Strategic Studies Center ,
National Defence Studies Institute

Senior Security Studies Program

Daniel K. Inouye Asia-Pacific
Center For Security Studies

Workshop 3

"New Security Challenges in the Cyber Domain"

Presented By

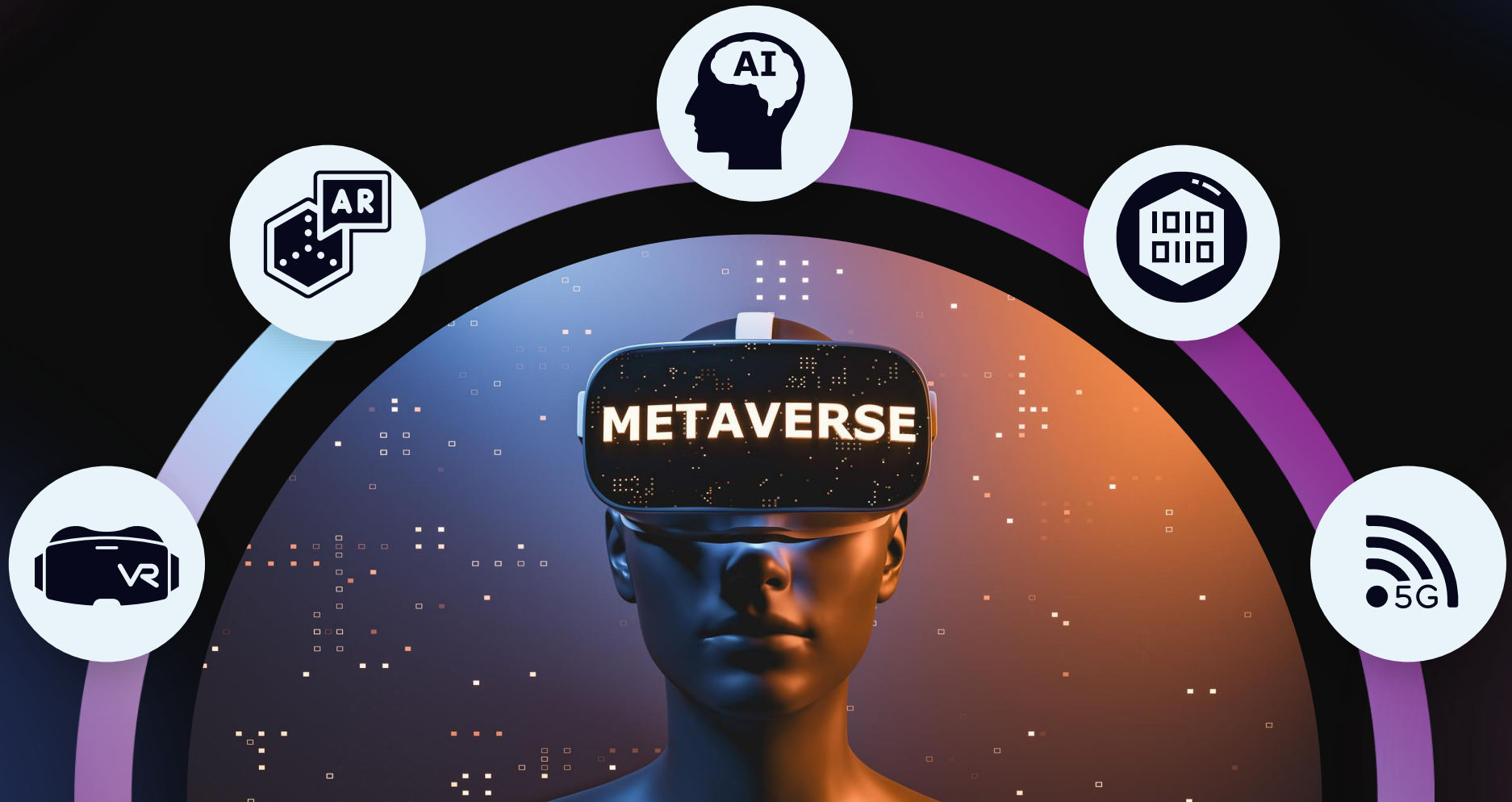
Group 2

Overview: Cyber Security in Thailand

Aspects	Cyber Security in Thailand
1. Cyber Threats	Increasing number of cyber threats and attacks, including hacking, data breaches, ransomware, phishing, and identity theft. Facing sophisticated cyber threats from both domestic and international sources, necessitating ongoing efforts to stay ahead.
2. Legal Framework	The enactment of the National Cybersecurity Act in 2019 establishes a legal framework for cyber security management and enforcement.
3. Government Initiatives	The Thai government has established the National Cybersecurity Agency (NCSA) to coordinate and oversee cyber security initiatives across sectors.
4. Public-Private Collaboration	Collaboration between government agencies, businesses, and international partners is crucial to address cyber security challenges effectively.
5. Cybersecurity Education	Promoting cybersecurity education and training programs to develop a skilled workforce in the field.
6. Continuous Monitoring & Cybersecurity Workforce	The need for continuous monitoring, threat intelligence sharing, and capacity building to respond to evolving cyber risks. Investing in cybersecurity professionals and encouraging research and innovation to enhance cyber defense capabilities.

Cybersecurity in Thailand:

Driving Forces and Challenges



1. Technological Advancement

- Rapid technological advancement
- Increased internet penetration and digital connectivity
- Proliferation of mobile devices and emerging technologies

2. Digital Transformation and Connectivity

- Digital transformation of businesses and government institutions
- Integration of cloud computing, IoT devices, and remote work arrangements
- Increased reliance on interconnected systems and digital services

3. Cybercrime Sophistication

- Advanced techniques employed by cybercriminals
- Social engineering, ransomware attacks, and zero-day exploits
- Challenges to traditional security measures

4. Lack of Cybersecurity Awareness

- Insufficient awareness among individuals and businesses
- Lax security practices and vulnerability to cyber threats
- Lack of knowledge about common threats and social engineering techniques

5. Insider Threats

- Intentional or unintentional actions by employees
- Compromising cybersecurity through access to sensitive data
- Risks of inadvertent exposure or malicious activities

6. International Cyber Threats

- Cross-border cybercriminal networks and state-sponsored attacks
- Collaboration with international partners
- Addressing global cyber threats effectively

7.Economic Factors

- Growth of the digital economy
- Attractiveness to cybercriminals
- Financial losses and disruption of business operations

8.Regulatory Environment

- Cybersecurity laws and regulations
- Protection of critical infrastructure and personal data
- Influence on cybersecurity preparedness

9. Skills Gap and Workforce Shortage

- Shortage of skilled cybersecurity professionals
- Impacts on system protection and incident response
- Efforts to bridge the skills gap through training programs

10. Government Initiatives and Support

- Agencies and committees dedicated to cybersecurity
- Cybersecurity strategies, frameworks, and regulations
- Financial support for research and development initiatives

Key Takeaways

- The impact on cybersecurity in Thailand is driven by a combination of factors.
- Addressing these driving forces and challenges is crucial to building a resilient cybersecurity ecosystem.

Cybersecurity in Thailand:

Policy Recommendations

1. Enhance Awareness and Education

- Conduct public awareness campaigns
- Promote best practices for cybersecurity
- Incorporate cybersecurity education in curricula
- Bridge the skills gap through specialized training programs

2. Develop Incident Response Capabilities

- Establish a centralized cybersecurity incident response team
- Create incident response plans and conduct drills
- Encourage reporting and provide support to affected entities
- Foster information sharing and collaboration during investigations

3. Strengthen Critical Infrastructure Protection

- Identify critical infrastructure sectors
- Implement robust security controls and incident response plans
- Enhance collaboration among critical infrastructure operators
- Invest in advanced technologies for protection

4. Establish Public-Private Partnerships

- Collaborate to share information and resources
- Develop innovative cybersecurity solutions
- Facilitate knowledge exchange and research initiatives

5. Promote International Collaboration

- **Engage in international cyber diplomacy efforts**
- **Collaborate with partners and organizations**
- **Share threat intelligence and best practices**
- **Participate in joint exercises and simulations**

6. Foster Innovation and Research

- Support R&D initiatives in cybersecurity
- Encourage startups and entrepreneurs
- Promote cybersecurity competitions and challenges

7. Continuous Monitoring and Evaluation

- **Assess effectiveness of cybersecurity measures**
- **Stay updated on emerging threats**
- **Conduct audits and risk assessments**
- **Adapt strategies accordingly**

Conclusion

- Implementing these strategies will strengthen cybersecurity in Thailand
- Collaboration, continuous learning, and proactive measures are key to success


JANTA BHANDAR
Since 1602 A.D.
ATM
WE ONLY BARTER


Thank You