



# Strategic AI Integration: Confronting Emerging Threats and Fortifying National Defense

\*\*\*\*CAUTION\*\*\*\*

There are some components of this discussion that may cause severe intellectual improvement, extreme success and enabling a select few to make a drastic contribution to society.

Look for Job Opportunities

Ask yourself – “Can I get a job doing this?” Military or Civilian

How do you become educated or informed in this field?

Where can you be a Subject Matter Expert?

**THERE ARE NO LIMITS!!!**

\*\*\*\*CAUTION\*\*\*\*

# Objective

- Really, what is Artificial Intelligence (AI)?
- Examine AI threats from adversaries of the United States while incorporating counter AI technology defense strategies.
- Prepare educate the warfighter to use AI decisively and effectively.

## THE AGE OF AI - SOMETHING TO THINK ABOUT

- Imagine waking up to a world where your very identity can be stolen in an instant, fake news floods your newsfeed, and autonomous weapons are deciding the fate of nations...

## Where We Now Stand With AI

- In 2024 these are not just science fiction scenarios but real possibilities we face with the rapid advancement of AI...
- The stakes have never been higher...

## Let's Take A Look

- Today, we will explore the multifaceted world of AI, its potential risks, various challenges, and how we can harness its power for utilization in the defense of the nation...

# The Virtual World

- It is a real place, or the stuff movies are made of



# Artificial Intelligence Explosion

- What is it
  - Human like intelligence demonstrated by machines
  - NOT predetermined coded routines
- Intelligence determinations derived through processes conducted by computer information systems
- Results In
  - Rapid Technological Advancement
  - Many Benefits and Positive Effects



# Types of Artificial Intelligence



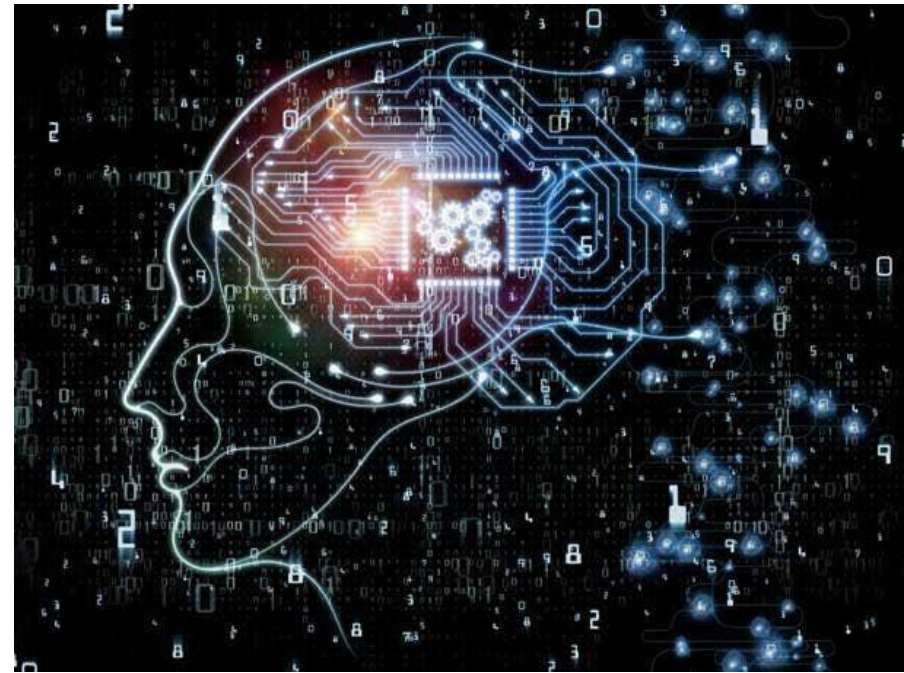
- Reactive Machines
  - Operates on set of rules and reacts to stimuli
  - IBM Deep Blue Chess Championship
- Limited Memory
  - Stores previous data and uses it to make future predictions
- Theory of Mind
  - Understands emotions, beliefs, thinking, and needs of individual humans and reacts in real time
- Self Awareness
  - Becomes self aware and forms its own identity

# Types of Artificial Intelligence

- Traditional AI (Narrow or Weak)
  - Performs specific tasks and has a defined scope - does not have general intelligence
  - Virtual personal assistant – Alexa and Siri
  - Expert systems – mimic decision making of a human expert
  - Machine Learning – Subset of AI where systems learn from data and improve their performance
    - › Spam Filters
    - › Recommendation Systems
    - › Fraud Detection
  - Natural Language Processing – Enables machines to understand interpret and generate human language
    - › Chatbots, language translation and voice activated assistance

# Types of Artificial Intelligence

- General AI – Strong AI - Ability to perform human intellectual task
  - Wild west
- Why is it Significant
  - Automation of Tasks
  - Enhanced Decision Making
  - Improved Healthcare
  - Economic Growth
  - Personalization
  - Enhanced Security
  - Natural Language Processing



# Generative AI



## ■ Generative AI – Strong

- Very distinctive Risk compared to regular AI
- Can create new content, text, images, audio, video based on trained data
- Use deep learning and neural networks
- Mimic human like creativity

## ■ Risks

- Disinformation – Deepfake, Fake News, Social Influence
- Intellectual Property Issues
  - GAI can inadvertently infringe on intellectual property rights by creating content that closely mimics existing works

# Generative AI

- Bias Amplification
  - GAI models trained on biased data can amplify those biases more visibly and impactfully, leading to the widespread dissemination of biased or harmful content
- Accessibility and Ease of Use
  - Tools are increasingly assessable and easy to use which lowers the barrier for malicious actors to misuse these technologies
- Regulatory Gaps
  - Regulatory framework for GAI is even less mature compared to other AI technologies which increases the likelihood of unethical use

# Generative AI - Probability of Misuse

- Risk Awareness – High
  - Broad recognition among experts about ethical misuse of AI
  - Employers are looking for AI auditors, policy makers and ethical experts
- Instances of Misuse - High
  - Tons of documented cases
  - It is happening already – it will increase
- Mitigation Efforts - Low
  - Efforts are growing they are not yet comprehensive or universally effective
- Probability of Misuse
  - Unethical use of AI - SIGNIFICANT
  - Must Implement – Continuous monitoring

# Types of Artificial Intelligence

- **Autonomous** Systems – Perform tasks without human intervention
  - Integrate with sensors, actuators and real time data processing to make on the fly decisions
  - Self Driving Cars
  - Robotics – Healthcare and Manufacturing
  - Smart Infrastructure – Smart Grids, Traffic Management and Public Transport
- Risks
  - Safety
  - Ethical and Legal issues – Makes decisions that effect human lives

# Primary World Threats

## ■ 1980's Primary Threat

- Cold War
- Massive Nuclear Arsenal
- Large Scale Warfare
- Patriotism – Fight Against Threats to the Homeland

## ■ 2000's Primary Threat

- Terrorism
- Targeted Attacks
- Jihad Driven

## ■ 2024 Primary Threat

- Nuclear War
- Terrorism
- Technological Adversary
- Human Intelligence Gathering



## Current Conflicts

- International events are playing out in the Virtual World and the Physical World
  - Russian Invades Ukraine

## Current Conflicts

- Director of National Intelligence - Avril Haynes stated weeks before the invasion of Ukraine, that Chevron and other companies were virtually attacked by Russia in an attempted to shut them down
  - Russia has multi-phase plans to destabilize the US power industry
  - Targeting the US financial sector
  - Due to the blurred lines between the virtual world and the physical world - Cyber attack could trigger NATO Article 5

## Current Conflicts

- Cybersecurity and Infrastructure Security Agency and FBI
  - Top pharmaceutical companies were targeted by Russian hackers
  - Done by cyber training units inside of Russia
  - Russia is deploying ransom ware across all agencies

# Russia Is Not Alone

- Collaboration Russia-China
  - Nicolas Chaillan, U.S. Air Force former Chief Software Officer
    - U.S is at kindergarten level relating to critical infrastructure compared to Russian-China alliance and cyber offensive capabilities
  - Russian-China cyber collaboration will be devastating to the US
- Conversely, the International Institute for Strategic Studies placed the US in its top tier of cyber powers and Russia and China in tier two

## China a Threat?

- CIA director says China is the greatest challenge to the US
- 100-year plan to destroy the US
- New Craze in US is Tik-Tok – Sen. Josh Hawley  
– Owned by Chinese businessman and is ultimately controlled by Beijing China

# Widespread Threats

- Pegasus Software
  - Developed by Israeli NSO Group
  - Made to compromise phones
    - Effected Heads of State, Reporters
  - Turns a phone into a surveillance device
    - Access Camera and Microphone
- Log4j
  - Log activities of consumer facing products
  - Can be used to capture and retrieve intellectual property
- Sen. Wyden from Oregon – SS7 International telecommunications protocol can be compromised and allow foreign actors to gain unauthorized access to our networks and intercept calls and texts

# Pictures are Deadly – Proud Papa



# Information Sharing Transition

- We have come from a society of privacy and keeping things to ourselves
- To a society of information flow, sharing and giving
- Everything is on-line



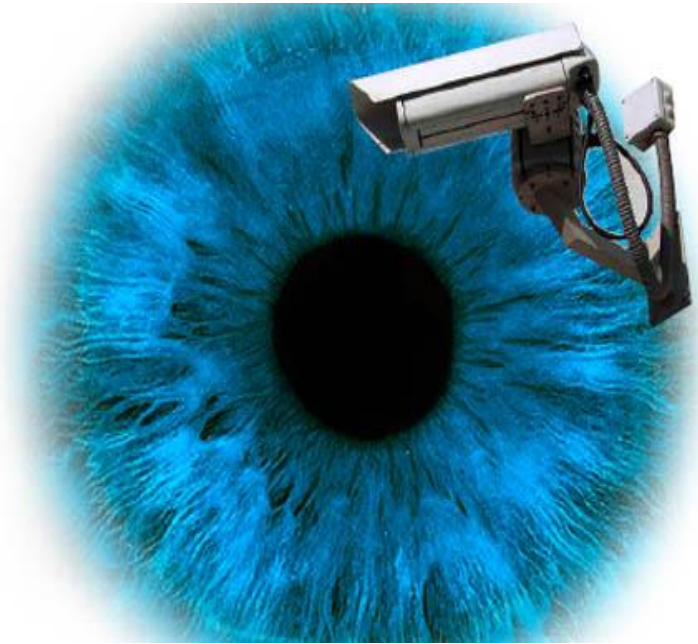
# Knowledge Explosion

- Information Sharing
  - Created a Knowledge Explosion.
  - Internet Use and Capability Grows Exponentially



# Who is Watching You?

- Do you ever feel like someone is watching you? Well, they are! Adversaries continually monitor web sites and personal activity to gather as much information on you as they can



# Human Intelligence Gathering

- What is it?
  - (HUMINT) Collection of data or information from people (humans) about any topic.
    - Collected Openly/Covertly
- Human Intelligence Gathering
  - Automatically Leads to Social Engineering

# Social Engineering

- What is it?
  - Tricking or coercing people into revealing information or violating security practices
  - Uses - Viruses, Trojan horses, Scareware, and Phishing all rely on trickery to be effective
    - Rely on the human element

# AI and Social Engineering

- Social Engineering
  - Analyze online behavior
  - AI bots – autonomously create and manage social media accounts, posting and sharing content to influence public opinion
  - Manipulate Images and Videos
  - Create Fake news articles, social media posts and blog entries
  - Voice Synthesis
    - Synthetic voice recordings indistinguishable from real human speech

# Artificial Intelligence In Social Engineering

- Spear Phishing
  - Automated - Review social/news media to create personalized attacks on specific individuals
- Voice Impersonation
  - AI can imitate a person's voice and voice characteristics
- Chatbots In Online Communities
  - Imitate real people and gather information for another attack
- Deepfake Videos
  - Create lifelike video producing social influencing messages
- Predict Behavior Patterns
  - Analyze data sets to predict patterns to influence social/political groups
- Absolutely Convincing
  - Analyze Phishing Detecting mechanisms criteria and produce a product that evades identification

# Artificial Intelligence in Human Intelligence Gathering

- Data Analysis and Pattern Recognition
  - Social Media
  - Data Interception
  - Identify Patterns Trends Anomalies
- Sentiment Analysis
  - Gauge public opinion
  - Used by foreign governments
  - Collects large scale Information
- Social Network Analysis
  - Analyze and identify various individuals, connections and relationships
    - Used to map social networks to identify weaknesses and vulnerabilities
- Anomaly Detection
  - Detect change in data patterns to identify vulnerabilities
  - Identify potential security risks
- Image and Video Analysis
  - Track individuals' movement and identify patterns of behavior
  - Predictive Analysis

# Dangers of Artificial Intelligence

- Jobs
  - Job Displacement – Job Loss
  - Current jobs being replaced by AI – Dark Factories
- Bias Decision Making
  - AI can inherit biases from its originators
- Ethical Concerns
  - Can ethics be programmed into AI and whose ethics are being used
  - Organizations and guidelines for ethical development
- Privacy Concerns – Collects a tremendous amount of PII at an accelerated rate
- Superintelligent AI – Surpass human process capabilities – Lose control
- AI Powered Networks and Weapons – Lose control

# Dangers of Artificial Intelligence

- Steel Identity

- Create Deepfakes

- Images
    - Videos
    - Audio

- Used to open bank accounts, make transactions or access personal information

- Phishing Attacks

- Highly Convincing
    - Designed to identity login credentials, financial details

- Credential Stuffing

- Test large amounts of usernames and password combinations to gain unauthorized access based on information obtained from various deepfakes and phishing attacks



# Implications of Bad Artificial Intelligence

- Profound Detriment to Society
- Perfect Weapon of Adversarial Nation States
  - The winner of AI dominance, dominates the world
  - Financial Loss
  - Reputational Damage
  - Erosion of Public Trust
  - Social Chaos
  - People Group Unrest

# Potential Risks and Ethical Challenges

## ■ Social Media Algorithms

- AI algorithms that curate and recommend content on social media platforms
- Algorithms can contribute to the spread of misinformation, echo chambers and polarization by prioritizing sensational or diverse content
- Impact mental health by promoting addictive behavior and negative content

## ■ Human Augmentation and Enhancement

- AI technologies used to enhance human physical and cognitive abilities
- Ethical concerns about fairness, consent, and the societal implications of augmenting human capabilities
- There is also a risk of exacerbating social inequalities if such technologies are not accessible to all

# Potential Risks and Ethical Challenges

## ■ Autonomous Weapons Systems

- AI powered weapons can select and engage targets without human intervention
- Risks – Lead to unintended escalations in conflict, accidental civilian casualties and violations of international humanitarian law
- Lack of accountability and control raises significant ethical and security concerns

## ■ Surveillance and Facial Recognition

- Unauthorized monitoring of one's physical, social and emotional attributes
- Risks – Privacy Invasion, human rights abuses

# Potential Risks and Ethical Challenges - Scraping

- FOR LAW ENFORCEMENT USE ONLY - Clearview AI
- Created software that scraped Billions of Faces off social media sites
  - Matched faces with names
  - Could identify people with only a small portion of their face visible
  - Social Media sites sent legal cease and desist order
  - Too late the software is out, and people are being tracked

# Potential Risks and Ethical Challenges

- Surveillance and Facial Recognition
  - AI technologies used for mass surveillance, identifying and tracking individuals in real-time
  - Risks – These technologies can be used to suppress dissent, invade privacy and discriminate against certain groups
    - Authoritarian regimes can use them to exert social control, leading to human rights abuses
- Hiring Algorithms
  - In 2018 Amazon was shown to discriminate against women
- Healthcare Algorithms
  - Shown to favor white people over black for additional healthcare
- Credit Scoring Systems
  - Shown to lower credit scores for particular zip codes automatically
- Content Moderation
  - Limiting hate speech to certain groups and not to others

# Potential Risks and Ethical Challenges

- Predictive Policing and Criminal Justice Algorithms
  - AI systems use to predict criminal activity and assist in judicial decisions
  - These systems can reinforce and amplify existing biased in law enforcement and the judicial system, leading to unfair treatment of minorities and marginalized communities
  - Lacks transparency and accountability

# Potential Risks and Ethical Challenges

- AI in Healthcare
  - AI systems used for diagnosing diseases, recommending treatments and managing patient data
  - Errors or biased in AI healthcare systems can lead to misdiagnoses or inappropriate treatments potentially causing harm to patients
  - Privacy Concerns handling sensitive medical and patient data
- Financial AI Systems
  - AI used in trading, credit scoring and fraud detection
  - AI-driven financial decisions can result in market instability, unfair lending practices and systemic biases in access to financial services
  - High frequency trading algorithms can exacerbate market volatility

# Autonomous Weapons System

- Lethal Autonomous Weapon Systems (LAWS) – Killer Robots
  - Engage Targets Without Human Intervention
  - Operate with sensors, decision making algorithms
  - Eliminates targets based on predefined criteria
- The Harpy Drone
  - Designed to detect and destroy radar emitters
  - On launch it will loiter in an area, identify enemy radar signals, dive in and destroy
  - Operates without human intervention
- Risks
  - Lack of Accountability
  - Risk of Malfunction
  - Ethical Implications – Makes life and death decisions

# Safe Artificial Intelligence - Oversight

- AI System Accountability – Very few initiatives currently in place or perfected
  - Companies have published their ethical principals
  - Companies do audit AI algorithms
  - Identify bias training datasets
- Transparent and Explainable AI – AI models that explain their decision-making process and how they arrive at their conclusions
- AI Impact Assessment
- AI Certification and Standardization
- Regulatory Initiatives
  - Requirements for transparency, data protection and compliance

# Safe Artificial Intelligence - Oversight

- Diverse Training Data
- Bias Detection and Correction
- Inclusive Design
  - Include diverse teams in the design and development of AI systems
- Regular Audits
  - Audit software
  - Algorithmic Auditing
  - AI audit training

# Safe Artificial Intelligence for Humankind

## ■ Ethical Framework

- Guiding principles for AI development
  - Fairness
  - Accountability
  - Transparency
  - Privacy
- Asilomar AI Principles

## ■ Ethics Committee

- Review AI projects for alignment with ethical standards

## ■ Public Stakeholder Engagement

- Civil Society Organizations – Vital Input

## ■ Education and Training

- Developers should be educated on ethical AI standards and policy

# Regulation and Ethical Guidance

- Effective Regulation
  - Legislation and Policies
  - Regulatory Bodies
  - Standards and Certifications
  - Impact Assessments
- Ethical Guidance
  - Ethical Frameworks and Principles
  - Ethics Committees
  - Public and Stakeholder Engagement
- Public Trust in AI
  - Importance of Transparency and accountability
- Communication and Education
  - Educating the public about the AI benefits and risks

# Artificial Intelligence Ethics Solutions

## ■ AI Governance

- Regulation and Policy - EU AI Act and US AI initiative
- Global Cooperation – Need for international standards

## ■ AI Safety

- Risk Management – Rigorous testing, validation
- Required Human-in-the-loop for all decision making

## ■ AI Transparency

- Black Box Problem
  - How to AI systems make a particular decision or arrive at a conclusion
  - Grey area
- Explainable AI
  - Techniques and methods designed to make the decision-making process of AI systems transparent
    - › BECOME A SME IN THIS FIELD!!!

# International Cooperation

- International Agreements and Standards
  - OECD Principles on AI
  - Global Partnership on AI (GPAI)
  - Treaties
  - Partnerships
  - Common Standards
  
- Global Forums and Collaboration
  - AI Governance
  - Global Partnership
  - Importance of International dialog
  
- Capacity Building and Cybersecurity
  - Assisting developing countries
  - Shared cybersecurity protocols

# Artificial Intelligence for the Cybersecurity Professional Employment Goldmine

- AI Security Specialists
  - Secures AI systems and protects them from other AI cyber threats
- AI Ethics and Governance Specialist
  - Ensures AI systems adhere to ethical guidelines and regulatory requirements
- AI Forensics Expert
  - Specializes in investigating security incidents involving AI systems
- Machine Learning Security Engineer
  - Secures machine learning models and infrastructure
  - Protects data used for training AI models and integrity of AI algorithms
- Cyber Threat Analyst for AI Systems
  - Monitor and analyze cyber threats targeting AI systems
- AI-Powered Security Solutions Developer
  - Develop AI-driven cybersecurity tools and solutions

# Artificial Intelligence for the Cybersecurity Professional Employment Goldmine

- AI Policy and Compliance Analyst
  - Ensures AI systems comply with cybersecurity standards and regulations
  - Create policies and guidelines for secure AI practices
- AI Security Researcher
  - Conduct research on AI security to identify new threats and develop innovative solutions
- AI Incident Response Specialist
  - Manage and respond to security incidences involving AI systems
- AI Privacy Engineer
  - Protect the privacy of data used in AI systems
  - Ensure AI applications comply with data privacy laws and best practices

# Artificial Intelligence Impact on Society

- We Have Created a Virtual World
- Unquenchable Thirst for Knowledge
- Developed and Mastered Intelligence Gathering
- Use Intelligence for Global Domination
- Introduced and Continually Advance Artificial Intelligence
- Positioned Future Technological Experts to Be Reliant on Artificial Intelligence
  - **Take Your Place In This New Frontier**

# AI in National Defense

- AI and the US Military
  - AI has been gradually integrated into military operations since the mid-20th century.
  - The Pentagon's Defense Advanced Research Projects Agency (DARPA) was established in 1958.
  - AI's evolution in defense has led to advancements in autonomous systems, data analysis, and decision-making capabilities.
- Importance of AI In The Military
  - Critical for enhancing decision-making speed, precision, and effectiveness.
  - Ability to process vast amounts of data in real-time is essential for modern military operations, including surveillance, threat detection, and **autonomous systems** deployment.

# Emerging AI Threats

- **Autonomous Weapon Systems**
- **Threat Overview:** Autonomous weapon systems (AWS) - Significant emerging threat,
  - Ability to make lethal decisions without human intervention.
  - Deployed in large numbers and could operate independently on the battlefield.
  - Escalate conflicts more rapidly, with the risk of unintended consequences or the loss of control over these systems.
- **Example:** Swarms of AI-powered drones could be used to overwhelm defense systems, targeting critical infrastructure or military assets with precision and speed that human operators might struggle to counter.

# Emerging AI Threats

- **AI-Driven Cyber Attacks**
- **Threat Overview:** AI-driven cyber attacks can adapt in real-time, learn from defense mechanisms, and exploit vulnerabilities faster than human hackers.
  - Scan networks for weaknesses.
  - Deploy malware and carry out coordinated attacks on critical infrastructure.
  - Military networks and communication systems.
- **Example:** An AI-powered malware could infiltrate military networks, autonomously mapping out critical systems and launching targeted attacks that disable communication between defense systems or compromise sensitive data.

# Emerging AI Threats

## ■ Deepfake and Disinformation Campaigns

- **Threat Overview:** Create deepfakes
  - Highly realistic but fake videos, audio, or images.
  - Create false information or impersonate leaders and military officials.
    - Confusion, distrust, and panic.
    - Disinformation campaigns.
    - Influencing public opinion and destabilizing societies during a crisis.
- **Example:** A deepfake video of a military leader issuing a false order or declaration could lead to chaos and miscommunication within the armed forces, potentially undermining military operations during a critical moment.

# Russia



&

# China



# Emerging AI Threats

## ■ Russia and China

- Rapidly advancing their AI capabilities with significant investments in military applications.
- Russia focuses on AI for cyber warfare and autonomous weapon systems.
- China is prioritizing AI for surveillance, propaganda, and information warfare.

# AI Russian Threats

## ■ Cyber Warfare

- Russia has been heavily investing in AI to enhance its cyber warfare capabilities.
- AI is used to develop more sophisticated cyberattacks.
- Autonomously identify vulnerabilities, conduct phishing attacks, or deploy malware.
- Target critical infrastructure, government networks, and private sector companies.
- **Example:** The 2020 SolarWinds cyberattack.
  - Russian intelligence services, involved sophisticated techniques.
  - Included AI-driven tools to infiltrate and remain undetected within the networks of numerous U.S. government agencies and private companies for an extended period.



# AI Russian Threats

## ■ AI Powered Autonomous Weapons

- Unmanned Aerial Vehicles (UAVs) and ground robots.
- Autonomously select and engage targets without human intervention.
- Deployment of such weapons lowers the threshold for military engagements and escalate conflicts more rapidly.
- **Example:** Autonomous tanks and drones equipped with AI-driven targeting systems.



# AI Russian Threats

## ■ Disinformation Campaigns

- Bots and algorithms are employed to create and spread false narratives.
- Manipulate social media platforms and influence public opinion in target countries.
- Destabilize political systems and create social discord.
- **Example:** During the 2016 U.S. presidential election.
  - Russian AI-driven bots were used to amplify divisive content on social media.
  - Impacting the political discourse in the United States.

# AI Chinese Threats

## ■ Mass Surveillance and Social Control

- Extensive AI-driven surveillance network that monitors and controls its population.
  - Facial recognition.
  - Gait analysis.
  - Data analytics to track and profile individuals.
  - Used domestically or for military intelligence and counterintelligence operations against other countries.
- **Example:** China's Social Credit System.
  - Monitor citizens' behavior and assign scores based on their compliance with government policies.
  - Adapted to identify and suppress dissent in occupied territories or during military operations abroad.

# AI Chinese Threats

- **Rapid Adversary Analysis and Military Decision-Making**
  - Military decision-making processes.
  - Faster analysis and execution of military strategies.
  - Analyze large satellite and signals intelligence datasets quickly.
  - Provide real-time insights and recommendations to military commanders.
- **Example:** Chinese military's use of AI in wargaming and simulations.
  - Testing of various military scenarios.
  - Refine wartime strategies against potential adversaries like the United States.

# AI Chinese Threats

## ■ AI-Enhanced Cyber Espionage

- Enhance cyber espionage capabilities.
- Targeting sensitive information from government agencies, defense contractors, and private companies.
- Enable Chinese hackers to automate the identification of valuable data and streamline exfiltration processes.
- **Example:** Chinese cyber espionage group APT10 (Advanced Persistent Threat 10).
  - Stone Panda - has been linked to extensive data theft operations against companies in the U.S. and Europe.



# Threat Mitigation

# Defense Contractors/Educators

- **Develop Comprehensive Training Programs**

- Training for all levels of military personnel, from enlisted members to top commanders.
- **Implementation:**
  - AI-specific training courses that cover the basics of AI, its applications in defense, and advanced techniques for those in technical roles.
  - Incorporate practical exercises, simulations, and real-world case studies to help personnel understand how AI can enhance their operational effectiveness.
- **On Notice:**
  - Notify me of where and how you feel AI can help you succeed.

# Public and Private Partnerships

## ■ Joint Partnership

- Department of Defense must join with tech companies, and academic institutions.

## • Implementation:

- Collaborations between the military, technology companies, and research institutions.
- Drive innovation and develop cutting-edge AI applications for defense.
- Partnerships can focus on joint research initiatives, technology transfers, and the development of AI tools tailored to military needs.

- **Outcome:** Leveraging the expertise and resources of the private sector and academia can accelerate the development and adoption of AI technologies, ensuring the military stays at the forefront of technological advancements.

# Incentivize AI Research and Development (R&D)

- **Government and Private Funding**
  - Defense contractors, startups, and in-house military R&D units.
- **Implementation:**
  - Funding opportunities, grants, and awards for AI-focused R&D projects with defense applications.
  - Innovation competitions or "hackathons" specifically aimed at solving defense-related challenges using AI.
  - Streamline the procurement process to make it easier for innovative AI solutions to be tested and adopted by the military.
- **Outcome:**
  - With financial incentives and recognition, the military can stimulate interest in AI development and encourage more entities to focus their efforts on creating AI solutions that address national defense needs.
- Create a robust environment that fosters the adoption and integration of AI into national defense, enhancing the military's capabilities and readiness.

# Practical Implementation

# AI In Special Warfare

- **Situational Awareness and Intelligence Gathering**
  - AI enhances situational awareness.
  - Processing and analyzing large volumes of data from multiple sources.
    - Satellite Imagery
    - Drone Feeds
    - Social Media
    - Signals intelligence
    - Pattern Prediction and Movement
- **Example:** Palantir's Gotham platform are used by special operations forces (SOF) to analyze data from various intelligence sources.
  - Quickly identify and track high-value targets, understand enemy tactics, and anticipate potential threats.

# AI In Special Warfare

## ■ Autonomous Drones and Robotics

- AI-driven drones and robotic systems.
- Infiltrate enemy-held areas, gather intelligence, or even carry out targeted strikes with minimal risk to human operatives.
- **Example:** The U.S. Special Operations Command (SOCOM) uses AI-enabled drones like the RQ-11 Raven for ISR (Intelligence, Surveillance, and Reconnaissance) missions.
  - Autonomously navigate and relay real-time video feeds and data to operators, providing critical insights during missions.



# AI In Special Warfare

## ■ Enhanced Cyber Warfare and Electronic Warfare

- AI to enhance their cyber warfare and electronic warfare (EW) capabilities.
- AI algorithms can detect, analyze, and exploit vulnerabilities.
- **Example:** AI-driven EW systems can jam or spoof enemy communications.
  - Disrupt command and control networks.
  - Protect special forces from electronic surveillance.
  - AI can automate the process of hacking into enemy networks to gather intelligence or disable critical systems.



# AI In Special Warfare

- **Predictive Analytics and Mission Planning**
  - Predictive analytics to assess the likelihood of mission success.
  - Quickly analyze historical data, environmental factors, and intelligence reports to suggest optimal strategies and tactics for special operations.
- **Example:** Used in mission planning to simulate different scenarios and outcomes.
  - Allowing commanders to choose the most effective approach.

# AI In Special Warfare

## ■ Human Performance Enhancement

- Enhance the physical and cognitive performance of special warfare operatives.
- Wearable sensors collect data on vital signs, fatigue levels, and stress, which AI algorithms analyze to optimize training regimens, recovery protocols, and mission readiness.
- **Example:** Performance Readiness Optimization Tools (PROT) to monitor the health and readiness of special operations forces.
  - Provide real-time feedback and suggest personalized interventions to maintain peak performance in the field.

# AI In Special Warfare

- **Advanced Targeting and Precision Strikes**
  - AI enhances the accuracy of targeting systems.
  - Algorithms process data from various sensors to identify targets, predict movements, and minimize collateral damage.
- **Example:** Special operations snipers and forward air controllers (FACs) use AI-powered targeting systems that incorporate computer vision and machine learning to improve accuracy in dynamic environments.
  - Automatically calculate ballistic trajectories and adjust for environmental factors.

# AI In Special Warfare

## ■ Logistics and Supply Chain Optimization

- Optimize the logistics and supply chains that support special operations.
- Managing the deployment of resources, ensuring the timely delivery of supplies, and reducing the operational footprint in hostile environments.
- **Example:** Logistics platforms predict supply needs based on mission parameters and environmental conditions.



# AI In Special Warfare

- **Combat Simulations and Training**

- Combat simulations provide realistic training environments.
- **Example:** Practice high-risk missions in virtual environments that adapt to their actions, offering a dynamic and immersive training experience.

# Artificial Intelligence In The Air

# AI In The Air

## ■ Autonomous Systems and Pilot Assistance

- Assist pilots during missions to handle complex tasks.
  - Controlling unmanned wingman drones.
  - Taking over certain flight operations, allowing the human pilot to focus on mission-critical decisions.
- **Example:** The U.S. Air Force has developed AI-powered unmanned combat aerial vehicles (UCAVs) like the XQ-58A Valkyrie.
  - Can operate alongside manned fighters, performing reconnaissance, electronic warfare, and even engaging in combat autonomously.

# AI In The Air

- **Enhanced Targeting and Threat Detection**
- Used to enhance the targeting systems of fighter jets.
  - Enabling them to identify, track, and engage multiple targets more efficiently.
  - Processes sensor data, identifies potential threats, and provides real-time recommendations to the pilot.
- **Example:** The F-35 Lightning II uses Distributed Aperture System (DAS), which provides pilots with 360-degree situational awareness.
  - AI processes the data from multiple sensors to detect and track airborne and ground threats, improving response times and targeting accuracy.

# AI In The Air

## ■ Predictive Maintenance and Health Monitoring

- Predict and diagnose maintenance issues in fighter jets before they become critical.
- Predictive maintenance algorithms analyze data from sensors embedded in various components of the aircraft to forecast potential failures and schedule maintenance proactively.
- **Example:** The F-22 Raptor and F-35 Lightning II programs use AI-driven predictive maintenance systems to monitor the health of key components, such as engines and avionics.
  - Reduces the likelihood of unexpected failures and extends the operational readiness of the fleet.



# AI In The Air

## ■ Combat Simulations and Pilot Training

- Advanced combat simulations to train fighter pilots.
- AI-driven adversaries in these simulations can mimic the tactics and behavior of enemy pilots.
- **Example:** The U.S. Air Force's Air Combat Command uses Autonomous Air Combat Operations (AACO) program to simulate dogfights.
  - Opponents that learn and adapt to the pilot's tactics over time.

# AI In The Air

## ■ Electronic Warfare and Cyber Defense

- Detect and counteract enemy radar and communication systems.
- Protect a jet's systems from cyberattacks, ensuring the integrity and security of mission-critical data.
- **Example:** The EA-18G Growler, an electronic warfare aircraft used by the U.S. Navy, incorporates AI to identify and jam enemy radar and communication signals more effectively.
  - Adapts in real-time to changing electronic warfare environments, improving mission success rates.

# AI In The Air

## ■ Mission Planning and Execution

- Analyzes vast amounts of data to optimize flight paths, weapon selection, and engagement strategies.
- Adapts to new information, such as the appearance of unexpected threats or changes in the battlefield environment.
- **Example:** Tools help pilots choose the best approach to a target, taking into account factors like enemy air defenses, weather conditions, and fuel consumption.

# Artificial Intelligence and Cyberwarfare

# AI and Cyberwarfare

- **Phase 1: Infiltration and Reconnaissance**
- **Adversary Background:** A technologically advanced nation-state adversary has developed sophisticated AI-driven cyber capabilities. This adversary is known for its advanced cyber espionage tactics and its focus on AI to enhance cyber warfare capabilities.
- **Target:** The adversary targets a U.S. defense contractor responsible for the development and maintenance of critical defense systems, such as missile defense networks or command-and-control systems.
- **AI-Powered Phishing Attack:** The adversary uses AI to launch a highly targeted phishing campaign against employees of the defense contractor. The AI analyzes social media profiles, email patterns, and other online behavior to craft convincing phishing emails tailored to each individual. One of these phishing attempts successfully compromises the credentials of a network administrator.

# AI and Cyberwarfare

- **Phase 2: AI-Enhanced Network Breach**
- **AI-Driven Lateral Movement:** With initial access to the contractor's network, the adversary deploys AI algorithms designed to mimic legitimate user behavior. These AI tools enable the adversary to move laterally within the network, avoiding detection by traditional security measures. The AI continually adapts its tactics based on the responses of the network's defense mechanisms.
- **Reconnaissance and Data Exfiltration:** The adversary's AI systematically maps the network, identifying key systems related to the defense contractor's work on missile defense. The AI identifies and exfiltrates critical data, including system schematics, software code, and encryption keys, sending this information back to the adversary in small, obfuscated data packets that evade detection.

# AI and Cyberwarfare

- **Phase 3: Manipulation and Sabotage**
- **AI-Driven Backdoor Installation:** Using the stolen data, the adversary's AI develops a tailored backdoor that can be inserted into the software updates or patches distributed by the defense contractor. This backdoor is designed to be dormant initially, activating only under specific conditions (e.g., when the system is deployed during a high-alert situation).
- **Compromise of Defense System:** The compromised software update is unknowingly deployed across the U.S. missile defense system. The AI backdoor remains undetected during routine operations, blending in with legitimate system functions.

# AI and Cyberwarfare

- **Phase 4: Exploitation**
- **Disruption of Defense Capabilities:** The adversary now has the ability to manipulate the missile defense system in real-time. They could choose to disable the system, redirect missiles, or cause the system to generate false positives and engage in self-sabotage, such as misfiring or targeting friendly assets.
- **Activation of Backdoor:** During a simulated missile attack drill or in response to an actual perceived threat, the backdoor activates. The AI inside the backdoor takes control of key components of the missile defense system, such as the targeting algorithms or communication channels between sensors and command centers.
- **Outcome:** The compromise of the missile defense system during a critical moment creates chaos and undermines confidence in the U.S. defense infrastructure. The immediate impact could be catastrophic, potentially leading to significant loss of life, damage to critical infrastructure, or a severe strategic disadvantage.

# AI and Cyberwarfare

- AI-Driven Cyber Capabilities:** The scenario leverages AI's ability to conduct sophisticated, adaptive cyberattacks, which are within the realm of current technological possibilities.
- Human Element Exploitation:** The use of AI-enhanced phishing and social engineering is highly plausible, given that human error remains a significant vulnerability in cybersecurity.
- Complexity of Defense Systems:** The interconnected nature of modern defense systems and the reliance on contractors for software updates make such a scenario technically feasible.

# AI and Cyberwarfare

- **Background**

- A foreign adversary, let's say a state-sponsored group from a technologically advanced nation, has been developing advanced AI capabilities aimed at cyber espionage and offensive cyber operations. Over the years, they have successfully infiltrated various networks globally, gathering intelligence and planting dormant malicious code within critical infrastructure systems.

- **Phase 1: Initial Infiltration and Data Collection**

- The adversary deploys AI-driven malware that uses machine learning techniques to infiltrate the networks of a U.S. defense contractor. The malware is designed to be extremely stealthy, evading traditional cybersecurity defenses by continuously learning and adapting to the network's environment.
- **AI Role:** The malware uses AI to mimic normal network traffic, making it nearly undetectable by conventional intrusion detection systems (IDS). It slowly gathers intelligence on the network architecture, user behaviors, and security protocols.
- **Outcome:** Over months, the AI-powered malware maps out the contractor's network, identifying the most critical systems and the defense systems they are connected to.

# AI and Cyberwarfare

## ■ Phase 2: Targeted Exploitation

- Once enough data is collected, the AI system identifies vulnerabilities in the defense contractor's connection to a domestic missile defense system (for example, a regional anti-ballistic missile defense network). The malware then evolves its attack strategy, focusing on these weak points.
- **AI Role:** The AI analyzes patch management practices and user credentials within the defense contractor's network. It identifies an unpatched vulnerability in a legacy system that is still connected to the defense contractor's infrastructure. The AI tailors a zero-day exploit that can be deployed at the opportune moment.
- **Outcome:** The adversary successfully plants a backdoor into the missile defense network through the compromised contractor system.

# AI and Cyberwarfare

- **Phase 3: Covert Command and Control**
- With the backdoor in place, the adversary gradually gains control over the missile defense system's command and control (C2) interface. However, instead of immediately seizing control, the AI-driven malware carefully observes normal operations, learning how the system is used during different conditions—peacetime, drills, and heightened alert.
- **AI Role:** The AI component of the malware monitors and records standard operating procedures, communication patterns, and even the timing of routine checks and updates. It can simulate these behaviors to avoid detection by system operators.
- **Outcome:** The AI-driven malware remains dormant, waiting for a critical moment to activate, such as during a military crisis when the system is most needed.

# AI and Cyberwarfare

- **Phase 4: Execution of the Attack**
- During a simulated military exercise in the U.S., where missile defense systems are expected to be fully operational, the adversary activates the malware. The AI's learning and observation allow it to disrupt communications between the missile defense system's components, feeding false data to operators while blocking real-time responses.
- **AI Role:** The AI manipulates sensor data to create the appearance of normal operations while actually preventing missile interceptors from launching or misdirecting them. It also initiates a parallel cyber attack on backup systems, ensuring that the disruption is sustained.
- **Outcome:** The missile defense system fails during the exercise, causing confusion and potentially opening a window for real attacks if this occurred during an actual conflict.

# AI and Cyberwarfare

- **Phase 5: Covering Tracks**

- After the attack, the AI malware executes a self-deletion protocol, removing all traces of its presence. The adversary then uses disinformation and diplomatic channels to divert suspicion, making it appear as though the failure was due to an internal technical error.
- **AI Role:** The AI ensures that all logs are modified or deleted, and any residual code is rendered inert, making forensic investigation extremely difficult.
- **Outcome:** The true nature of the breach may remain undiscovered for an extended period, leaving the adversary with a significant strategic advantage.

# AI and Cyberwarfare

- **Conclusion**

- This scenario highlights the plausible and insidious ways an AI-powered cyberattack could allow a foreign adversary to gain control over a domestic defense system. By using AI for advanced infiltration, data analysis, and operational deception, the adversary could bypass traditional defenses, potentially causing catastrophic consequences during a critical moment.
- The scenario underscores the importance of incorporating AI-driven defenses and robust cybersecurity measures to detect and mitigate such advanced threats.

# Technology AI Usage

- **Implement AI-Driven Decision Support Systems**

- **Description:** Develop and deploy AI-powered decision support systems that assist commanders and military planners in making faster and more informed decisions. These systems can analyze vast amounts of data from various sources (intelligence reports, satellite imagery, battlefield sensors) and provide real-time recommendations.
- **Technology Example:** AI algorithms that incorporate machine learning and natural language processing (NLP) can be used to sift through intelligence data, identify patterns, and predict potential threats or outcomes, helping to inform strategic and tactical decisions.
- **Outcome:** By integrating AI into the decision-making process, military leaders can make more accurate and timely decisions, improving operational efficiency and effectiveness.

# Technology AI Usage

- **Enhance Autonomous Systems with AI**

- **Description:** Invest in the development and deployment of AI-enhanced autonomous systems, such as drones, unmanned ground vehicles (UGVs), and autonomous naval vessels. These systems can perform a wide range of tasks, from reconnaissance and surveillance to logistics support and even combat operations, with minimal human intervention.
- **Technology Example:** AI algorithms can enable autonomous systems to navigate complex environments, identify and track targets, and make real-time adjustments to their mission objectives based on changing conditions on the battlefield.
- **Outcome:** AI-driven autonomous systems can operate in dangerous or inaccessible environments, reducing the risk to human personnel while increasing the military's operational capabilities.

# Technology AI Usage

- **Deploy AI-Enhanced Cyber Defense Mechanisms**

- **Description:** Integrate AI into cybersecurity frameworks to enhance the military's ability to detect, analyze, and respond to cyber threats. AI can be used to identify anomalous behavior, predict potential cyberattacks, and automate the response to mitigate risks.
- **Technology Example:** AI-based intrusion detection systems (IDS) can continuously monitor network traffic, detect suspicious activities, and respond in real-time by isolating affected systems or neutralizing threats. Machine learning models can also be trained to recognize new types of cyberattacks and update defense mechanisms accordingly.
- **Outcome:** AI-enhanced cyber defenses provide a more robust and adaptive security posture, protecting critical military infrastructure from increasingly sophisticated cyber threats

# Revolutionize Defense Operations

# Quantum Computing in Cryptography and Communications

- **Enhanced Cryptography**

- Quantum computing has the potential to break traditional encryption methods.
- Pose a significant risk to national security if adversaries develop this capability first.
- Offers the ability to create virtually unbreakable encryption through quantum key distribution (QKD).
- Secure military communications and data against any future quantum-based threats.

- **Example:** Quantum computers could solve complex cryptographic problem in seconds

- Normally take classical computers thousands of years, allowing for secure communications even in hostile environments.

- **Strategic Advantage:** Implementing quantum-resistant encryption will give a strategic edge in protecting sensitive information.

- Defense operations remain secure even in the face of emerging quantum threats.

# Advanced Machine Learning for Predictive Analytics and Decision-Making

- **Predictive Maintenance**
  - Advanced machine learning models can predict equipment failures before they happen.
  - Predictive capability allows for proactive maintenance, reducing downtime and ensuring that critical military hardware is always ready for deployment.
- **Enhanced Decision-Making:**
  - Machine learning algorithms can analyze vast amounts of data to provide decision-makers with real-time, actionable insights.
  - Simulate different scenarios, predict outcomes, and recommend optimal strategies, significantly improving the speed and accuracy of decision-making in complex military operations.
- **Example:** Process satellite imagery, drone feeds.
  - Real-time assessments of enemy movements and suggest the best course of action.
- **Strategic Advantage:** The ability to anticipate and react quickly to changing conditions on the battlefield provides a crucial advantage, allowing for more precise and effective operations.

# AI in Autonomous Systems and Combat Simulations

- **Autonomous Combat Systems**

- Advanced AI models enable the development of autonomous drones, vehicles, and robotic systems that can perform complex tasks independently.
- Carry out missions that are too dangerous for human soldiers.

- **AI-Powered Simulations:**

- Create realistic combat simulations that adapt to the actions of human operators, providing more effective training for military personnel.

- **Example:** Autonomous drones equipped with AI can operate in swarms, coordinating their actions without human intervention to overwhelm enemy defenses or gather intelligence in contested areas.

- **Strategic Advantage:** Reduces the risk to human life while increasing operational flexibility and effectiveness.

- Improve readiness and adaptability, ensuring that forces are prepared for a wide range of potential threats.

# What is the Common theme?

## Conclusion

Where do we go from here?

As a Nation?

As Military Personnel?

As a Person?