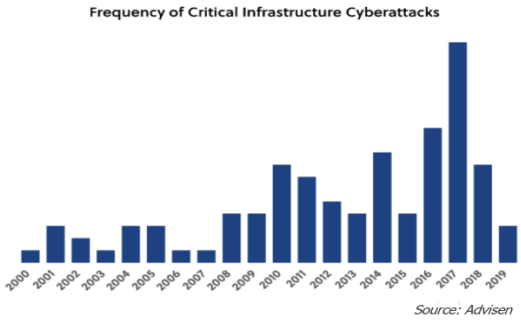
Leveraging Cyber Threats and National Security

FEYISAYO OGUNMADE
University of Louisville

Abstract- ***The more sophisticated and wide-ranging cyber-attacks present new threats to governments, critical infrastructures, and businesses across the world. National interest and public safety demand these dynamic hazards be understood for safeguarding. Cyber threats include APTs, ransomware, and cyber-espionage. The threats touch on economic stability, resilient infrastructure, military operations, and personal privacy, which put national security at risk. Despite the growing threat environment, the landscape of detecting, analyzing, and responding to cybersecurity threats has been changing through artificial intelligence. AI-based solutions detect abnormalities, trends, and threats swiftly and effectively in terms of security through state-of-the-art algorithms, machine learning, and predictive analysis. Soon, AI is predicted to aid cybersecurity experts in attack prediction, defense, and enhancing national cyber resilience. This research paper reflects on AI-led cybersecurity solutions and supports persistent research, investment, and collaboration on the front to tackle new cyberthreats.***

I. INTRODUCTION

In an age of digital interdependence, national security is under threat due to cyber assaults. With growing global interdependence, the dangers of cyberspace increase, leaving individuals, organizations, and governments exposed. The character of the need for a strong and flexible cybersecurity posture varies from state-sponsored attacks down to ransomware attacks. Cyberattacks also endanger critical infrastructure, financial systems, intellectual property, and sensitive information. In a globalized world, DDoS attacks, data breaches, and spying activities are considered nothing short of threats to national security. AI is the new frontier of cybersecurity in times of growing cyber threats. AI-powered systems, armed with brute algorithms, machine learning models, and predictive analytics, bring about accurate and timely identification of trends, anomalies, and emergent hazards like never before. Resulting from AI in cyberwar is an improvement in situational awareness and active defense for a cybersecurity practitioner (Sarker & Nowrozy et al., 2021).



The study comprises various objectives, which include describing the changeable nature and tactics of cyberattacks, how cyber threats affect economic resilience, infrastructure security, and geopolitical stability, and learning how AI-driven cyber protection systems are increasing threat detection, reducing incidents, and reducing risks. This discourse will help the readers navigate the labyrinth of cybersecurity, cyber warfare, innovation, and resilience. Cyberthreats and AI-powered solutions help readers identify with national security in a digital era. Proactive cyber defense is, therefore, a must, as the digital world keeps developing by the minute. AI-driven technologies, collaboration, and innovation could make for greater cyber resilience in the defense of democracy, liberty, and prosperity in the digital age (Taddeo & Floridi et al., 2019).

Background and Current State of Cyber Threats

As cyberspace continues to advance, cybercriminals become smarter, more relentless, and bolder. Cyberthreats have evolved from isolated incidents and enthusiastic hackers to a sly menace to national security and public safety. An individual must study the techniques used by cyber opponents, their objectives, and the far-reaching impact of their wicked activities to understand the current cyber threat picture. Malicious adversaries launch cyber weapons

for entry, harm, and theft of critical data from unsuspecting victims. Some of the cyber-attacks that are quite common, and devastating include ransomware, phishing, and DDoS attacks. The digital plague is ransomware, locking critical data and demanding money. This stealth cyberattack has attacked government, healthcare, international, and educational institutions. The Not Petya and WannaCry attacks on ransomware destroyed infrastructure, supply chains, and sensitive data globally at the cost of billions (Hodges & Creese 2015).

Other risks of cyber threats include phishing, which is the application of social engineering to defraud people with the objective of exposing them to sensitive information or clicking on dangerous links. Spear phishing includes various operations targeted at high-ranking governmental leaders, business executives, and, in some cases, even military officials through persuasive and targeted communications with the aim of stealing private information or even internal network hacking. Such kinds of attacks are called distributed denial of service attacks, targeting systems with a malicious traffic flood with the intent of rendering them inaccessible to genuine users (Margulies 2013). The worst cases were those of the botnets of hacked devices and systems that led to their disruption of services, financial losses, and erosion of public faith in digital infrastructure in financial institutions, online shops, and government organizations.

Cyber adversaries make use of disinformation and cyber-espionage, among other tactics, to disrupt government services, damage critical data, and attack democracy. Cyber threats are attacks on the critical infrastructure that provides power for energy, transportation, health, and finance and is required to be upheld in modern society. An attack on this infrastructure can destroy electricity, transportation, public safety, and national security. Cyberattacks could affect small and large private sector organizations across domains. Financial loss, reputational damage, regulatory penalties, or even risk to company continuity and stakeholder trust from a cyberattack on a private sector organization present various serious concern. The issue of national security and matters of public safety has come into sharp focus in the country over the past few days after a spate of high-profile cyber incidents. Russian state-sponsored hackers attributed the attack to the sophisticated SolarWinds supply chain, compromising sensitive information and eroding digital infrastructure confidence at a host of government agencies and commercial businesses (Zhou & Miao 2016, September).

The ransomware attack against the East Coast's petroleum supplies of the Colonial Pipeline by the DarkSide cybercrime group throws into focus the possible susceptibility of critical infrastructure to cyberattacks and the economic and social aftermath. State-sponsored espionage, sabotage, and propaganda have blurred the boundary between cyber combat and regular fighting (Hsiao & Kao 2018, February). Russian meddling in elections and Chinese cyber theft of intellectual property and sensitive government information are vivid examples of how, in modern times, nation-states are increasingly applying cyberspace for geopolitical rivalry and pressure.

The Evolution of Cyber Threats

Cyber threats change, evolve, and grow. From the first viruses and worms to state-backed cyber espionage and ransomware-as-a-service, cyber threats have matured right alongside technology and human ingenuity—both good and bad. In the past, cyber hazards used to originate from early digital viruses and worms spread via floppy drives and rudimentary networks. In 1988, Robert Tappan Morris developed the Morris worm; it infected thousands of computers and interrupted the internet, thereby prognosticating the modern state of cyberattacks. Armed with internet and digital technology penetration into every part of modern life, cyber threats used digital infrastructure and human psychological flaws. Attackers utilized psychology to deceive, manipulate, and exploit unsuspecting victims in phishing and spear-phishing campaigns (Orman 2003).

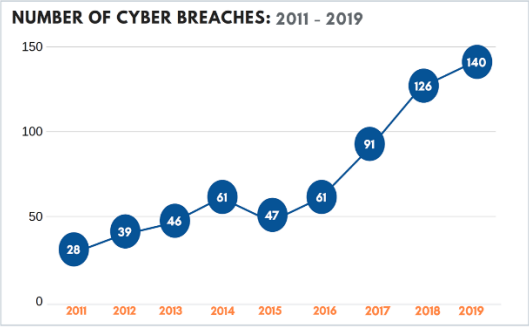
The rapidly growing statistics and trends for cyber-attacks that are increasingly complex point to a dangerous environment. According to the Verizon Data Breach Investigations Report (DBIR) 2021, 36% of the breaches were associated with phishing efforts, indicating methods of social engineering that may break through cybersecurity (Baker & Neal et al., 2011). In particular, ransomware-as-a-service (RaaS)

and crypto-enabled extortion have made it a huge threat to businesses and individuals. The COVID-19 pandemic has accelerated ransomware attacks on critical infrastructure, healthcare, and government agencies, precipitating a global disaster.

In recent years, states have indeed backed state cyber operations to carry out activities relating to sophisticated espionage, sabotage, and disinformation campaigns to support strategic aims and influence in online environments. Russian state-sponsored hackers targeted the SolarWinds supply chain, exposing vulnerabilities within the software supply chain and systems and compromising dozens of governments and private sector networks. This showed the systemic risks of cyberattacks in a connected world.

As the IoT, ML, and AI continue to scale up in cyberattacks, the demarcation lines between humans and algorithms will get increasingly blurred. By GANs and autonomous malware, an AI system could autonomously target flaws at a machine scale and speed, thus remaining undetected in cat-and-mouse games with human defenders (Henry & Brantly 2018). As cyber threats rise, the job of cybersecurity practitioners and politicians becomes to build defenses, predict assaults, and adjust national security and public safety. Experts identified that realizing cooperation, innovation, and investing in cybersecurity is the key tenet necessary for steering countries in cyberspace, guaranteeing sovereignty, security, and resilience in the digital era.

Cyber threats are only growing in complexity, obscurity, and deadliness with the digital frontiers' explosion. Cyberfoes are potent, persistent, and ever-changing, menacing modern civilization through the dark web and capitals of the globe.



National Security Implications

National security is underpinned by stable economies that possess sophisticated financial systems, supply networks, and digital economies. Cyber-attacks induce a lot of disruption to commerce, business, and investment, thus leading to the destruction of consumer confidence. Financial institution cyberattacks like data theft or even online banking outages may trigger the perception of a financial crisis, reduce the trust of investors, and plunge global economic results into losses.

Another front line of our critical infrastructure, such as energy, transportation, healthcare, and telecommunications, where these different forms of conflict called cyberwar can potentially wreak havoc. The critical infrastructure of electrical grids, transportation, healthcare systems, and even emergency services—all are potential targets for hacking that could create fear and death. Cyberspace could be a potential threat to the military effort for the defense of national sovereignty as well as any international threats. It could play a hindering role in military command and control, intelligence gathering, and even logistic support. A drop in operational effectiveness, falling short of mission goals, and strategic advantage in conventional, hybrid, and asymmetric warfare are potential issues that result from cyber-attacks on military infrastructure (Hodges & Creese 2015).

Cyberattacks against critical services and infrastructure pose threats to the safety of democracy and social cohesiveness. They enable disruptions of emergency services, first responders, health care, and transportation networks in an instant, impinging upon public safety. A cyberattack on traffic control and emergency response systems could cause an accident in many places around the world, causing injuries or death. If left unmanaged, such emerging threats could cause destruction to societies in the real world. The inability to counter the cyber threat could ruin economies, infrastructure, military capability, and public safety, and it could also imperil national security and the social compact between governments and communities. Cyber threats put trust, confidence, and resilience in peril; undermine democratic governance; deepen social inequality; and contribute

to a digital age of dread, uncertainty, and insecurity (Margulies 2013).

Role of AI-driven Technologies in Cyber Threat Intelligence

Cybersecurity requires innovation and adaptation to stay ahead of threats. AI and ML are going to revolutionize the world of digital cyber-threat intelligence and security. We picture a research inquiry of the latest AI and ML methods, applications, and effects for the newly emerged capacity to reveal, evaluate, and lessen risks in cyberspace with unparalleled speed, precision, and correctness. AI helps cybersecurity defenders go through big data sets, find patterns in them, and act on digital noise. Machine learning, a part of AI, is the ability of computers to learn from experience, adjust to new data, and make predictions or decisions without being programmed. It becomes ideal for the dynamic and adversarial kind of cyber warfare (Sarker & Nowrozy et al., 2021).

AI is necessary for anomaly detection in large sets of data, while ML algorithms are required for this in cyber threat intelligence. Signature-based and static rule-based cybersecurity cannot keep track of cyber threats, as means of attack are variable. Yet anomaly detection might find new threats and zero-day vulnerabilities, thereby cutting chances for undetected breaches and decreasing the impact on businesses and individuals from cyberattacks. Predictive analytics makes the firm foresee dangers, trends, and vulnerabilities before they turn into assaults. Predictive analysis is defined as the process of analyzing past data, correlating indicators, and predicting events likely to happen in the future. Predictive analytics can turn reactive cybersecurity into proactive risk management in that, with it, one can predict phishing attacks on user demographics or the outbreak of a virus affecting the linked networks (Taddeo & Floridi et al., 2019).

Cyber threat intelligence can be imbued with natural language processing (NLP), which is a part of AI that explores human-computer communication. NLP algorithms look for cyber threats, language patterns, and moods in unstructured text data, mostly from threat reports, social media feeds, and dark web forums. This helps businesses learn about new threats and how attackers usually do things. NLP-powered chatbots and virtual assistants may speed up incident response and communication under duress.

Graph-based analytics is a new field in AI-enabled cyber threat intelligence that lets you see and analyze complex dependencies and links in linked datasets like supply chain relationships, network traffic logs, and social media interactions. This analytic capability is possible through graph-based analytics, which could help in discovering hidden patterns, clusters, and anomalies. These anomalies may serve as precursors to some malicious or hostile behavior by modeling interacting entities as nodes and edges in the network graph (Zheng & Zhao et al., 2022). In an ever-connected world, graph-based analytics identify hidden communications networks used by fraudsters while mapping the distribution of malware to devices to put cyber risks into perspective and highlight areas for priority remediation. AI-powered cyber threat intelligence technologies take digital protection and resilience standards much further. Incorporation of machine intelligence in the cyber threat environment will empower the security experts in the company with heightened situational awareness, prediction, and response agility. Moreover, AI-based cyber threat intelligence will have the power to democratize advanced security capabilities, which in turn will empower all scales of organizations with resources to guard themselves from cyberspace attacks (Ansari & Yathiraju et al., 2022).

Case Studies

Numerous real-world and hypothetical case studies demonstrate the usefulness of AI-driven technology in identifying and mitigating cyber threats in the ever-changing cybersecurity scene. AI-powered solutions can detect sophisticated malware campaigns, identify insider threats, and mitigate ransomware attacks, improving cyber defense capabilities and protecting organizations from cyberspace threats. We examine AI-driven technologies' practical advantages in fighting cyber-attacks and strengthening digital resilience via case studies and hypothetical scenarios.

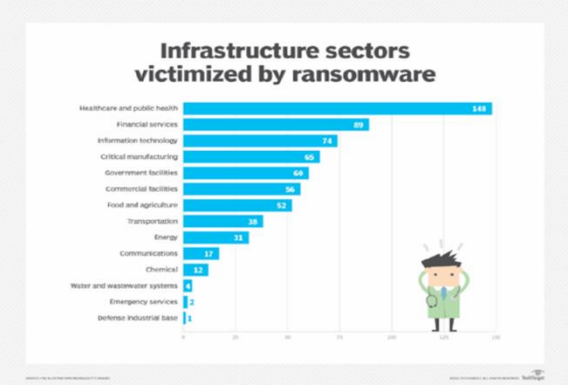
The Stuxnet Worm

Researchers discovered Stuxnet, a highly sophisticated cyberweapon, in 2010. It could utilize several zero-day vulnerabilities to annihilate centrifuge controllers at the nuclear enrichment

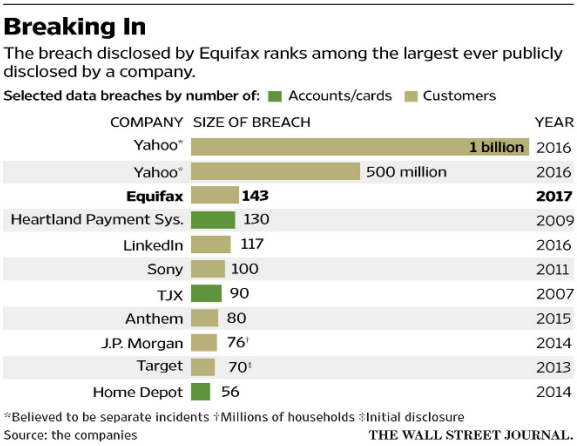
facilities in Iran, thus bringing to a standstill the country's nuclear program altogether. Thus, Stuxnet epitomizes the combining of both cyber and kinetic warfare, hence showing the necessity for effective detection of threats to sophisticated, targeted operations that are intended to be annihilated (Karnouskos 2011, November).

Just imagine a country using some AI-based system to detect threats to critical infrastructure at the country level and protect them from cyberattacks. These help in the real-time detection of Stuxnet-like cyber-attacks from its algorithms, which engage strong machine learning and behavioral analytics. AI-based measures of protection interconnect the symptoms of compromise and conduct their analysis at the scale of network data to mitigate sabotage and other offenses against national security and key services.

The WannaCry ransomware attack:
In 2017, a Windows vulnerability helped WannaCry compromise more than 200,000 PCs in 150 countries. The breach had Bitcoin ransoms on critical data, including attacks on healthcare, banking, and government systems (Hsiao & Kao 2018, February). The fast propagation of WannaCry underlined the need to find and kill ransomware proactively before it can cause such catastrophic loss. For instance, imagine a company integrated with AI-driven endpoint security that can detect ransomware. In this case, the malware detection solution employs learning models based on wide databases of malware samples and conducts behavior analysis, thereby detecting and preventing any possible attacks on spreading or encrypting the targeted critical data. AI-powered defenses scrutinize the behaviors of files, system activities, and network traffic in terms of the execution of ransomware payloads, which in turn saves money, reputation, and downtime for organizations.



The Equifax Data Breach was a significant event that had far-reaching consequences:
In 2017, hackers breached Equifax, one of the giants in the field of credit reporting in the United States, exposing data from over 147 million people. Attackers then utilized the source code and guidelines for Apache Struts applications to steal Social Security numbers, birth dates, and bank information (Wang & Johnson 2018). In the case of the hack against Equifax, it showed how monitoring vulnerabilities and ensuring subsequent patching reduce cyber risk, therefore protecting sensitive data. Equifax could potentially use an AI-driven vulnerability management solution to identify and repair security weaknesses present in its digital infrastructure. The firm can enable the patching of critical vulnerabilities in advance of actual attacks by allowing prioritization for patching based on severity of risk, exploitability, and effect using machine-learning algorithms trained on historical vulnerability data and threat intelligence feeds. Automating the review and prioritization of vulnerabilities and repairs by AI-powered defenses to reduce both data breaches and regulatory penalties against Equifax's cyber resilience.



Insider Threat Detection:

In 2013, an NSA employee, Edward Snowden, disclosed classified documents that unveiled the massive surveillance exertions of the NSA and its foreign associates. The revelations by Snowden underpinned the insider threat from trusted workers and contractors with privileged access to sensitive material and stated the need for advanced insider threat detection capabilities to identify and close classified data breaches (Branum & Charteris-Black 2015). A case in point: a government agency using AI-driven UBA to detect insider risk. The systems detect deviant activity by using machine learning algorithms trained on previous user behavior data, in addition to contextual information, to access usage and communication patterns. AI-powered defenses connect strange behavior with risk indicators like job status and access credentials and pick out odd actions that need to be investigated further. This keeps important data safe from threats from insiders.

Challenges and Limitations of Implementing AI-Driven Solutions in Cybersecurity:

AI has revolutionized cybersecurity and consequently improved human potential in combating cyber threats. Some AI-driven cybersecurity solutions have negatives. Challenges surrounding data privacy, the need for big data for training, and the risk of AI being used nefariously by bad actors to secure their digital assets and security with AI must be addressed by firms. The first section investigates the challenges of embracing AI-based cybersecurity solutions and proposes ways of reducing risks while increasing the benefits of cyber defense with AI (Henry & Brantly 2018).

Data privacy concerns:

Data privacy problems are a roadblock to AI-driven cybersecurity. AI algorithms use large datasets to learn and predict, an issue that has caused concern over data privacy and security. AI-powered solutions may be reliant on network traffic records, activity patterns of users, and feeds for threat intelligence to detect and mitigate cyber threats. Such information thus gives rise to the ethical and legal questions of data privacy, consent, and GDPR and CCPA compliance about the collection, retention, and processing of the data. Enterprises need to architect the data governance mechanisms and policies of privacy within their domains to have responsible AI use for cybersecurity. Other possible measures to stop unwanted access might include anonymization or pseudonymization of sensitive data before training models, reducing the collection and retention of data, and securing data in transit and at rest using encryption. Data privacy and privacy by design in AI-based cybersecurity solutions help build the trust of stakeholders toward a business organization and show commitment to protecting sensitive data (Orman 2003).

The Importance of Large Datasets for Training:

Furthermore, AI-driven cybersecurity solutions face the challenge of handling huge and diverse datasets that are necessary for training models in an AI environment. AI systems but deep learning models, require large amounts of labeled dataset training in order to understand intricate data patterns and provide accurate predictions or classifications. Generally, the cyber threat data at hand is rare, imbalanced, and noisy, which makes it hard to train AI models that generalize well over such diverse and evolving threats. Data augmentation, transfer learning, and synthetic data generation might, however, help cybersecurity organizations enhance the variety and representativeness of their training datasets to overcome some limitations of the dataset. Rotation, scaling, and noise injection enhance the training datasets. Transfer learning uses pre-trained models on massive datasets like natural language processing or computer vision to bootstrap AI models on cybersecurity concerns with little data. Because of this, generative methods based on generative models or simulation can make up for the lack of training data by giving companies generated data samples that can

help them make good cybersecurity AI models (Margulies 2013).

Potential for AI Exploitation by Malicious Actors:
The third challenge lies in adversaries who make use of AI to evade detection or manipulate AI systems in doing attacks themselves. Through the full spread of AI technologies in cybersecurity, cyber attackers have been learning to exploit AI system flaws and overcome AI-powered defenses. Attackers manipulate the training or inference data by adding adversarial motivated inputs or pert method modifications, aiming to influence the decision-making of AI systems and act against AI-based cybersecurity solutions. The use of strong authentication, limitation of access, and monitoring should serve as a barrier to any hostile actor attempting to use AI, and indeed, they may help to identify and respond to suspicious behavior of AI systems (Zheng & Zhao et al., 2022). This could include making models explainable and interpretable to make AI decision-making more open and accountable, checking AI systems for flaws and bias, and finding and stopping adversarial attacks in real time. The best practices in AI security can protect AI-driven cybersecurity solutions from being misused.

Interpretability and explainability of AI models:
The fourth barrier to AI-driven cybersecurity solutions is the interpretability and explainability of AI models—especially in cases where mission-critical applications require human intervention and their accountability. Cybersecurity practitioners have difficulty understanding AI decisions and predictions because AI algorithms, such as deep neural networks, are opaque. Model opacity and inexplicability render it difficult to test the insights, repair errors in the models, and justify AI-driven decisions to stakeholders, reducing trust, transparency, and accountability in cybersecurity operations.

They are featuring visualization, attribution, and post-hoc explanation, among others, that may make the cybersecurity model understandable and explainable by helping to clarify the AI model and its decisions to the human analysts. Cybersecurity experts can apply t-SNE and PCA to the analysis of high-dimensional data and to input feature-model prediction correlations. It serves to attribute input features to the contributions behind model predictions and, thus, reveal factors driving decisions resulting from AI algorithms (Henry & Brantly 2018). Both decision trees and rule-based systems enable cybersecurity professionals to provide AI-driven insights, explainable in human language, for further use in real life.

Security organizations that focus on model interpretability and explainability as components of AI-driven cybersecurity offerings enable businesses to increase human understanding and confidence in AI-driven decisions, the cooperation of the analyst with the AI system, and cybersecurity responsibility and transparency overall. AI models that can be understood and explained might help make AI-powered cybersecurity systems less likely to make mistakes, have unintended effects, or be biased. This will make them more reliable and protect them from cyberattacks (Razzaq & Masood et al., 2013, March).

Scalability and resource constraints:
This limitation may, however, occur where the scalability and resource restrictions of either resource-poor computer situations or enterprises with poor computer resources or technical skills will not allow adoption of an AI-driven cybersecurity solution. Deep learning models require computing power, hardware acceleration machines, machine learning, and data science capabilities to train and deploy as AI algorithms. Large-scale AI-driven solutions will have infrastructural, deployment, and operational overhead for small to medium-scale cybersecurity firms, which would have both financial and technical constraints (Abu & Yusof 2018).

This leads to the democratization of AI technologies, as it will bring down the adoption hurdle for many less capable and knowledgeable enterprises to be able to afford, develop, and integrate AI. This way, organizations can design and deploy AI-driven cybersecurity solutions using on-demand computational resources and scalable storage from AWS, Azure, and GCP. Amazon Sage Maker, Azure Machine Learning, and Google AI Platform manage infrastructure to the point of providing a pre-configured environment and toolchain to design, train, and deploy models, so that it frees the enterprise to handle AI-driven cybersecurity.

Given this, AI services, especially in the areas of cloud and open-source frameworks, can scale organizations in deploying AI-driven cybersecurity solutions to tap into the disruptive potential of AI in the identification, assessment, and mitigation of cyber threats. All the above clearly states that the use of cloud-based AI solutions enables the organization to raise strong cybersecurity defenses in this digital era with flexibility, agility, and scalability to respond to evolving cyber threats and business demands (Shabut & Hossain et al., 2016, December).

Recommendations for Enhancing National Security

Government, business, academia, and civil society must work together to improve national security in cyberspace's dynamic and interconnected terrain. In the face of evolving cyber threats and rapid technological innovation, AI-driven technologies can improve national security efforts to protect critical assets, preserve sovereignty, and uphold democratic values. This review outlines concrete methods for politicians, cybersecurity experts, and the tech industry to use AI to improve national security and address digital age concerns.

Foster collaboration between the public and private sectors:

National security guidelines allow public-private collaboration and information sharing. From business, government, and universities, among others, there is a need for collaboration in being able to detect, analyze, and manage organizational and jurisdictional cyber threats. Policymakers should, therefore, support public-private partnerships, the sharing of information, and platforms that can enable the sharing of threat intelligence, best practices, and actionable insights. Governments should, therefore, encourage research and development in cybersecurity by the private sector through tax incentives, subsidies, and regulation. The environment should be one in which the stakeholders from the public and commercial sectors are aligned with each other and able to trust one another as they seek to enhance their cyber resilience and responsiveness, hence securing the nation and its prosperity in cyberspace (Zheng & Zhao et al., 2022).

Invest in cybersecurity research and development:

"Cybersecurity R&D catalyzes innovation, supports national security, and develops technology to defend against cyber threats. Governments should therefore fund foundational and applied research, interdisciplinary collaboration, and the sharing of ideas amongst academics, engineers, and practitioners to promote the security of cyberspace, AI, and related domains. Research institutes, innovative hubs, and collaborative consortia should be set up to fast-track the development of cyber threat solutions. Investments in cybersecurity R&D and the creation of an innovation ecosystem of talent and knowledge are needed for nations to be at the forefront of cybersecurity innovation and resilience in the era of the digital revolution (Henry & Brantly 2018).

Enhance Cybersecurity Education and awareness:

The third national security initiative is letting lawmakers, cybersecurity professionals, and the public at large know about the issues in cybersecurity. A very strong and secure society needs an awareness of cybersecurity that can help in the detection, prevention, and response of cyberattacks. And thus, there should be an emphasis on cybersecurity education and training from the basic to the college level so that students can be educated for the future generation of the digital environment. The policymakers should work together with various industry organizations, non-profits, and community groups to develop campaigns, outreach programs, and educational material for increasing awareness of the dangers of cyber, as well as best practices understood in cybersecurity hygiene. Ultimately, this will act as a defense for individuals and businesses from cyber threats due to investment by the government in education and awareness (Razzaq & Masood et al., 2013, March).

Strengthen legal and regulatory frameworks:

The fourth issue of national security of great importance is the perfecting of the legal and regulatory framework for counteraction against cyber threats, protection of critical infrastructure, and preservation of digital sovereignty. We require comprehensive cybersecurity laws and regulations, standards and processes, and enforcement mechanisms that safeguard critical assets, secure sensitive data, and reduce threats across sectors. Governments are

therefore expected to subscribe to the development and adoption of cyberspace laws, norms, and responsible behavior agreements with international partners as mechanisms for enhancing trust, cooperation, and stability in the global cyber ecosystem. This, in addition to the need to channel funds for law enforcement, judicial training, and international coordination in the battle against cybercrime, punishing bad actors, and deterring state-sponsored cyberattacks, A stronger legal and regulatory framework in the digital world would provide a catalyst for cybersecurity innovation, investment, and collaboration, thus enhancing national security and resilience (Abu & Yusof 2018).

Promote ethical and responsible AI development:
The fourth challenge is to get the legal and regulatory framework right regarding above issues such as the definition of cyber threats, vital infrastructures, and digital sovereignty. What should be in place is the set of well-articulated laws and regulations in cybersecurity that will contain both rules, standards, and protocols, and the enforcement that protects our key assets, sensitive data, and mitigates threats in all industries. Governments are therefore expected to subscribe to the development and adoption of cyberspace laws, norms, and responsible behavior agreements with international partners as mechanisms for enhancing trust, cooperation, and stability in the global cyber ecosystem (Shabut & Hossain et al., 2016, December). This, in addition to the need to channel funds for law enforcement, judicial training, and international coordination in the battle against cybercrime, punishing bad actors, and deterring state-sponsored cyberattacks, A stronger legal and regulatory framework in the digital world would provide a catalyst for cybersecurity innovation, investment, and collaboration, thus enhancing national security and resilience.

CONCLUSION

National security requires an energetic, multidimensional policy that includes innovation, collaboration, and adaptation to rising cyber threats. This report probed cyber dangers and provided digital national security solutions. By implementing public-private sector collaboration, investing in research and development in cybersecurity, increasing awareness of cybersecurity, boosting the legal and regulatory frameworks, and also promoting the development of ethical and responsible AI, nations are able to come up with defenses in cybersecurity that are resilient, adaptive, and secure in nature, therefore protecting the assets critically and inculcating sovereignty and democratic ideals (Zhou & Miao 2016, September).

Such projects' developments are driven by the belief that AI will revolutionize cybersecurity. AI assists defenders in finding, assessing, and removing cyber threats quickly, accurately, and precisely. AI will help transform the application of anomaly detection and predictive analytics in natural language processing and graph-based analytics in the digital era (Hsiao & Kao 2018, February). AI supports governments in predicting and reacting, as well as protecting against cyber-attacks. Safe and strong cyber futures are not easy to achieve. From data privacy problems and the need for huge datasets for training to AI exploitation by the same kind of hostile actors to AI model interpretability and explainability, there are numerous challenges businesses must surmount to fully harness AI's cyber-defense potential. " Working collaboratively to drive innovation and being ethical stewards in these matters will allow governments to overcome these challenges and make way for a better and more secure tomorrow for all.

Finally, these are key to understanding and countering quickly evolving cyber threats. With technology and smart adversaries, these stakes are higher than ever. AI-based technologies and probably knowledge and creativity from cross-sectors will guide nations to handle the challenges of the digital age with confidence, resilience, and determination. Working together can make cyberspace secure, resilient, and valuable to everybody.

REFERENCES

[1] Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of conflict and security law*, *17*(2), 229-244. https://academic.oup.com/jcsl/article-abstract/17/2/229/852823

[2] Margulies, P. (2013). Sovereignty and cyber attacks: Technology's challenge to the law of

state responsibility. *Melbourne Journal of International Law*, *14*(2), 496-519. https://search.informit.org/doi/abs/10.3316/INFORMIT.117621131187624

[3] Hodges, D., & Creese, S. (2015). Understanding cyber-attacks. In *Cyber Warfare* (pp. 33-60). Routledge. https://books.google.com/books?hl=en&lr=&id=yFKsCQAAQBAJ&oi=fnd&pg=PA33&dq=state+of+cyber+attacks&ots=ve0DUiAW4V&sig=4arpqXVRi2oDFwSRiktERIoAB_c

[4] Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371-379. https://www.academia.edu/download/70021757/8222.pdf

[5] Henry, S., & Brantly, A. F. (2018). Countering the cyber threat. *The Cyber Defense Review*, *3*(1), 47-56. https://www.jstor.org/stable/26427375

[6] Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, *8*(4), 422-435. https://www.sciencedirect.com/science/article/pii/S235286482100047X

[7] Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: a case study of the Equifax data breach. *Issues in Information Systems*, *19*(3). https://iacis.org/iis/2018/3_iis_2018_150-159.pdf

[8] Branum, J., & Charteris-Black, J. (2015). The Edward Snowden affair: A corpus study of the British press. *Discourse & Communication*, *9*(2), 199-220. https://journals.sagepub.com/doi/abs/10.1177/1750481314568544

[9] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*, 1-18. https://link.springer.com/article/10.1007/s42979-021-00557-0

[10] Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557-560. https://www.nature.com/articles/s42256-019-0109-1

[11] Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *International Journal of Advanced Research in Computer and Communication Engineering*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323317

[12] Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. *Cyber, Intelligence, and Security*, *1*(1), 103-119. https://www.academia.edu/download/52464497/Artificial_Intelligence_in_Cybersecurity.pdf

[13] Orman, H. (2003). The Morris worm: A fifteen-year perspective. *IEEE Security & Privacy*, *1*(5), 35-43. https://ieeexplore.ieee.org/abstract/document/1236233/

[14] Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C., ... & Neal, C. (2011). 2011 data breach investigations report. *Verizon RISK Team, Available: www. verizonbusiness. com/resources/reports/rp_databreach-investigationsreport-2011_en_xg. pdf*, 1-72. https://www.wired.com/images_blogs/threatlevel/2011/04/Verizon-2011-DBIR_04-13-11.pdf

[15] Karnouskos, S. (2011, November). Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society* (pp. 4490-4494). IEEE. https://ieeexplore.ieee.org/abstract/document/6120048/

[16] Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013, March). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)* (pp. 1-6). IEEE.

https://ieeexplore.ieee.org/abstract/document/6513420/

[17] Zhou, Y., & Miao, Z. (2016, September). Cyber attacks, detection and protection in smart grid state estimation. In *2016 North American Power Symposium (NAPS)* (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/7747874/

[18] Shabut, A. M., Lwin, K. T., & Hossain, M. A. (2016, December). Cyber attacks, countermeasures, and protection schemes—A state of the art survey. In *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)* (pp. 37-44). IEEE. https://ieeexplore.ieee.org/abstract/document/7916194/

[19] Hsiao, S. C., & Kao, D. Y. (2018, February). The static analysis of WannaCry ransomware. In *2018 20th international conference on advanced communication technology (ICACT)* (pp. 153-158). IEEE. https://ieeexplore.ieee.org/abstract/document/8323680/