was declared a state of emergency status in 18 states to aid in the shortages. Five days since the shutdown prompted by the attack, Colonial Pipeline still cannot resume full operations.[3] The attackers had demanded a ransom of almost $5 million from the victim company, that was paid several hours after the attack and data of 99 victim companies has been leaked to the dark web. Colonial Pipeline recovered some data compromised by the attackers. Even after receiving the decrypt or, the pace to restore the systems remained very slow because of the decrypting tool they got from the attackers, and it had to continue using its own backups to restore its systems[4].

The 2017 ransomware attack on WannaCry and the Colonial Pipeline ransomware attack this year present a geopolitical scenario in which cybercriminals mount cyberattacks on critical infrastructures. 'WannaCry' ransomware, attributed to the North Korean group Lazarus, showed the world how ransomware might be used as a state-sponsored tool not only in crippling economies but as geopolitical pressure in targeting global systems for highlighting lapses in international cooperation relative to cybersecurity norms. Carried out by the hacking group DarkSide, the Colonial Pipeline attack became the latest in a string of ransomware attacks, underlining the increased sophistication of RaaS operations that had substantial economic consequences, such as fuel shortages up and down the U.S. East Coast. This also served to raise tensions between the U.S. and Russia, since groups like DarkSide were said to operate within the Russian sphere of influence. In both cases, the vulnerability of critical infrastructure was underlined, raising debate on international cybersecurity structures, public-private collaboration, and the ethics of ransom payments.

Strategic implications for national security and geopolitics

AI-driven ransomware represents a threat to national security, especially when we talk about critical infrastructure systems such as energy, healthcare, and finance. These are important features in the running of society, and any disruption to the same translates into widespread consequences for both public safety and economic stability. Energy or healthcare access can be disrupted when such facilities fall prey to a ransomware attack, thereby putting lives at risk while weakening peoples' confidence in the security that the government provides. Thus, in this sense, the national security influence of ransomware can be best described by the example of the enormous NotPetya attack in 2017 targeting Ukrainian businesses and government institutions and afterwards quickly propagated to important critical world industries: shipping and energy. While this latter attack was ostensibly financially motivated, the geopolitical consequences were extraordinary, where it seriously disrupted the operations of several multinational companies and caused billions of dollars in

[1] *WannaCry Malware Trends*, https://any.run/malware-trends/wannacry (23.11.2024)

[2] TechTarget, *Colonial Pipeline Hack Explained: Everything You Need to Know*, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know (03.11.2024)

[3] TrendMicro, *What We Know About Dark Side Ransomware and the US Pipeline Attack,* https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html (23.11.2024)

[4] Kaspersky ICS-CERT, *Dark Chronicles: The Consequences of the Colonial Pipeline Attack*, Kaspersky ICS-CERT Publications, https://ics-cert.kaspersky.com/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/ (23.11.2024)

economic damage. Because of its impact, the incident has been described by some governments as a kind of cyberwar[1].

Ransomware attacks attributed to state-sponsored actors escalate tensions between nations, and even have been known to lead to diplomatic or military action where, the complication for attribution arises when state actors allegedly support or enable ransomware groups to blow up diplomatic impasses: countries might resort to imposing sanctions, restricting trade, and even cyber-retaliation as deterrents. For instance, ransomware operations that were apparently conducted by Russian groups forced many Western nations to impose sanction and diplomatic measures on Russia for quota increases in international cyber relations[2].

Sanctions and countermeasures only play into the increasingly significant role of cyberspace in geopolitical strategy-where ransomware attacks are not only a question of extracting ransom but also tools of economic destabilization and psychological warfare. This makes the AI emergence in ransomware potentially amplify these effects, since machine learning allows for more targeted and efficient attacks, therefore making large-scale disruption even more likely. It is a strategic use of ransomware that shows how international relations debates about norms in cyberspace, accountability, and the threat of retaliation have to balance the option of exacerbating conflicts as a whole[3].

Beyond the economic costs, ransomware attacks affect public trust in institutions' capabilities for securing basic services. This is further complicated with an uptick in AI-driven ransomware, as this malware evolves around classic defenses, raising both frequency and severity. Such an erosion of trust calls for new regulations on cybersecurity from governments, including mandatory reporting requirements for critical infrastructure and an increased regulation of the cybersecurity practices pursued by the private sector. The emergence of ransomware has, hence, given way to the formulation of policies on infrastructural resilience, defensive policy founded on co-operation, and response[4].

The economic consequence of ransomware is severe, from direct costs-like ransom paid and remediation-to indirect costs, including business interruption and supply chain delays, which impose long-term economic burdens. The most important incidents of ransomware have forced governments and businesses to make a very substantial resource investment in recovery efforts, budgetarily straining and compromising public confidence in institutional cybersecurity measures. The Colonial Pipeline incident is a perfect example of such manifestations since it led to fuel shortages in the Southeastern United States, where gasoline prices rose and industries that depended on the transportation of fuel were affected[5].

Conclusions

Started as financially motivated cybercrime, ransomware escalated in a tool of hybrid warfare, threatening critical infrastructure disruption, economic disruption, and geopolitical destabilization by way of state-sponsored ransomware groups. As ransomware has increasingly become intertwined with AI, it has taken on new capabilities, including adaptive encryption, evasive techniques, and targeted delivery.

The most striking, is how ransomware integrating AI raises the scale, speed, and complexity of a threat that was unprecedented in its proposition towards national security, international relations, and economic stability. Understanding these transformations is essential in crafting effective defenses against this persistent threat. The RaaS model will continue to grow, where less sophisticated cybercriminals will utilize extremely powerful ransomware tools, thereby increasing the frequency and severity of the attacks. Nation-states will leverage malware to conduct espionage, sabotage, and even open conflict. Already, cyber weapons can take the lead in future conflicts; attacks against the critical infrastructures are intended to ensure general chaos.

Nations need to emphasize AI-fortified cyber defense and international cooperation. The integration of AI and ML into malware will open the door to new forms of autonomous, adaptive threats. The use of

[1]CloudFlare, *What are Petya and NotPetya*?, https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/ (05.11.2024)

[2] Hansel Mischa, Silomon Jantje, *Ransomware as a threat to peace and security: understanding and avoiding political worst-case scenarios*, "Journal of Cyber Policy", September 2023, https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2357092#abstract (06.11.2024)

[3] *Idem*

[4] *Idem*

[5]The New York Times, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, https://www.nytimes.com/2021/05/12/business/economy/colonial-pipeline-economic-impact.html (06.11.2024)

ransomware by state actors in hybrid war mechanisms underlines an ever-growing element of complexity and geopolitical importance in cyber warfare. Continuous research in the evolving role of AI in cyber war and further collaboration by nations on the legal frameworks. Ransomware tactics are used by state-sponsored hybrid warfare to disrupt critical infrastructure, destabilize nations, and undermine public confidence. Often, these tactics combine ransomware attacks with other forms of cyber aggression in ways that create unique and complex challenges for defending nations and organizations. The dynamically complex nature of ransomware in state-actor hybrid warfare underlines increasingly complex and geopolitically significant methods of cyber war.

In these ways, the attack of critical infrastructure and forms of ransomware are highly sophisticated, allowing state-sponsored actors to achieve goals of strategic disruption with limited attribution. Due to the inherent difficulties in defending against such kinds of attacks-rapid response, complexity, and the fog of misinformation-considerations should also be made for new approaches: cross-border intelligence sharing, AI mechanisms of defense, and unequivocal policies in terms of incident response for critical sectors. Ransomware being used by state actors as part of hybrid warfare represents an emerging layer of complexity and geopolitical relevance for cyber warfare. But ransomware attacks provide a continuously developing menace against national security, economic stability, and international relations when there is hybrid war. AI-driven ransomware becomes even smart, covers traditional defenses, and complicates attribution.

Case studies like the Colonial Pipeline Attack and similar cases and the hypothetical disruption of communication networks powered by AI require urgent calls for cybersecurity strategies. Lessons learnt from incidents highlight the operational importance of following improvement in attributions, AI-enhanced defense mechanisms, zero-trust policies, and public-private partnerships. Because developments regarding ransomware will continue to go forward with proactive international cooperation, defense against the next generation of hybrid warfare threats must be developed. AI-powered security tools add a new level of sophistication to the cyber defense against ransomware by using predictive algorithms, behavior analysis, and anomaly detection in real time. As AI can amazingly improve response times and threat detection rates, it also introduces challenges. For instance, limitations in adaptability and vulnerability to adversarial attacks. On the other hand, AI also poses certain specific significant challenges that balance its effectiveness in ransomware defense, such as limits to adaptability, adversarial AI attacks, and resource demands.

Gaps in current research

Up until this point, little attention has been paid to offensive and defensive AI in research, as most relevant literature remains anchored to the technological dimension of both defensive-adversarial and offensive AI. This underlines the need for more holistic research on AI in cybersecurity, considering non-technical factors that may influence AI-driven threats. Most research reporting on AI-driven attacks focuses on their technical engineering aspects. This gap points to a more holistic approach in carrying out research on the malicious potential of AI and its social impact, with particular emphasis on trying to understand what the current situation is regarding the AI-driven cyberattack landscape, motivation, mitigation strategies, and social impact. Even with lots of research in the application of AI in cybersecurity, there exists an obvious literature gap in terms of the long-term implications of AI-driven defense strategies. There is significant rare in-depth research evidence that has addressed socio-economic, ethical, and legal issues regarding this integration.

The absence of research in the literature underlines the need for a comprehensive investigation that goes beyond the technical effectiveness of AI in cybersecurity, while emphasizing the larger organization and societal ramifications that influence how digital defense mechanisms develop in the future. Research into the application of AI technologies to cybersecurity makes clear a series of challenges and limitations that use of these advanced technologies will need to be considered. In the context of AI driven cybersecurity, adversarial attacks stand out as a major concern. AI systems have vulnerabilities that malicious actors take advantage of in order to abuse them and produce results that are compromised. This underlines the importance it is to have strong security measures in place that can protect these technologies from manipulation by adversaries. There is a limit introduced by using historical data.

While AI systems are great, they excel at recognizing patterns in historical data; they could be challenged to identify previously unseen threats-what are called “zero-day threats” utilized by ransomware cybercriminals. In the dynamic and constantly changing area of cybersecurity, continuous monitoring, evaluation, and enhancement of AI algorithms become critical to maintaining state-of-the-art threat detection.

If AI is to be used to strengthen cybersecurity without sacrificing the robustness and agility of the mechanisms of defense against sophisticated threats, these issues must be resolved.

Future research directions

Asymmetrical development in cyber war has given rise to much more powerful and devastating attacks due to the wide adaptation and employment of AIs in generating and executing zero-day attacks. Key issues identified in AI-driven cybersecurity, so far, are indirect development of malicious AI-based software; the rising need to understand the reasoning behind AI-driven decisions; and dealing with new types of cyber-attacks whose nature may be devious to the AI mechanism. It is a challenge to have a balance in this aspect since transparency, explainability, fairness, and accountability in view mean that AI cyber resilience supported across the domain is one of those major challenges.

The rapid progress of AI reshapes the ransomware threats, mainly within the quite complex framework of hybrid warfare with state and non-state actors combining cyberattacks with the conventional means. Concretely, findings in the current domain of literature can be directed at areas for future research: the ways in which AI is used in the evolution of ransomware tactics into more dynamic and adaptive forms of malware using machine learning algorithms to evade traditional mechanisms of detection. For example, research can be performed to understand how attackers are using AI to optimize ransomware distribution, personalize ransom demands, and automate reconnaissance on targeted systems. Knowing these developments is bound to be crucial in developing countermeasures by using AI in predictive threat analysis, anomaly detection, and real-time response to these increasingly complex cybersecurity ecosystems.

Other studies might investigate how AI can reinforce a set of defensive measures against ransomware in hybrid warfare attacks since, in general, such attacks target technical and psychological vulnerabilities concurrently. Further research could be conducted on how AI-powered threat hunting tools, like neural networks, which utilize patterns indicative of ransomware before it is fully executed, could apply. The effectiveness of combining AI with blockchain technology for secure data backup and immutable logging of incidents should be one of the core research areas, considering resilience against ransomware and ensuring transparency and accountability in hybrid warfare situations.

Bibliography

Studies and Articles

1. Alfurhood, Badria, Sulaiman; Mankame, Dattatreya; Dwivedi, Meenakshi, *Artificial Intelligence and Cybersecurity: Innovations, Threats, and Defense Strategies*, https://www.researchgate.net/publication/376375202_Artificial_Intelligence_and_Cybersecurity_Innovations_Threats_and_Defense_Strategies
2. Fazley, Rafy, *Artificial Intelligence in Cyber Security*, https://www.researchgate.net/publication/377235308_Artificial_Intelligence_in_Cyber_Security
3. Ferdous, Jannatul, et.all., *AI-Based Ransomware Detection: A Comprehensive Review*, "IEEE Xplore", Vol. 12, September 2024, https://ieeexplore.ieee.org/document/10681072
4. Hoffman, Frank; Neumeyer, Matt; Jensen, Benjamin, *The Future of Hybrid Warfare*, Center for Strategic and International Studies, July 2024, https://www.csis.org/analysis/future-hybrid-warfare
5. Hull, Gavin; Henna, John; Budi, Arief, *How to improve cybercrime investigations: A review of the digital forensic literature in the wake of recent technological advancements*, "Crime Science", Vol. 8, No. 9, September 2019, https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-019-0097-9
6. Jada, Irshaad; Mayayise, Thembekile, *The impact of artificial intelligence on organizational cybersecurity: An outcome of a systematic literature review*, "Data and Information Management", June 2024, https://doi.org/10.1016/j.dim.2023.100063
7. Jensen, Benjamin; Atalan, Yasir; Macias Jose, *Algorithmic Stability: How AI Could Shape the Future of Deterrence*, Center for Strategic and International Studies, June 2024, https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-deterrence
8. Jensen, Benjamin; Atalan, Yasir; Macias Jose, *Algorithmic Stability: How AI Could Shape the Future of Deterrence*, Center for Strategic and International Studies, June 2024, https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-deterrence

9. Malatji, Masike; Tolah, Alaa, *Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI*, Springer, February 2024, https://link.springer.com/article/10.1007/s43681-024-00427-4#citeas
10. Masike, Malatji; Alaa, Tolah, *Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI*, "AI and Ethics", February 2024, https://doi.org/10.1007/s43681-024-00427-4
11. Mischa, Hansel; Jantje, Silomon, *Ransomware as a threat to peace and security: understanding and avoiding political; worst-case scenarios*, "Journal of Cyber Policy", September 2023, https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2357092#abstract
12. Salem, Aya Azzam Saffa, *Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques*, "Journal of Big Data", Vol. 11, No. 105, August 2024, https://doi.org/10.1186/s40537-024-00957-y

Documents and reports

1. *2024 Ransomware Radar Report*, October 2024, https://www.rapid7.com/globalassets/_pdfs/2024-rapid7-ransomware-radar-report-final.pdf
2. *AI-Powered Behavioral Analysis*, CrowdStrike Cybersecurity 101, https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/ai-powered-behavioral-analysis/
3. Broadcom, *Symantec Internet Security Threat Report*, "Symantec", Vol. 3, January 2023, https://docs.broadcom.com/doc/istr-03-jan-en
4. Broadcom, *Symantec Ransomware Threat Landscape 2024*, https://www.symantec.broadcom.com/hubfs/Symantec_Ransomware_Threat_Landscape_2024.pdf?hsCtaTracking=767be7a3-c8a1-4cd1-8387-7ec8ac770b3c|e27274de-c76f-4496-ac64-e943054afaa8
5. CloudFlare, *What are Petya and Not Petya?,* https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/
6. CSO, *A history of ransomware: The motives and methods behind these evolving attacks*, July 2020, https://www.csoonline.com/article/569617/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html
7. CSO, *Wanna Cry Explained: A Perfect Ransomware Storm*, https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html
8. Cybersecurity and Infrastructure Security Agency (CISA), *Ransomware Guide*, https://www.cisa.gov/stopransomware/ransomware-guide
9. Fortinet, *Network Traffic, Fortinet Cyber Glossary*, https://www.fortinet.com/resources/cyberglossary/network-traffic
10. HacknJill, *Can Cybersecurity Be Replaced by AI?*, https://hacknjill.com/cybersecurity/advanced-cybersecurity/can-cybersecurity-be-replaced-by-ai/
11. IBM, *AI Cybersecurity*, https://www.ibm.com/ai-cybersecurity
12. IBM, *Predictive Analytics*, https://www.ibm.com/topics/predictive-analytics
13. Kaspersky ICS-CERT, *Dark Chronicles: The Consequences of the Colonial Pipeline Attack*, https://ics-cert.kaspersky.com/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/
14. Microsoft Corporation, *Audience Targeting*,
15. https://about.ads.microsoft.com/en/tools/performance/audience-targeting
16. Microsoft Corporation, *Microsoft Digital Defense Report 2024*, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024
17. Microsoft Corporation, *What is Behavioral Analytics?*, https://www.microsoft.com/en-us/dynamics-365/topics/ai/customer-insights/what-is-behavioral-analytics
18. Tang, Jennifer; Saade, Tiffany; Kelly, Steve, *The Implications of Artificial Intelligence in Cybersecurity*, "Virtual Library Reports", October 2024, https://securityandtechnology.org/virtual-library/reports/the-implications-of-artificial-intelligence-in-cybersecurity/
19. TechTarget, *Colonial Pipeline Hack Explained: Everything You Need to Know*, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

20. Total Military Insight, *Historical Examples of Hybrid Warfare*, https://totalmilitaryinsight.com/historical-examples-of-hybrid-warfare/
21. Trend Micro, *Spear Phishing*, http://www.trendmicro.com/vinfo/us/security/definition/spear-phishing
22. Trend Micro, *What We Know About DarkSide Ransomware and the US Pipeline Attack,* https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html
23. The New York Times, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity,* https://www.nytimes.com/2021/05/12/business/economy/colonial-pipeline-economic-impact.html
24. *Types of Social Engineering Attacks*, Cybersecurity 101, https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/
25. *Wanna Cry Malware Trends*, https://any.run/malware-trends/wannacry
26. *What is Polymorphic Malware?*, https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-polymorphic-malware/
27. World Economic Forum*, AI and Cybersecurity: How to Navigate the Risks and Opportunities*, https://www.weforum.org/stories/2024/02/ai-cybersecurity-how-to-navigate-the-risks-and-opportunities/

Websites

1. https://any.run/
2. https://www.broadcom.com/
3. https://www.cloudflare.com/
4. https://www.crowdstrike.com/en-us/
5. https://www.csoonline.com/
6. https://www.cisa.gov/
7. https://www.fortinet.com/
8. https://hacknjill.com/
9. https://www.ibm.com/us-en
10. https://ics-cert.kaspersky.com/
11. https://www.microsoft.com/en-us/
12. https://www.rapid7.com/
13. https://www.sentinelone.com/
14. https://www.techtarget.com/
15. https://www.nytimes.com/
16. https://totalmilitaryinsight.com/
17. https://www.trendmicro.com/en_us/business.html
18. https://www.weforum.org/