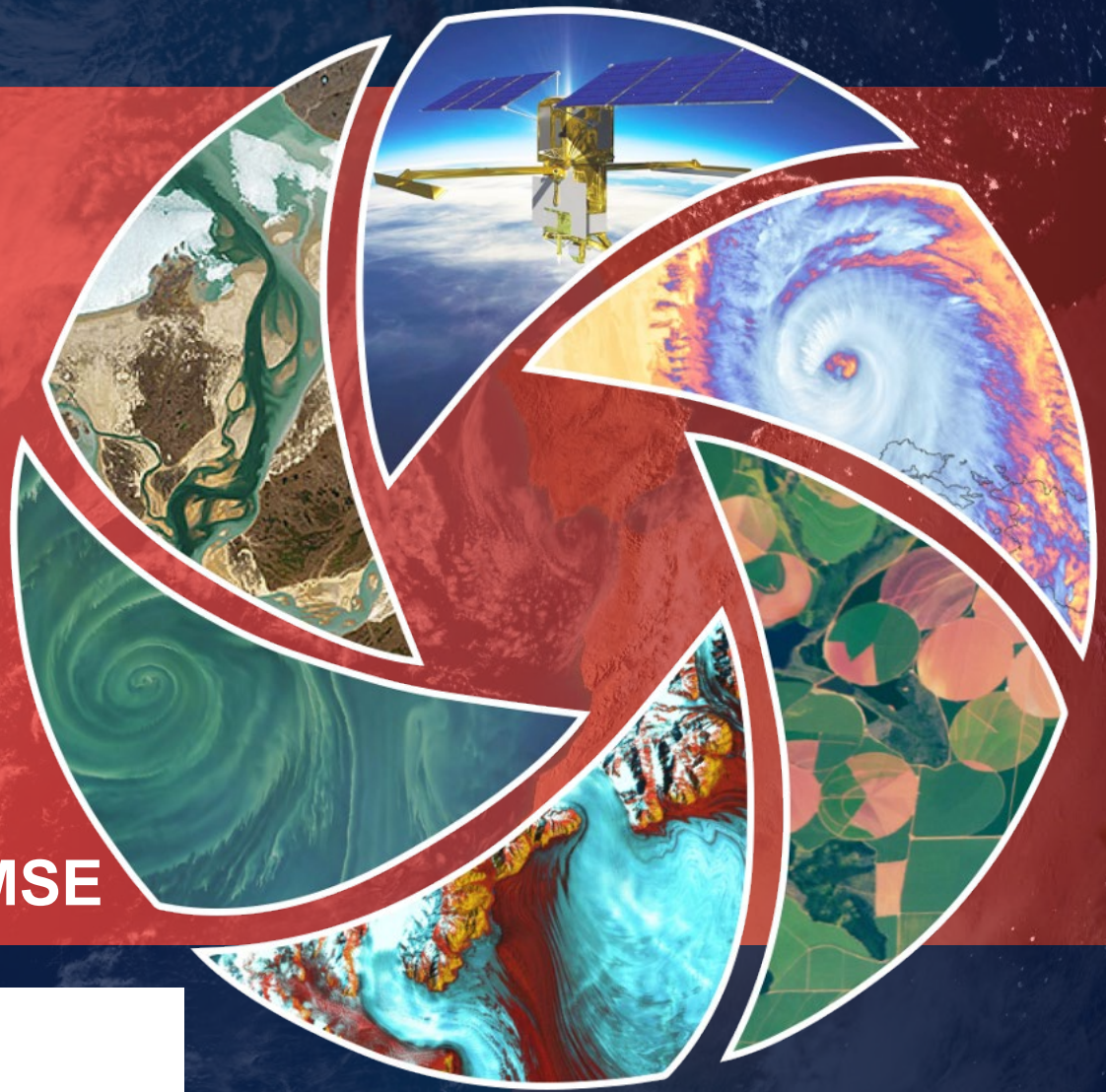
Understanding the Implications of Cyber-relevant Cognitive Vulnerabilities and Their Impacts on Protecting Space and Flight Systems from Cyber Attacks



March 22, 2024

Presented by: Prof. Lori D. Coombs, MBA, MSE

2024 Human Systems Conference
National Defense Industrial Association (NDIA)

Acknowledgements / Thanks:

- Institutional Affiliation: Marymount University
- **Don B. Coombs**, Director of WWCM Academy and WWCM for support & contributions.
- **Michael Hayden**, Program Chair, University of Arizona Global Campus (MISM)/(BISM) – Information Systems, Environmental Science and Advanced Air Mobility (AAM) collaboration.
  - UAGC is an FAA-approved Test Administrator of The Recreational UAS Safety Test (TRUST) for drones and unmanned aerial vehicles (UAV).
- **Doctoral Committee:** Dr. Nathan Green, Dr. Kateryna Nesvit, Dr. Alex Mbaziira, and Dr. Andrew Hall

Meet Lori D. Coombs

- **United States Senate / Capitol Hill**
  - Appointed Female Delegate to the DNC – Former President Al Gore and US Vice Presidential Nominee Lieberman (2000), US Presidential Nominee (2004), US Senator, (CT), Capitol Hill (1989-2013)
- **Marymount University**
  - Doctor of Science (D.Sc.) in Cybersecurity | MBA: Mgmt, MS: Systems Engineering, BS: Business Admin, Mktg
- **University of Arizona Global Campus**
  - Associate Professor – Master of Info Systems Management (MISM), Drone Aviation Education: Integrating drones in cybersecurity
- **University of Richmond**
  - Advisor – School of Professional & Continuing Studies: Distinguished Women in Leadership Program
- **WWCM and WWCM Academy (501c3)**
  - Cybersecurity, Heliophysics, Adv Air Mobility, Clean/Renewable Energy Sys, Sys & Cloud Integration, DevSecOps, AI, ML, PaaS, IaaS, C6ISR
- **NASA Goddard Spaceflight Center, DoD, Private & Public Industries**
  - Earthdata Infrastructure and Login | 2024 NDAA | HR 2670: Sections on the Committee on Science, Space & Tech, Aviation Assets, Software and Digital Tech Pilot Programs, R&D Test & Evaluation Div G: Intelligence Auth Act,| Title 51 USC: National and Commercial Space Programs
- **Research Interests**
  - Geospatial Systems, AI, ML, Cybersecurity, Environmental Science, Adv Air Mobility, Space Policy, Astronomy, Geology, Heliophysics

Agenda

- **Introduction**
  - ✓ How research supports Protection, Sustainment, and Warfighter Performance (PS&WP) initiatives for cognitive preparedness, assessment, warrior systems integration, and analysis
  - ✓ Key Terms, Acronyms, and Statistics
  - ✓ What a Space System Consists of
  - ✓ Cyber War: How Space and Flight Systems Can Become Compromised
    - ➢ **Super-EMP Weapons, Hypersonic Ballistic Tracking Space Sensors (HBTSS), U.S. Cyber Command (USCYCOM) for Defense Against Cyber Adversaries**
- **Research Objectives, Scope & Approach**

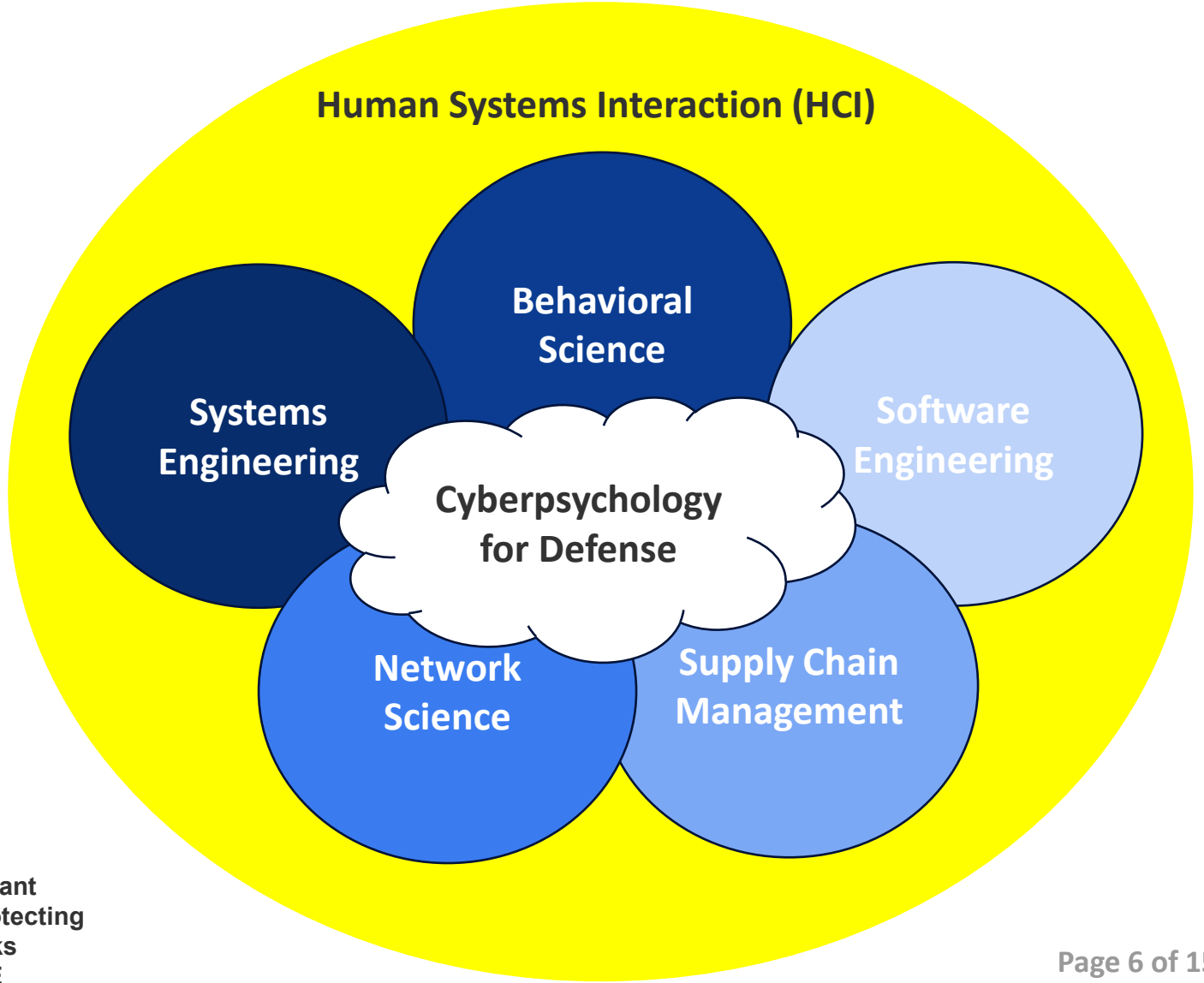
  General Strategy Used to Conduct Research
- **Conclusion**

  The importance of human systems interaction (HSI) to keep pace with the evolving needs of warfighters and the systems they use

Key Terms and Acronyms

Acronym	Definition
APhiDs	**Adaptive Psychological-informed Defenses** automate the Cyberpsychology-informed Defenses (CyphiDs) via modeling techniques.
C6 ISR	(**Command, Control, Communications, Computers, Cyber-defense, Combat Systems**) (**Intelligence, Surveillance and Reconnaissance**) are technologies and services that optimize situational awareness for decision makers.
CISA	**Cybersecurity and Infrastructure Security Agency:** Provides regional cyber and physical services to support security and cybersecurity events in the US.
CogVul	**Cognitive Vulnerability:** Erroneous belief, cognitive bias, or patterns of thought that predispose a person to psychological problems. The tendency of a person to generate overly negative inferences about the cause, consequences, and self-worth. (e.g., vulnerabilities to loneliness, depression, and anxiety, etc.); COVID-19 impacts
Cyber Deception	**Cyber Deception** is a defensive technique that considers human factors and the components of a cyber-attack. Deception aims to make it more difficult for hackers.
CyphiDs	**Cyberpsychology-informed Defenses** are developed by identifying the impacts of cyber-relevant cognitive vulnerabilities.
Cyberpsychology	**Cyberpsychology** studies the mental and emotional effects, implications, and phenomena of digital devices and internet use.
fMRI	**Functional Magnetic Resonance Imaging:** Measures the small blood flow that happen with brain activity. Used to examine which parts of the brain are handling critical functions. *(e.g., effects of stroke)*
fNIRS	**Functional Near-Infrared Spectroscopy:** Non-invasive, portable method that employs near-infrared light propagating through the scalp and brain for functional monitoring and imaging. *(Frontal regions)*
Human-Computer Interface (HCI)	The interface between humans and computers. *(e.g., desktop apps, internet browsers, and handheld computers that exploit graphical user interfaces (GUI) and voice user interfaces (VUI) for hands-free driving capabilities).*

Research Objectives & Scope



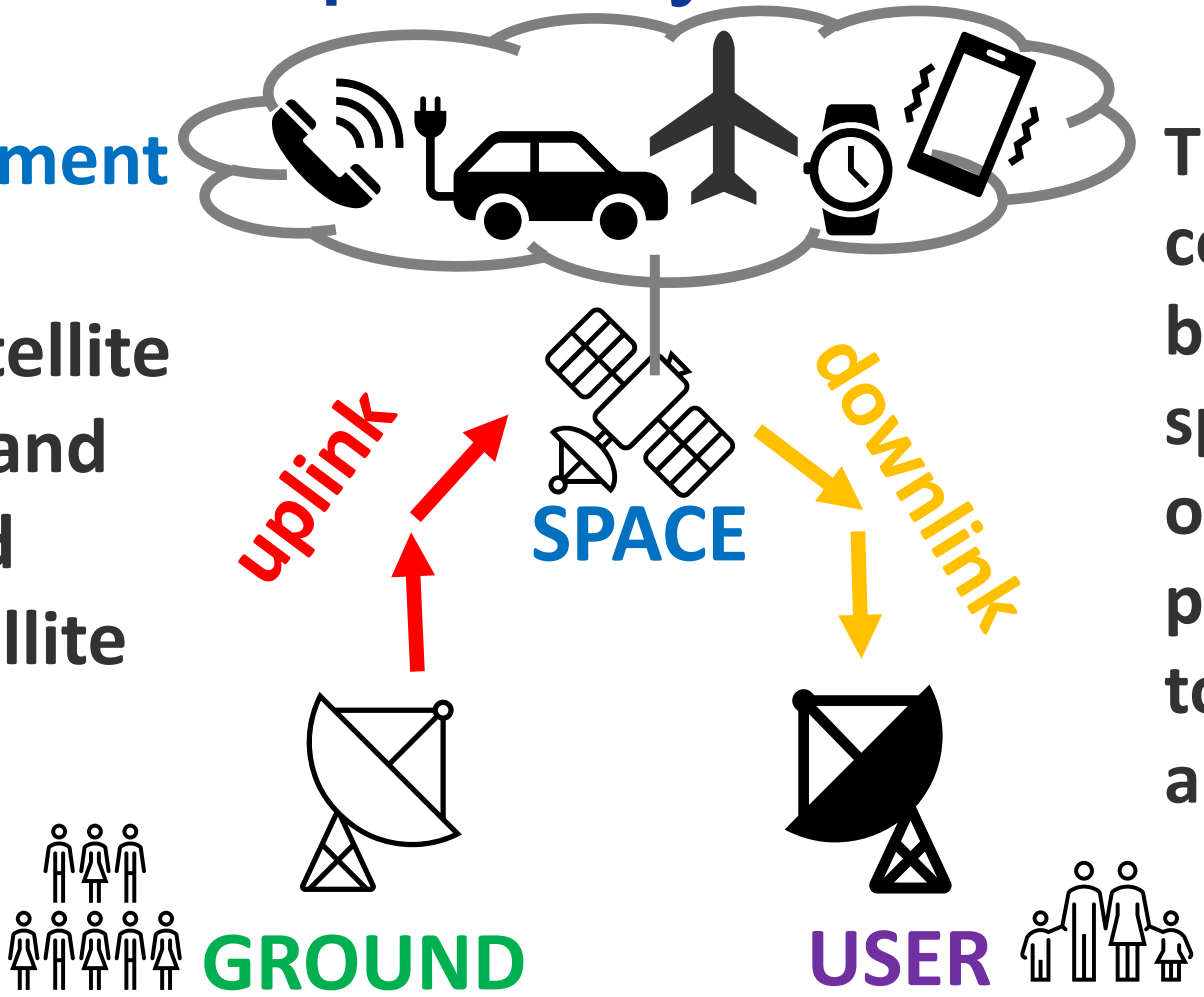
Cybercrime Impacts: Social Isolation During the COVID-19 Pandemic

- Daily cybercrime complaints increased by 300 – 400 %.
- Average ransomware payment amounts increased by 60 % in 2020.
- Google blocked 18 million COVID-19-related scams daily.
- Phishing attacks increased by 220 % compared to the annual average.

(Source: Fichtenkamm, M., Burch, G., Burch, J. (2022). Cybersecurity in a COVID-19 World: Insights on How Decisions Are Made. ISACA. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/cybersecurity-in-a-covid-19-world)

What does a space system consist of?

The space segment comprises the satellite or satellite constellation and the uplink and downlink satellite links.



The ground segment is comprised of ground-based elements of a space system used by operators and support personnel, as opposed to the space segment and user segment.

Source: This satellite system is *adapted from Defending, Spacecraft in the Cyber Domain. The Aerospace Corporation, 2019.*

Cyber War: How do space and flight systems become at risk to cyber attacks?

Common Cyber-Attacks to Segments			
SPACE	**LINK**	**USER**	**GROUND**
Command Intrusion	Spoofing	Phishing	Hacking
Payload Control	Denial of Service (DoS)	Out of Date / Unpatched Software	Hijacking
Denial of Service (DoS)	Malware	Ransomware	Malware
Malware		Social Engineering	
		Malware	

Source: ***Adapted from Defending, Spacecraft in the Cyber Domain, 2019. The 7 Biggest Cybersecurity Threats To Your Clients & Customers, Milosh, A., 2019.***

MAJOR THREAT TO ALL SEGMENTS:
Super Electromagnetic Pulses (EMPs)
(1) Natural: Solar Geomagnetic Disturbances, Extreme Space Weather
(2) Man-made: Thermonuclear Detonation or CYBER-ATTACK

“Approximately 58% of the world’s 7 billion people use the internet”

(Clement, 2019).

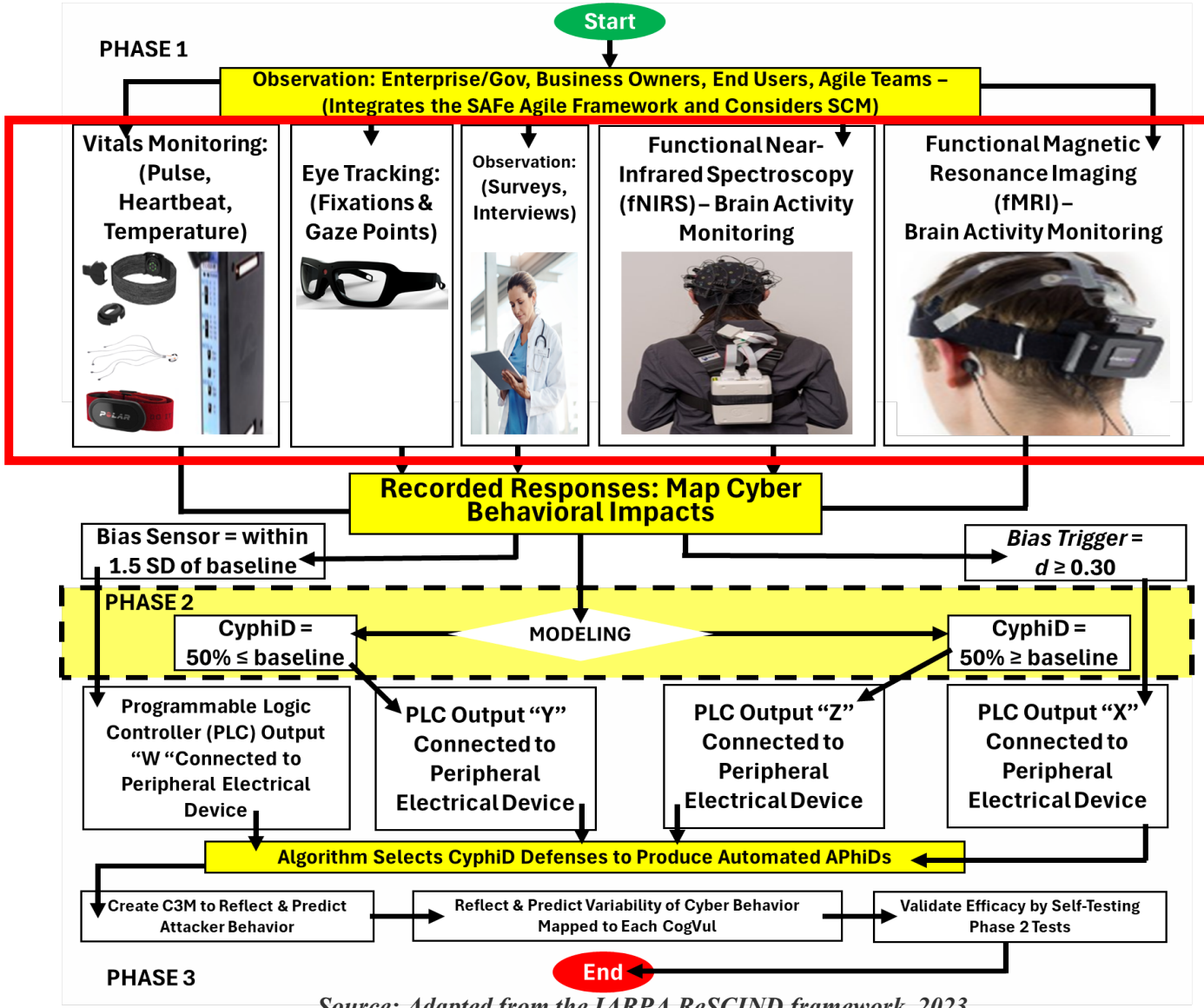
Relevant Areas to Cyberpsychology	
1	Online Behavior and Personality
2	Social Media Use and Psychological Functioning
3	Games and Gaming
4	Telepsychology
5	Virtual Reality (VR), Artificial Intelligence (AI) and Applications

(Source: Adapted from Cyberpsychology: Defining the Field. Ancis, J. (2020). Cyberpsychology Today.)

Research Approach – Phase 1: (Observation)

General Strategy Used to Conduct Research:

(**PHASE 1**): The Theory of Planned Behavior approach leverages understanding human factors that determine attitudes, behavioral intentions, and decision-making processes using questionnaires and observations that examine norms.

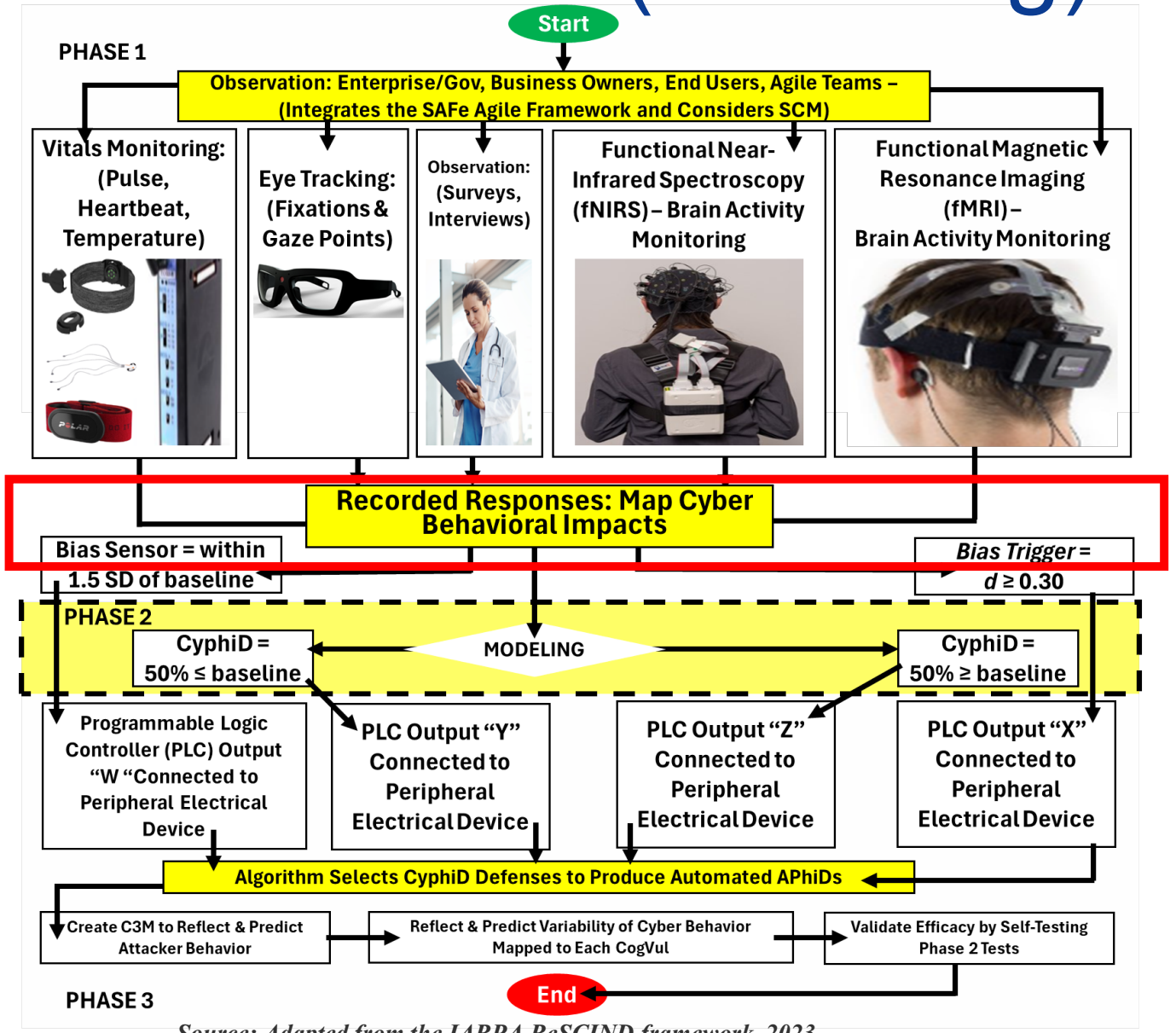


Source: Adapted from the IARPA ReSCIND framework, 2023.
Photo Credit: iMotions vitals, eye tracking, fNIRS and NIRx fNIRS products.

Research Approach – Phase 2: (Modeling)

General Strategy Used to Conduct Research:

(**PHASE II**): The Grounded Theory leverages ways to develop models that reflect and predict attacker behavior based on grounded data that will be systematically collected and analyzed to develop CyphiDs by qualitative observation.



Source: Adapted from the IARPA ReSCIND framework, 2023.
Photo Credit: iMotions vitals, eye tracking, fNIRS and NIRx fNIRS products.

Research Approach – Phase 3: (Automation)

General Strategy Used to Conduct Research:

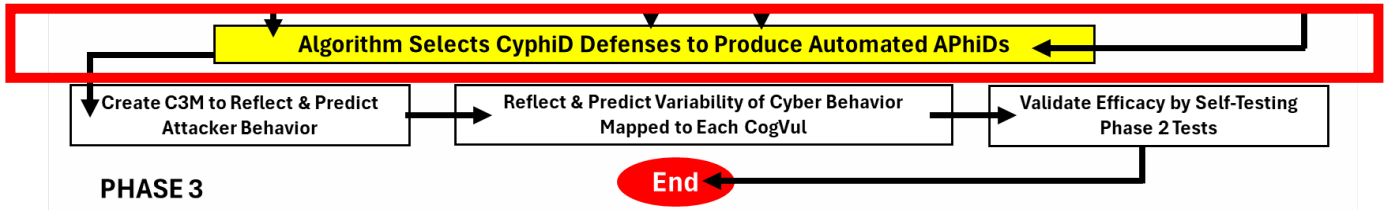
(**PHASE III**): The Quantum Cognition Theory can be used to select CyphiDs by creating cyber-specific computational cognitive models (**C3M**) and leveraging math principles involving quantum mechanics to understand human behavior, judgment, decision-making, reasoning, memory, and perception for probability-based decision models that produce Adaptive Psychological-informed Defenses (APhiDs) to automate the CyphiD sequences.

Within Research Scope

- **Predictive Analytics:** Uses statistical algorithms, machine learning (ML) to predict future events or outcomes.
- **Cognitive Analytics:** Uses AI and ML algorithms, to process unstructured data. Data Types: text, images, audio, and/or video
  - **Natural Language Processing (NLP):** Extracts large unstructured data sets
  - **Deep Learning Capabilities:** Predicts future patterns
  - **Automated Capabilities:** (**e.g., CyPhiDs**) Automates the extraction process. Reduces time in large sets.

Out of Research Scope

- **Prescriptive Analytics:** Takes predictive analytics a step further by providing recommendations and actions based on the predictions.
- Answers the "What should we do?"



Source: Adapted from the IARPA ReSCIND framework, 2023.
Photo Credit: iMotions vitals, eye tracking, fNIRS and NIRx fNIRS products.

Conclusion

- **Further research of Cyber Deception & Cyberpsychology for Defense**
  - Advanced Persist Threats
  - Anomaly Detection
  - AI Resilience
  - Securing Critical Cyber-physical Infrastructure
  - Vulnerability Identification
  - Insider, New and Emerging Cyber Threats
- **Future research supports:** National Security and Defense, Space Commercialization, Digital Transformation, and bolstering US cybersecurity posture to support Propulsion Technologies, Advanced Air Mobility, Heliophysics and Commercial Space Transportation advancements

Thank You! | Questions?

LORI D. COOMBS, MBA, MSE

WWCM
Science.Technology.Engineering.Art.Math

https://wwcapmgmt.com

Lori.D.Coombs@wwcapmgmt.com

WWCM ACADEMY
Science.Technology. Engineering. Art. Math

https://wwcmacademy.org

Lori.D.Coombs@wwcmacademy.org

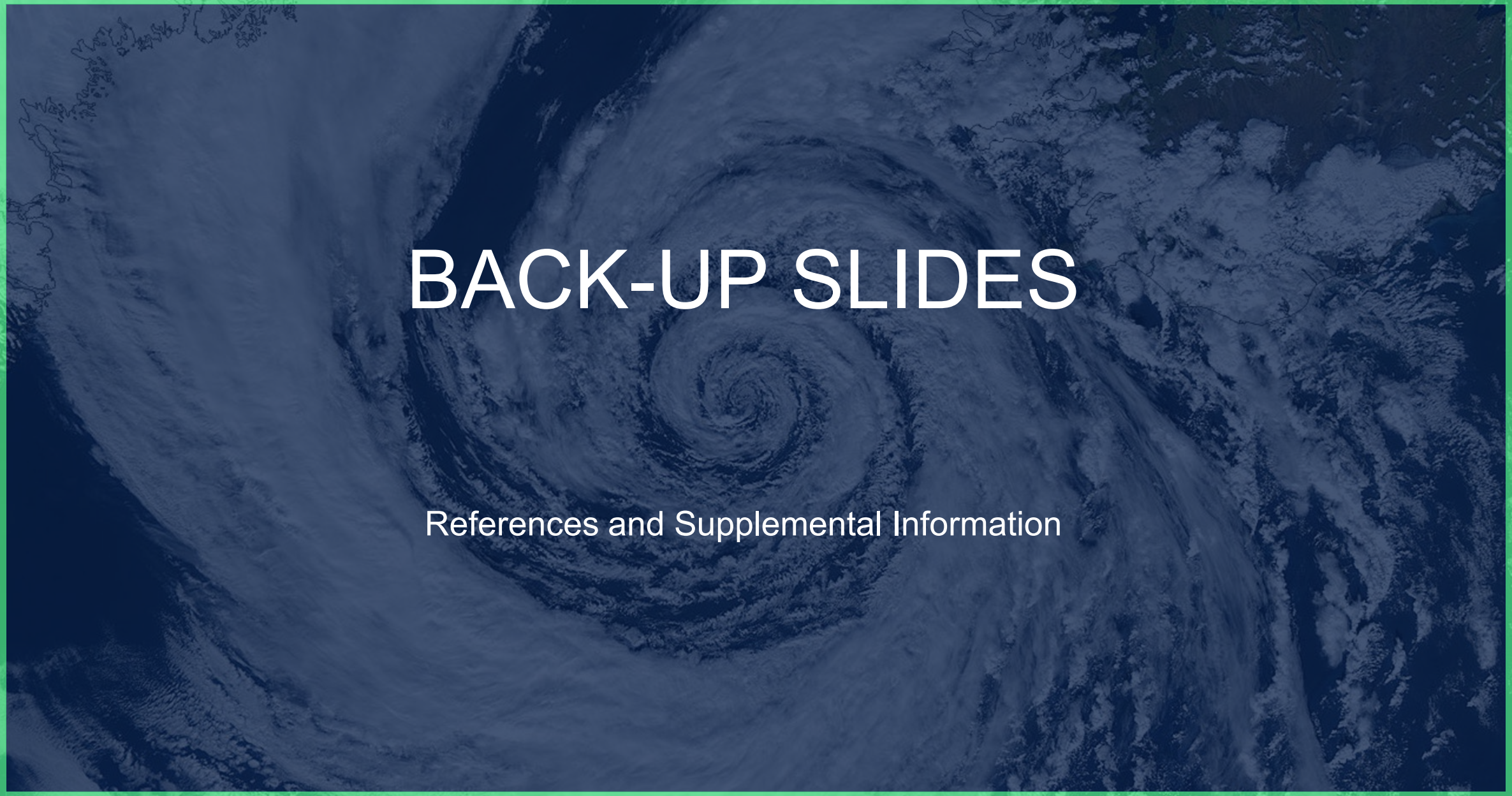
NASA

Lori.D.Coombs@nasa.gov

LinkedIn: https://www.linkedin.com/in/lori-d-coombs/

MARYMOUNT UNIVERSITY: LDC72459@marymount.edu

UNIVERSITY of ARIZONA Global Campus: Lori.Coombs@faculty.uagc.edu



BACK-UP SLIDES

References and Supplemental Information

References

Iyengar, R. and Duffy, C. (2021). CNN Business. Hackers Have a Devastating New Target. Retrieved from: https://www.cnn.com/2021/06/03/tech/ransomware-cyberattack-jbs-colonial-pipeline/index.html#:~:text=But%20there%20is%20a%20growing%20trend%20of%20hackers,make%20it%20easier%20to%20carry%20out%20such%20attacks.

Johnston, S. (2023). Machine Learning Algorithms Can Find Anomalous Needles in Cosmic Haystacks. Universe Today. Space and Astronomy News. Retrieved from: https://www.universetoday.com/163350/machine-learning-algorithms-can-find-anomalous-needles-in-cosmic-haystacks/

Kan, M. (2022). Hacker Uses James Webb Telescope Image for Malware Attack. PC Magazine. Retrieved from: https://www.pcmag.com/news/hacker-uses-james-webb-space-telescope-image-for-malware-attack

King, M. and Goguichvili, S. (2020). Wilson Center, CTRL Forward, Cybersecurity Threats in Space: A Roadmap for Future Policy.

Milosh, A. (2019). The 7 Biggest Cybersecurity Threats To Your Clients & Customers. Retrieved from: https://www.valueglide.com/blog/7corecompetenciesofsafe#:~:text=The%20seven%20core%20competencies%20of%20the%20Scaled%20Agile,Agility%206%20Continuous%20Learning%20Culture%207%20Lean-Agile%20Leadership

Mikalauskas, E. (2021). Critical US Infrastructure Can Be Hacked By Anyone. Cybernews. Retrieved from: https://cybernews.com/security/critical-us-infrastructure-can-be-hacked-by-anyone/

Rosenbusch, H., Soldner, F., Evans, A., Zeelenberg, M. (2021). Supervised machine learning methods in psychology: A practical introduction with annotated R code. Social and Personality Psychology Compass. Retrieved from: https://doi.org/10.1111/spc3.12579

Smith, A., & Anderson, M. (2018). Social media use 2018: Demographics and statistics. Pew Research Center: Internet, Science & Tech.

Thomas, D. (2023). Key findings: The State of Ransomware 2023 report. SC Media. Retrieved from: https://www.scmagazine.com/resource/key-findings-the-state-of-ransomware-2023-report

References

Ancis, J. (2020). Cyberpsychology: Defining the Field. Psychology Today. Retrieved from: https://www.psychologytoday.com/us/blog/the-cyberpsychology-page/202011/cyberpsychology-defining-the-field

Bailey, B., Speelman, R., Doshi, P., Cohen, N., Wheeler, W. (2019). Center for Space Policy and Strategy. Aerospace Corporation. Defending Spacecraft in the Cyber Domain.

Conca, J. (2023). China Has 'First-Strike' Capability To Melt U.S. Power Grid With Electromagnetic Pulse Weapon. Forbes. https://www.forbes.com/sites/jamesconca/2020/06/25/china-develops-first-strike-capability-with-electromagnetic-pulse/?sh=25925c2ee190

Bruza, P., Wang, Z., Busemeyer, J. (2015) July, pgs. 383-393. Quantum cognition: a new theoretical approach to psychology. Trends in Cognitive Sciences. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S1364661315000996

Brossard, D., & Scheufele, D. A. (2013). Social science. Science, new media, and the public. Science, 339(6115), 40–41. https://doi.org/10.1126/science.1232329

Cybersecurity & Infrastructure Security Agency (CISA). Secure-by-Design. (Oct 2023). Retrieved from: https://www.cisa.gov/securebydesign

Clement, J. (2019). Worldwide digital population as of October 2019. https://www.statista.com/statistics/617136/digital-population-worldwide.targetText=How%20many%20people%20use%20the,in%20terms%20of%20internet%20users

Decker, A. (2023). HASC chair: Space Command's temporary office is insecure. Officials: untrue. DefenseOne. Retrieved from: https://www.defenseone.com/policy/2023/09/space-command-pushes-back-rogers-claims-classified-work-abandoned-colorado-buildings/390767/

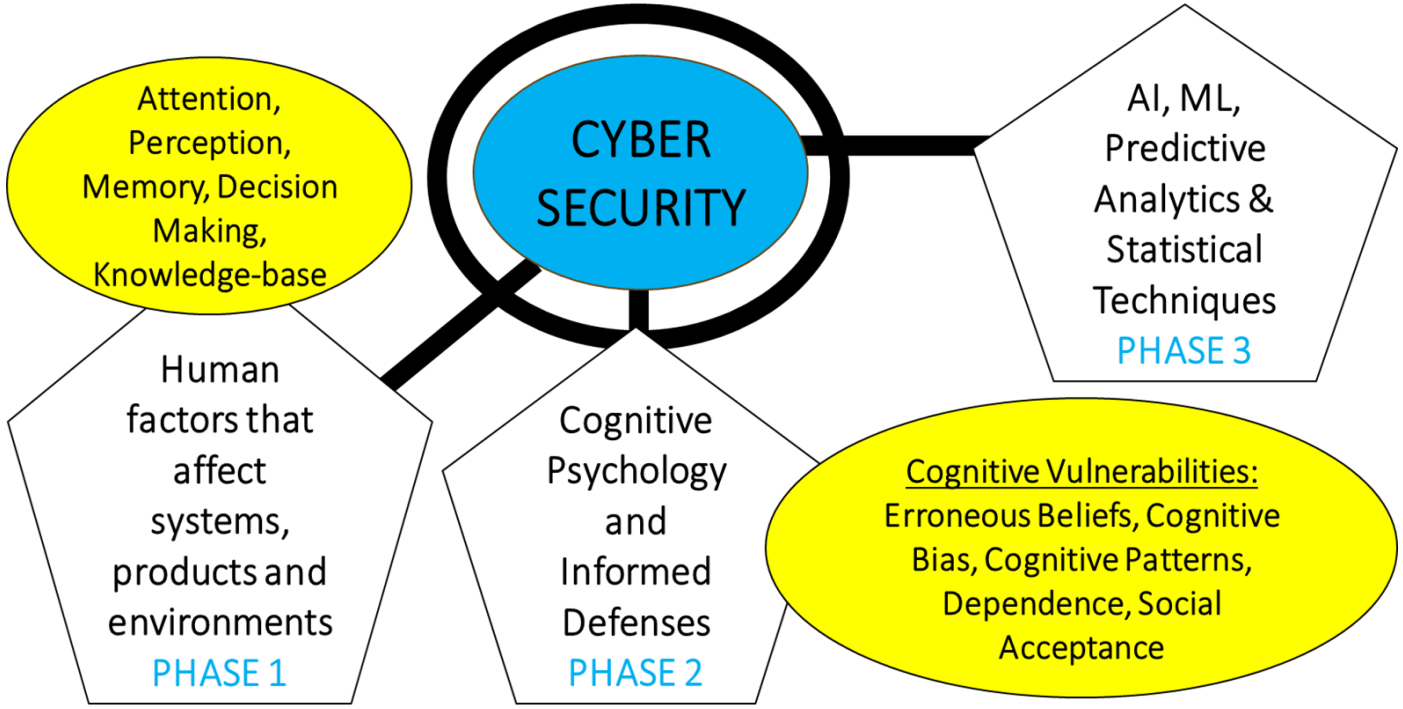
Fichtenkamm, M., Burch, G., Burch, J. (2022). Cybersecurity in a COVID-19 World: Insights on How Decisions Are Made. ISACA. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/cybersecurity-in-a-covid-19-world

Research Method

- Observation
- Expert Elicitation
- Mixed Methods
- Experimentation

3 STAKEHOLDER LEVELS:
Systems, Cloud Infrastructures, Applications

1. **Enterprise / Government / General Public End Users/Customers**
   a. Internal Service Level Agreements (SLAs)
2. **Business Owners (Product/Service Managers & Architects)**
   a. Software Bill of Materials (SBOMs)
3. **Agile Teams (Engineers, Developers, Systems Administrators)**
   a. Secure Coding Practices



Source: The Research Method is adapted from the IARPA ReSCIND framework, 2023.

SAFe 6.0