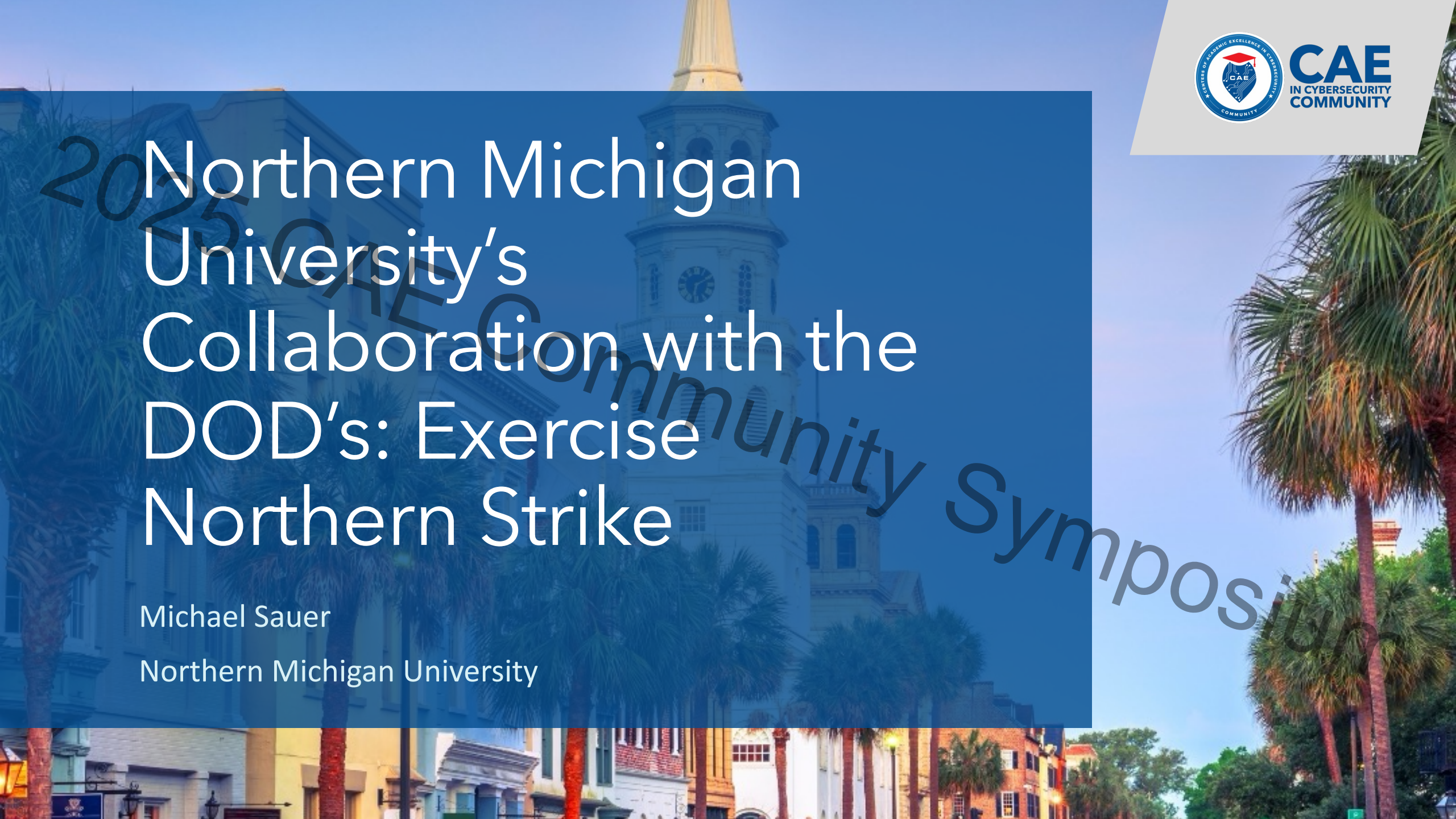


Northern Michigan University's Collaboration with the DOD's: Exercise Northern Strike

Michael Sauer

Northern Michigan University

PRESENTATION OUTLINE

- Northern Strike Overview
- Engagement with military and political leaders
- Mission Briefing
- Day 1 and Day 2 Objectives
- Skills and tools used in the mission
- Student reflection
- Pictures and video from the mission
- Summary and Lessons Learned
- Thanks
- Q &A

NORTHERN STRIKE EXERCISE

- Northern Strike is a joint training capability exercise that occurs annually at the **Camp Grayling – National All Domain Warfighting Center** in Grayling, Michigan. Camp Grayling is the largest National Guard base in the United States
- During the exercise, 5000+ National Guard, Active Duty, and NATO troops converged at Camp Grayling for joint force training in combat readiness
- 2024 was the first year that National Guard and NATO Cybersecurity teams used offensive cybersecurity skills to increase battlefield capability by providing intelligence and situational awareness to troops that were performing a live ground operation

NORTHERN STRIKE EXERCISE OVERVIEW

Sustainment
- Operational Logistics Control (BDE)
- Joint Medical Events (Role I – III)
- Air Mobility & Sustainment
- Joint Contested Logistics (LSCO)
- Pre-MOB evaluation/validation
- Agile Combat Employment (ACE)
- Multi-Modal Patient Movement (MMPM)

Fires
- Joint Fires Integration with BCD
- Operational Level Target Development
- Q53 Radar / Q64 Sentinel Radar
- Lethal and Non-lethal Effects
- Counter Land (AI/CAS)

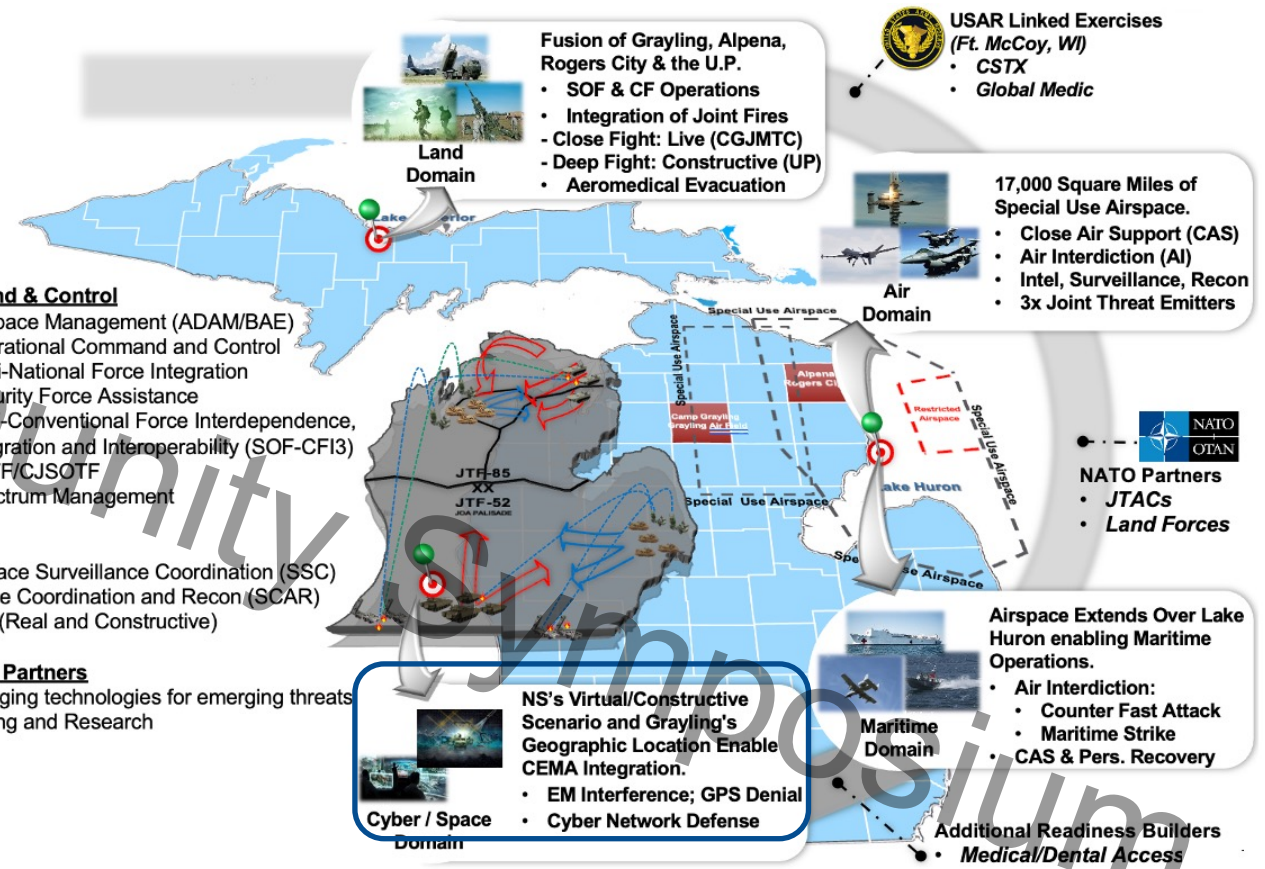
Movement & Maneuver
- Headquarters Mission Command (BDE)
- Full Mission Profiles (SOF)
- Foreign Internal Defense (SOF)
- Maritime Strike/Recovery
- Lift Capability
- Battalion Air Assault (R/W)
- Intra-theater Airlift
- Non-conventional Assisted Recovery (NAR)
- CSAR

Protection
- BDOC: CUAS/CEMA/Cyber
- Firefighter Operations
- Engineer Operations
- Airborne Maritime Mining (AMM)
- Integrated Air and Missile Defense

Command & Control
- Airspace Management (ADAM/BAE)
- Operational Command and Control
- Multi-National Force Integration
- Security Force Assistance
- SOF-Conventional Force Interdependence, Integration and Interoperability (SOF-CFI3)
- SOTF/CJSOTF
- Spectrum Management

Intel
- Surface Surveillance Coordination (SSC)
- Strike Coordination and Recon (SCAR)
- ISR (Real and Constructive)

Industry Partners
- Emerging technologies for emerging threats
- Testing and Research



POLITICAL / MILITARY ENAGAGEMENT

- U.S. Senator Elissa Slotkin visited Northern Michigan University's (NMU) campus to tour the cybersecurity center and Upper Peninsula Cybersecurity Institute in February of 2024
- Senator Slotkin is a former CIA officer who served three tours in Iraq and held defense and intelligence positions under President Bush and Obama and continues to have strong connections to the U.S. intelligence and military communities
- Senator Slotkin proposed the idea of the Northern Strike collaboration.
- NMU President, Brock Tessman, and NMU Executive Director of Government Relations, Deanna Hemmila, had a follow up visit to Slotkin's D.C. office to firm up details.
- From that visit, I was put in contact with the military resources required to approve the students' participation.

MISSION BRIEFING

- **Mission Objective: Discretely infiltrate a network used for communications and security cameras that are compromised by a foreign adversary**
  - U.S. ally Gorgon (Ukraine) is occupied by a hostile country, Donovia (Russia)
  - The U.S. is assisting the Gorgon troops in retaking a key piece of critical infrastructure located in a government building, which will be re-taken through an infantry assault
  - Gorgon indicates that the building has CCTV cameras which could be used to identify hostile troop positions within the building. However, Donovia has taken control of the network since the invasion
  - Allied cybersecurity teams are tasked with discretely infiltrating the network and security cameras so that they can provide a live video feed to the special forces team that is re-taking the building
  - The intelligence will provide a battlefield advantage and limit potential casualties during the assault

DAY 1

- **Red Team (Friendly)**
  - NMU students were tasked with being the red team and gaining access to the security cameras to provide a live feed to the task force assaulting the building
  - Students used network sniffing, and decompiling tools to determine the the authentication handshake between the camera and client application
  - Students researched known exploits for the types of cameras being used
  - Students used password cracking tools to
- **Blue Team (Hostile)**
  - Troops from the 172nd Cyber Protection squadron were tasked with protecting the network and alerting superiors if unusual activity was detected.
- **Mission Outcome**
  - The NMU Team was successful in gaining access to the cameras.

DAY 2

- Red and blue teams switched sides, so each team was able to practice offensive and defensive security skills.
- After the mission, NMU students partnered with troops from the 172nd Cyber Protection Team and worked alongside on both teams.
- In the afternoon, the teams visited the building in the urban combat range, where the building, security cameras, and simulated assault took place.
- In a truly unique learning opportunity, NMU students observed the assault team breach the building using the intelligence that was gained from the security cameras from a nearby roof top
- After the cybersecurity mission was completed, NMU was invited to a barbeque with troops from the 172nd Cyber Protection and Latvian Cybersecurity Teams
- NMU students and instructors were given 172nd insignia patches for their participation in the mission

TOOLS USED IN MISSION

- **Burp Suite**: Web security testing
- **Wireshark**: Network Protocol analyzer
- **Kali Linux & Hydra**
- **Hydra**
- **Reolink**: Web cameras and client
- **CLI Tools**: netstat, nmap, netcat
- **NCRC**: National Cyber Range Complex

REFLECTIONS

- **Student reflection: Jef Leroux**

  “The exercise gave us the chance to not only learn about how the Guard handles cybersecurity but also make important connections for a possible future career in defense and cyber operations. Being part of both red and blue team simulations provided invaluable hands-on experience in offensive and defensive cyber tactics. Observing National Guard soldiers in action highlighted the real-world applications of what we were learning and gave me a greater appreciation of the critical role cybersecurity plays in modern defense strategies.”

- **Professor reflection: Dr. Jim Marquardson**

  “I was impressed by our students' ability to analyze the situation, think critically and stay positive. I'm proud of the way our students represented Northern and demonstrated the hands-on skills our cybersecurity curriculum emphasizes. We were unsure what scenario our students would face, so we had to work collaboratively to solve several challenges. The National Guard was a great host, and we felt very welcomed. I look forward to participating again next year.”

PICTURES / VIDEO FROM MISSION

Mission Briefing

SUMMARY / LESSONS LEARNED

- NMU's participation is the first time there has been a collaboration with higher education at the Northern Strike exercise.
- Even through higher education collaboration had been on Northern Strike Leadership's "to-do" list, it likely would not have occurred without political support from Senator Slotkin.
- Engaging in a DOD military exercise required a lot of planning over the course of several months, but it is feasible.
- National Guard Leadership was pleased with the collaboration outcome and is excited to grow and formalize partnerships for future exercises.
- With this being the first year, NMU students lacked access to the National Cyber Range Complex (NCRC) used in the exercise. We were able to work around the limitation but were encouraged to get a student list to leadership earlier so background checks can be completed to grant access to the NCRC!

THANKS

- **Thank you to the following individuals who made this partnership and collaboration possible:**
  - U.S. Senator Elissa Slotkin
  - Major Ryan Reynolds, MI Army National Guard: DV Coordinator
  - Lieutenant Colonel John Brady, MI Air National Guard: Commander USAF 272nd Cyber Operations Squadron
  - Lieutenant Colonel Kathleen Prince-Sayward, MI Army National Guard 172nd Cyber Operations Team Chief
  - Captain Andrew Scott, MI Army National: 172nd Cyber Operations Team
  - Dr. Brock Tessman, NMU President
  - Deanna Hemmila, NMU Executive Director - Board and Government Relations
  - Carol Johnson, Dean – NMU College of Business

Thanks!

Questions ???