CICI: UCSS: Human-Centered Cybersecurity in Robotic Surgery (HCCRS) - Coordinating the Human and Cyber Infrastructure for Cybersecurity (Award 2615835)

Jackie Cha, PhD (University of Wisconsin-Madison) Jackie.Cha@wisc.edu
Dan Li, PhD (University of Washington) dli27@uw.edu

Department of Industrial and Systems Engineering
UNIVERSITY OF WISCONSIN–MADISON

INDUSTRIAL & SYSTEMS ENGINEERING

Motivation

Existing cyberinfrastructure security in robotic surgery do not fully consider *users'* cybersecurity awareness and knowledge as well as evaluate training and mitigation for cyberattacks

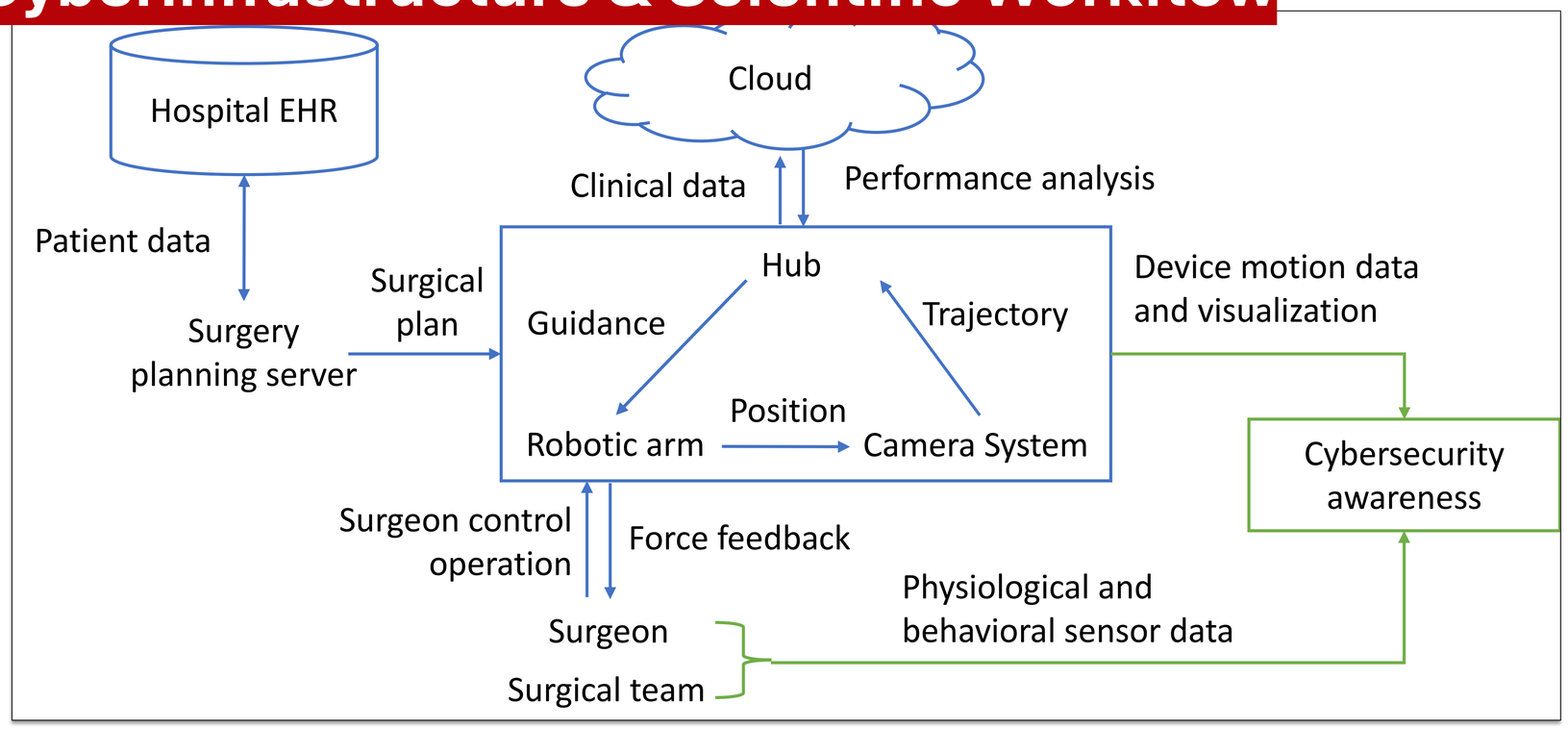
Goal

Design new human-centered algorithms to *detect, identify, and mitigate* cyberattacks in the robotic-assisted surgery (RAS) cyberinfrastructure

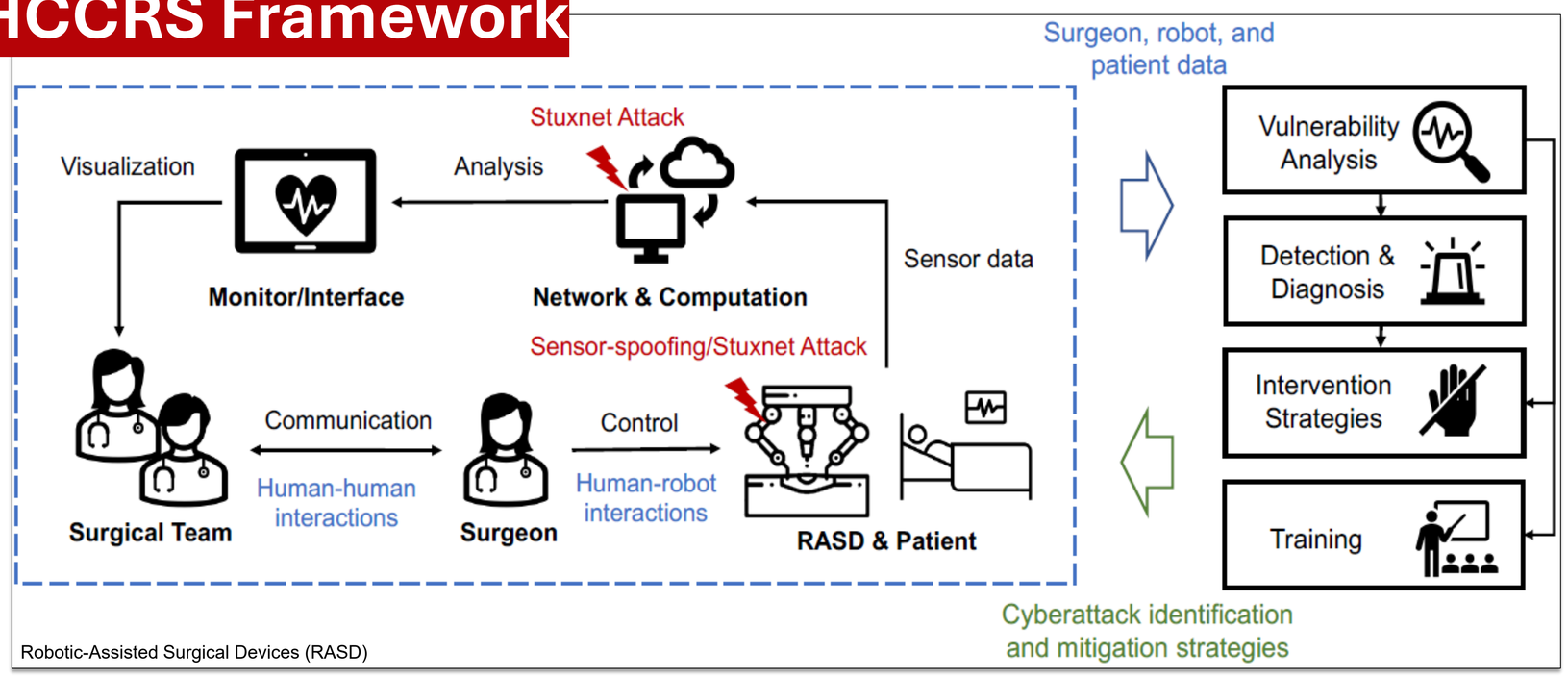
Research Thrusts

1. Identifying and quantifying robotic-assisted surgery (RAS) cybersecurity vulnerabilities and risks
2. Developing human-centered cyberattack detection and identification techniques
3. Mitigating cyberattack impact via training and an attack-impact transparency system for safer robotic surgery cyberinfrastructure

Cyberinfrastructure & Scientific Workflow



HCCRS Framework



Research Products

1. Fuller, P., Duffie, H., Li, D., Carbonell, A., Perkins, N., & Cha, J. S. (2026). Cybersecurity risks and vulnerabilities in robotic-assisted surgery. *Human Factors*, *68*(4), 447-469.
2. West, J., Singh, C., Cha, J., & Li, D. (2025). s-DResNet: an adversarial domain residual adaptation network for mental workload detection in robotic assisted surgeries. *IISE Transactions on Healthcare Systems Engineering*, *15*(3), 201-211.

Intellectual Merit

1. Assess RAS stakeholder cybersecurity awareness and evaluate HCCRS integration into RAS scientific workflows
2. Design an AI-driven framework to quantify cyberattack impact and identify attacks using fused multimodal physiological and clinical data
3. Develop RAS cybersecurity training materials and evaluate an attack identification transparency intervention through human-subjects experiments

Broader Impacts

1. Advance cybersecurity awareness among healthcare stakeholders, translatable to the National Initiative for Cybersecurity Education
2. Create a RAS cybersecurity training module and attack impact quantification system for operators and patients
3. Integrate developed tools and frameworks into future RAS scientific workflows and cyberinfrastructure