Artificial Intelligence

oC

Embracing positive aspects of technology to encourage and enhance innovation.



D

FORWARD

BY PATRICK GAUL

As the rapid development of artificial intelligence (AI) continues to produce new opportunities to improve nearly every industry, the National Technology Security Coalition (NTSC) believes that AI should be legislated, not regulated, to encourage and enhance innovation. Al is the future, and we at the NTSC want to embrace the positive aspects of that future, but we also recognize that it needs to be governed with an eye for the collective good. The best way to do this is to enable the private and public sectors to engage in an open, active, and ongoing dialog. It will not be just one conversation but countless conversations spanning decades. It should be bipartisan and inclusive of different perspectives. There is not one right answer for the situation, which is complex and nuanced and will change as AI changes. You will see in this white paper that AI will take on many forms, and those forms will warrant different solutions. It is vital to ensure that future conversations are unencumbered by partisanship and fear-mongering, but instead, they should be welcomed by open mindedness and logic. I believe we can do this, but we must all work together, for together we are stronger.

TABLE OF CONTENTS

Introduction Section One: Where is AI Today?		3	
		3	
•	What is AI?	3	
•	What are the Kinds of Al	4	
•	What is Possible Today with Alin Cyber?	4	
Section Two: What's Happening with AI Globally?		5	
•	In the US	5	
•	In the EU	5	
•	In Asia (with a focus on China)	6	
Section Three: What Are the Benefits of AI in Cyber?		7	
•	Increased Efficiency and Productivity	7	
•	Enhanced Data Analysis and Insights	7	
•	Improved Accuracy and Reduced Errors	8	
Section Four: What AI Tools Are in Play Today?		8	
•	NVIDIA	8	
•	Google Al	8	
•	OpenAl	9	
Section Five: What Does the Future Look Like for AI?		9	
•	Advanced Cybersecurity Defense	9	
•	Personalized Experiences and Solutions	10	
•	Enhanced Automation and Robotics	11	
Conclusion		12	

INTRODUCTION

The <u>concept</u> of AI is thousands of years old, but not until the mid-20th century did humans have the computing

did humans have the computing power to make theoretical ideas about nonhuman machines come alive. Over the past 75 years, AI has matured from a computer program that plays checkers to common tools of daily life in the internet era: search engines, voice assistants, and autonomous robots. While the future of AI is unknown, it is being written every day, with every advancement in neural networks, machine learning algorithms, data processing, and more.

How should organizations make sense of Al? One way is to understand that it will absolutely change your industry. Still, it will most likely happen in fits and starts, with advancements and retrenchments, slowly and steadily, until one day you realize that the AI technology underpinning our world is 10x more powerful than it was five years-or even one year-ago. The exact speed at which AI will grow and evolve depends on which expert you follow. They all have various predictions for adoption levels. Our goal is not to predict the speed of adoption but to help you survive and thrive in this environment, which requires a clear understanding of what's happening and what's important. Our white paper will dive into where AI is today, what the global landscape is, what the main benefits of AI are, what the top tools are in industry today, and we end with immediate future might look like for AI. So, where is society today when it comes to AI?

SECTION ONE: Where is AI Today?

The field of AI is booming, spurred by rapid advancements across various technologies, and with great implications for multiple industries. Machine learning, a powerful subset of AI, utilizes sophisticated algorithms to learn from data and make predictions, which powers applications in self-driving cars and medical diagnosis tools. Deep learning, a specific type of machine learning, utilizes artificial neural networks to mimic the human brain's functionality, enabling tasks like natural language processing (NLP) and image recognition. As these areas of AI develop, they open doors to incredible possibilities, from personalized healthcare and automated manufacturing to climate change mitigation and space exploration.

What is AI?

In general, AI refers to the ability of machines to simulate human intelligence processes. For a long time, machines have far exceeded the human capacity for capturing, organizing, sorting, computing, and even analyzing raw data at scale. The next major step is for machines to learn from and reason with data to solve problems, predict outcomes, and make decisions. This is why, under the <u>AI umbrella</u>, machine learning and deep learning are the subsets that enable all advances!



What are the Kinds of AI

There are three distinct types of AI that we will cover in this white paper:

- Artificial Narrow Intelligence Today, the reality is that all AI remains purely theoretical, except for a kind of AI called Artificial Narrow Intelligence, or "Weak AI." This means that the AI exists strictly within the boundaries of its single, defined task. Examples are voice assistant tools like Siri and Alexa or chatbots like OpenAI's ChatGPT and Google's Gemini. Within narrow AI, these chatbots can be further classified as instances of Generative Artificial Intelligence (GenAl or GAI) for their ability to use prompts to generate text, images, and videos. This functionality is enabled by a type of artificial neural network called large language models (LLMs), which use NLP to determine the probability that, for instance, the next word in a sentence will be
- General AI (theoretical) When you exchange messages with ChatGPT, you may feel you're living in the future. But you're still living in the world of Narrow AI because a human is training the underlying learning models. Once machines can learn, develop, and execute new skills outside their original without human intervention, we will have reached the state of General AI.
- Super AI (theoretical) When General AI takes another leap into developing emotions and belief systems and acting on them in other words, when machines innately learn to reason and make judgments and consequential decisions for the human-based world—we will have achieved the third kind of AI, Super AI, where human and machine become less distinguishable.

In this paper, AI always refers to Artificial Narrow Intelligence (aka GAI) unless we explicitly state otherwise. Again, this is ChatGPT or what most of us are familiar with when we experience AI today.

What is Possible Today with Al... in Cyber?

Regarding cybersecurity, AI is one more tool in a cyber bad actor's toolkit. But there is one big difference between this tool and others: unprecedented speed, power, and efficiency—plus a few new tricks. For instance, cyber bad actors still use social engineering to access accounts, steal money and data, and compromise systems with malware. But now those cyber bad actors can use AI chatbots to quickly and easily create more compelling phishing emails and authenticlooking fake websites. They can use AI tools to increase their attack's scale, intensity, and flexibility, and they can automate elements of their attacks,

making it extremely hard for traditional defenses to keep up. Bad cyber actors can also use AI to create deepfakes—fake audio and video content that the human eye and ear recognize as real—to supplement and enhance their attacks.

Both bad and good actors are using AI, but we must ensure companies are allowed to develop and stay steps ahead of bad actors.

Yet AI can also improve

cybersecurity defense measures using the same logic of speed and power. The ability to automate the scope of threat detection and response will continue to increase as AI learns to analyze massive amounts of data faster and more accurately. Identifying suspicious activity, malware patterns, and potential <u>vulnerabilities</u> are already tasks for sophisticated software. AI will only increase the ability to detect zero-day threats and emerging attacks in real-time, automate incident response, and prioritize vulnerabilities for patching. AI can analyze user behavior <u>patterns</u> to identify potential insider threats and prevent unauthorized access. Altogether, these capabilities will significantly reduce the risk of successful cyberattacks.

As you can see, both bad and good actors are using AI, but we must ensure companies are allowed to

4

develop and stay steps ahead of bad actors. To do so, AI will need support and incentives through strategic legislation that allows AI innovation to flourish. This is where bad actors have an advantage over good actors, they aren't held back by legislative bodies. They are free to push the envelope. Let's consider that as we look at what's happening with AI globally.

SECTION TWO

What's Happening with Al Globally?

As AI adoption and advancements surge globally, governments increasingly recognize the economic potential, with one estimate suggesting AI could contribute \$15.7 trillion to the economy by 2030. However, AI could also negatively impact economies worldwide by displacing jobs. One study found that in May 2023, AI was responsible for eliminating 4,000 jobs. AI algorithms can also potentially disrupt societies and marketplaces in the form of biases, hallucinations (when an AI model generates inaccurate or misleading information that appears to be true), and other issues we can't yet imagine or predict.

To balance the rapid pace of this transformative technology, governments around the globe are legislating AI. This usually <u>begins</u> with a national strategy around AI ethics, which considers various policies and laws to help AI innovation flourish while mitigating potential risks. At least <u>24</u>. <u>countries</u> have AI legislation in place, with a few standing out as leaders in AI development and policy. We want to focus on the US, the European Union (EU), and China.

In the US

Overview of the AI Landscape

The US is the global AI leader, buzzing with AI activity and <u>attracting</u> more elite AI talent than any other country in the world. Open-source models like Meta's LlaMa and OpenAI's GTP-4/ DALL-E 3 have made powerful text and image generation tools accessible, and the most powerful tech companies in the world – <u>Microsoft</u> and <u>Alphabet</u> – are now positioning themselves as AI companies. Altogether, of the world's top AI institutions, 60% are in the United States, 35% of global AI companies <u>are in</u> the US, and the US is home to <u>thousands</u> of AI startups.

Overview of AI Legislation

In the US, there is no federal legislation or regulation for AI. However, legislators have proposed dozens of bills, numerous bills are moving through state legislatures, and the federal government has issued various frameworks and <u>guidelines</u> for AI, including a 2019 executive order from the white house dedicated to maintaining the country's AI advantage. More recently, the fall of 2023 saw a flurry of Al-related events, with the Senate holding the first of nine unprecedented closed-door "<u>Al Insights</u>" forums with Al industry leaders. In October 2023, the latest AI executive order from the white house directed more than 50 federal entities to take more than 100 specific actions to implement the guidance set forth across eight overarching policy areas, including safety and security, innovation and competition, and the federal use of AI. And December 2023 saw the settlement of a landmark case, with the Federal Trade Commission (FTC) banning Rite Aid from using AI facial recognition technology for surveillance purposes for five years, settling charges that the retailer failed to implement reasonable procedures and prevent harm to consumers.

In the EU

Overview of the AI Landscape

Europe is a significant global player in AI, with about <u>150 startups</u> harnessing the power of AI to develop new products. The United Kingdom is the runaway leader in the space, with 48 companies, while Germany is not far behind with 27. Londonbased <u>Snythesia</u> is an AI-powered video maker with clients like Reuters, Accenture, Amazon, and the BBC, while Germany's <u>Aleph Alpha</u> is a platform to help businesses and governments develop AI tools and research. France is also attracting AI talent: <u>Mistral AI</u> is the country's rival to the US-based OpenAI (which developed ChatGPT) and <u>Poolside AI</u>, which powers software development, which <u>relocated</u> from California to Paris after raising over \$100M funding and is now

Europe is a significant global player in Al, with about 150 startups harnessing the power of Al to develop new products.

Overview of Al Legislation The EU plans for Al began in 2019 with the Coordinated Plan on Artificial Intelligence, which aimed to accelerate Al investment. More recently.

seeking a \$2B valuation.

the landmark <u>EU AI Act</u>,

which began to be implemented in May 2024, set a global precedent for AI regulation by establishing a comprehensive risk-based framework for AI application development. The EU AI Act establishes four levels of risk: minimal, limited, high, and unacceptable, "unacceptable" risks from AI systems are defined as ones where the application could cause a person significant harm by exploiting their vulnerabilities, using manipulative, deceptive, or subliminal techniques to influence them; or using real-time biometric data in a law enforcement capacity. The EU AI Act focuses on ethical considerations alongside continued investment in Al research and innovation through initiatives like Horizon Europe. Horizon Europe aims to position the EU as a leader in shaping a future where AI innovations benefit society. That said, legislation like the <u>AI Liability Directive</u> is designed to address potential harms from AI. And across from mainland Europe, the UK has taken a decidedly pro-innovation approach to AI regulation. Prime Minister Rishi Sunak stated in a landmark speech in October 2023, "the future of AI is safe AI. And by making the UK a global leader in safe AI, we will attract even more of the new jobs and investment that will come from this new wave of technology." To achieve this, the UK is investing substantially in Al.

In Asia-with a focus on China

Overview of the AI Landscape

Like the US and the EU, Asia, particularly China, is witnessing a surge in AI advancements, with a strong focus on AI tools. Government initiatives and substantial investments are fueling research and development in this area. Healthcare is a prime example, where AI is used for early disease detection, personalized medicine, and patient care management; AI also plays a critical role in China's military <u>modernization</u> strategy. In terms of attracting AI talent, China has expanded its domestic AI talent pool over the last few years. The percentage of the world's top AI researchers from China rose from 29% in 2019 to 47% in 2022.

Overview of Al Legislation The foundation for China's Al surge was laid out in the <u>New Generation Artificial</u> <u>Intelligence Development</u> <u>Plan</u> in 2017. The plan details how, by 2030, China will be the global leader in Al theories, technologies,

The percentage of the world's top AI researchers from China rose from 29% in 2019 to 47% in 2022.

applications, and innovation. In terms of regulations, China was one of the first countries to implement AI regulations. Its most impactful AI <u>regulations</u> have been for recommendation algorithms (2021), the rules for synthetically generated content (2022), and draft rules on generative AI (2023), the latter of which occurred months after the release of ChatGPT. Compared to the US and EU, China tends to move quickly toward AI, making its next set of regulations eagerly <u>anticipated</u>.

The global landscape of AI is rapidly evolving, with immense potential and significant challenges. As AI algorithms become more sophisticated, we've seen the economic upsides, potential job displacement risks, and the need for ethical considerations.

Let's explore how AI is being leveraged to improve various aspects of our lives in cyber, from increased efficiency to improved accuracy.

SECTION THREE What Are the Benefits of AI in Cyber?

Al is often at its most powerful when it automates repetitive tasks, boosting efficiency and productivity while freeing humans up for more strategic endeavors, like building a multimillion dollar business centered around innovative engine design or leading a large project team address complex customer system requirements. Al analyzes massive data sets and uncovers hidden patterns and trends that enable better decisionmaking, forecasting, and risk assessment in finance, healthcare, and logistics. Finally, AI systems perform tasks with high precision, minimizing human error and ensuring consistent results, making them particularly valuable in domains like medicine and manufacturing, where accuracy is crucial.

Increased Efficiency and Productivity

Al excels at automating repetitive tasks, whether coordinating projects, scheduling meetings, calendar scheduling, or prioritizing tasks. Humans rarely have the raw power to crunch the data necessary to quickly and efficiently do these things at scale. When we try, we quickly get bogged down in the impossible minutiae, making us less productive and more demoralized. AI doesn't succumb to those feelings; it just makes a decision and allows you to determine the right one. Regarding cybersecurity, one meta-analysis of 69 research studies showed that artificial neural networks could detect spam, malware, and network intrusions with well over 90% accuracy. When AI is that efficient, humans get time back, which we can spend on activities where we outperform AI. However, the ultimate benefit will not just be outsourcing tasks to AI to improve productivity and efficiency but using AI to augment human intelligence and transform our ability to make decisions. So instead of a person/team assessing if a network intrusion has taken place,

an organization can redirect personnel to focus on designing a network to proactively deter a data breach.

Enhanced Data Analysis and Insights

Al algorithms can process massive amounts of data much faster and more accurately than humans, uncovering hidden patterns and trends. This enables better decision-making, forecasting, and risk assessment across various fields, from finance and healthcare to marketing and cybersecurity. In cyber, threat detection models already leverage deep learning to prevent malware and phishing attacks. As deep learning models continually train on massive datasets, they learn patterns that enhance their predictive threat detection capabilities. However, to capture the total value of data analysis from AI and to continually build on that value, organizations need to upskill their workforce by investing in AI architects, developers, translators, and all sorts of positions with full AI literacy. According to Gartner, more than 50% of Chief Data and Analytics Officers (CDAOs) will secure funding for data literacy and Al literacy programs by 2027, continuing to build on the AI pilot programs that 53% of CDAOs say they've already deployed or committed to piloting right now.



Improved Accuracy and Reduced Errors

Al systems' ability to perform exact, repetitive tasks can minimize human error and ensure more consistent results. In health care, for instance, Al's ability to crunch data can lead to more precise personalized treatment plans considering patients' medical history, environmental factors, lifestyles, and genetic makeup. In manufacturing, Al is poised to improve quality control while reducing cycle time, improving maintenance, and strengthening security, among other benefits. And in cybersecurity, where human error accounts for 80% of incidents, AI could help compensate for human failings-as we noted above, AI can help reduce phishing attacks. NLP has proved to be highly reliable and accurate in keyword extraction in email domains and messages to detect phishing and malware.

Overall, AI empowers security teams by handling routine tasks, providing deeper insights from data, and minimizing human error. This allows security professionals to focus on higher-level strategies to keep systems safe. Let's take a look at some of the main AI tools in play today.

SECTION FOUR What AI Tools Are in Play Today?

Al tools are deeply embedded in the fabric of life. Every day, for instance, 50% of mobile phone users in the US <u>use</u> voice search, which is powered by NLP. And major tech companies like <u>Microsoft</u>, <u>Meta</u> (Facebook), and <u>Amazon</u> have significant Al divisions and offer powerful tools in various areas. However, the three companies: NVIDIA, Alphabet (specifically Google AI), and OpenAI, stand out for their pioneering contributions and the widespread impact of their Al tools.



NVIDIA

One of the three most <u>valuable</u> companies in the world, NVIDIA produces hardware and software that power AI development. Their flagship products include:

NVIDIA <u>GPUs</u> (Graphics Processing Units): These specialized chips are highly efficient for processing the massive amounts of data required for AI tasks like deep learning and image recognition.

CUDA (Compute Unified Device Architecture): This parallel programming platform optimizes software code to run efficiently on NVIDIA GPUs, significantly accelerating AI applications.

TensorRT: This software library provides highperformance inference for deploying trained AI models on various platforms.

Google Al

Alphabet's valuation is <u>skyrocketing</u> as it prepares to embed Al into all its products. Google Al, a subsidiary of Alphabet, already boasts a wide range of tools and platforms across various Al domains: <u>TensorFlow</u>: This open-source machine learning library is famous for building and training various Al models, including deep learning networks. <u>Cloud TPUs</u> (Tensor Processing Units): Google's custom-designed chips are specifically optimized



for machine learning workloads, offering superior performance for training and inference. <u>AI Platform</u>: This cloud-based platform provides a comprehensive suite of tools and services for developing, training, and deploying AI models.

OpenAl

Few companies have done more to advance and popularize AI tools than OpenAI, which <u>launched</u> ChatGPT in November 2022. OpenAI continues to develop powerful AI models and conduct research on advanced AI capabilities, such as:

<u>GPT-4</u> (Generative Pre-trained Transformer 4): This LLM is renowned for generating realistic and coherent text, translating languages, and answering your questions informally.

DALL-E 3: This AI model creates incredibly realistic and detailed images based on textual descriptions. **OpenAI API:** This allows developers to integrate the capabilities of OpenAI's models into their applications.

These companies have shaped the AI landscape by providing the fundamental building blocks and groundbreaking advancements in AI capabilities. The future of AI will have other players in the space, but it is hard to see a near future without these three AI titans.

SECTION FIVE What Does the Future Look Like for AI?

As AI futurists assess the possibilities, they have tended to <u>fall</u> into two general camps, especially in <u>Silicon Valley</u>, arguably the center of the AI world. On one side are the "doomsayers"—those who believe that super intelligent AI is advancing so rapidly and uncontrollably that it <u>poses</u> an existential threat to humanity, and it's only a matter of time before the weaponization of AI <u>presents</u> security risks that are likely putting us on a path toward extinction.

On the other side are the optimists, those who see current developments more resemble a time of the second industrial revolution. From this point of view—which many believe <u>represents</u> the majority of AI futurists—AI will unleash unprecedented innovation in medicine, transportation, energy, and communications. All the pressing issues of today's world can be addressed in the future. Enabled by the increasing sophistication of AI-powered machines and algorithms, humans can solve problems that today are impossible.

Given the global impact that AI has already had on industry, government, technology, and everyday life, we anticipate AI's optimistic outlook to prevail partly because AI can be harnessed as a force for improved security systems and measures. It's one of the clearest ways that AI will change life. Let's peek at what that future may look like.

Advanced Cybersecurity Defense

With the cost of global cybercrime estimated to steadily grow to \$13.8 trillion by 2028, the ability to secure digital systems and networks will increasingly give organizations a competitive advantage. Not only will bad cyber actors never relent, but the savvier ones will find clever ways to harness the power of AI to enhance their attacks. Staying ahead of them and safeguarding the digital world so AI innovations can flourish will require equally powerful tools. This is why cybersecurity

a

will arguably be the <u>foundational</u> application of AI.

Many companies are already using AI to reinforce their existing cybersecurity efforts in a myriad of ways, and 70% of CISOs say that doing so gives them the edge over cyber attackers. However, to maintain that edge, CISOs must help their organizations continue to innovate. As bad cyber actors expand their AI efforts' size, scope, and effectiveness, cybersecurity teams must redouble theirs. In the future, here are three ways they will do so:

- Proactive Threat Detection: To stay ahead of bad actors, cybersecurity must transform from reactive to proactive defense measures. The ability to detect and defend against threats before they occur is critical. But this is impossible for a human to do at the scale that the AI-powered attacks of the future demand. So, cybersecurity teams must use AI algorithms that continuously analyze network traffic and user behavior to identify real-time anomalies and potential attacks. With attackers lurking in networks for 280 days on average, stopping them from breaching the network in the first place is critical. But if they breach your network, Alenabled threat detection will allow you to leverage Al to become "threat hunters," operating in realtime at speeds that aren't possible otherwise. Seamlessly transforming into an automated incident response mode.
- Automated Incident Response: If an organization experiences a cyber event, a rapid and coordinated response is key to minimizing damage and downtime. In the future, AI will be able to analyze massive amounts of data from across the organization in real time and automatically develop the most effective response. The entire incident response process might be an AI-enabled defense making complex decisions in fractions of a second, identifying and stopping the bad actor moments after a cyber event. This lays the foundation for an adaptive defense system.

• Adaptive Defense Systems: Cyber threats are constantly evolving by nature, as threat actors abandon outdated and unsuccessful tactics in favor of new approaches. Al will increase the volume and rate of changes, which means defensive measures must counter even more quickly to stay a step ahead. The more Al systems gather data from Al cyberattacks, the more effective they should become at analyzing complex behaviors and adapting to them in real time. In the future, a defensive measure like signature-based malware detection may still exist, but it will be complemented by Al-powered adaptive antivirus software.

Personalized Experiences and Solutions

A great promise of AI is that it can separate the signal from the noise in all areas of life. Put another way, AI can help people quickly figure out what matters, what is worth paying attention to, what can be ignored, and what they might want if only it were presented to them. While AI-powered recommendation algorithms have existed for a while—by 2017, for instance, Netflix viewers found 80% of their shows through them—the future will be even more precise. The more AI trains on data from human interactions, experiences, and products, the more accurately it will be able to tailor solutions to individual needs and preferences. Let's look at three examples:

• Adaptive Education: In the future, the experience of sitting through a lecture where everyone is taught at the same pace may be obsolete. Instead, Al-powered learning platforms will personalize education, adjusting difficulty levels and content based on individual students' strengths and weaknesses. This could help fill specific learning gaps and make learning more precise, collaborative, and engaging for students of all ages, from young children to professionals trying to upskill their careers.



- Precision Medicine: The human body is impossibly complex. Let's consider how many hundreds of thousands of years it took our species to develop what we call "modern" medicine. This repository of knowledge allows us to live vastly longer and healthier lives than at any time in the past. LLM-powered healthcare chatbots will continue to improve in <u>categories</u> like accuracy, trustworthiness, empathy, and computing performance. Among the next steps in this evolution will be leveraging AI to analyze vast amounts of medical data to personalize treatment plans and predict potential health issues for individuals, leading the way to precision medicine.
- Hyper-Targeted Marketing: If you've ever been shopping-in-person or online-you know how guickly your tastes and preferences can change. A shirt looks great but fits awkwardly; a new drink flavor is enticing until you see four more options. The same applies in a business context—which suppliers offer you the optimal mix of features, functions, support, and pricing for the specific problem you must solve? Precision marketing is good for digital marketers trying to keep pace with buyer behavior, but hyper-targeted marketing is better. In the future, AI will have the data, the algorithms, and the power to understand this behavior and personal preferences on deeper and more granular levels to provide consumers and businesses with ever more refined options in their marketing campaigns.

Enhanced Automation and Robotics

Robots, especially autonomous ones, are where Al software and hardware meet. Al-powered robots (as well as <u>cobots</u>, or collaborative robots) are already <u>prevalent</u> in manufacturing, where the ability to automate complicated tasks and increase quality and productivity creates a competitive advantage. As these machines ingest vastly more datasets, they'll continue to refine their capabilities and assume more complex tasks, ultimately transforming areas like:

- Autonomous Vehicles (AVs): While fully self-driving cars have been promised for years, advancements in AI will ultimately help them become commonplace, revolutionizing transportation and logistics. For instance, the major roadblock in testing AVs is access to datasets, as there isn't enough data on unique real-life situations that human drivers routinely encounter and easily navigate. To build that data to train AVs, researchers are building that training data with AI and neural networks to reinforce learning.
- Smart Factories: AI-powered robots will help manage production lines, optimize processes, and ensure quality control in manufacturing. AI will help predict maintenance needs so companies can address critical failures before they occur, and AI-enabled machines will be powerful enough to 3D print custom products on demand.
- Elderly Care: In elder care, AI-powered robots, assistants, and wearables will provide companionship, support, and health monitoring for aging populations. These advances will enable personalized assistance, allowing for individualized treatment plans, real-time health monitoring, and heightened safety, all permitting older adults to live autonomously for extended periods.

CONCLUSION

In this white paper, we explored the current state of AI, its global landscape, its benefits in cybersecurity, the powerful tools shaping AI today, and what the future might hold. We discussed the ethical considerations surrounding AI development and the potential risks bad actors pose. However, the optimistic outlook prevails, with AI poised to revolutionize various aspects of our lives, from cybersecurity to healthcare and education.

The future holds immense potential for AI advancements. As AI evolves, it's crucial to develop ethical frameworks and rules to ensure responsible use. But we can't do that in a vacuum where conversations are marred by partisanship and fear-mongering; instead, discussions should be welcomed by openmindedness and logic. As said at the start, we can do this, but we must all work together, for together, we are stronger. By harnessing the power of AI for good, we can create a safer, healthier, and more prosperous future for all.

The National Technology Security Coalition (NTSC) is a non-profit, non-partisan organization that serves as the preeminent advocacy voice for Chief Information Security Officers (CISOs) across the United States. Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.



2625 Piedmont Road NE Suite 56-370 Atlanta, Georgia 30324 **ntsc.org**