CSL
CENTER FOR STRATEGIC LEADERSHIP
U.S. ARMY WAR COLLEGE

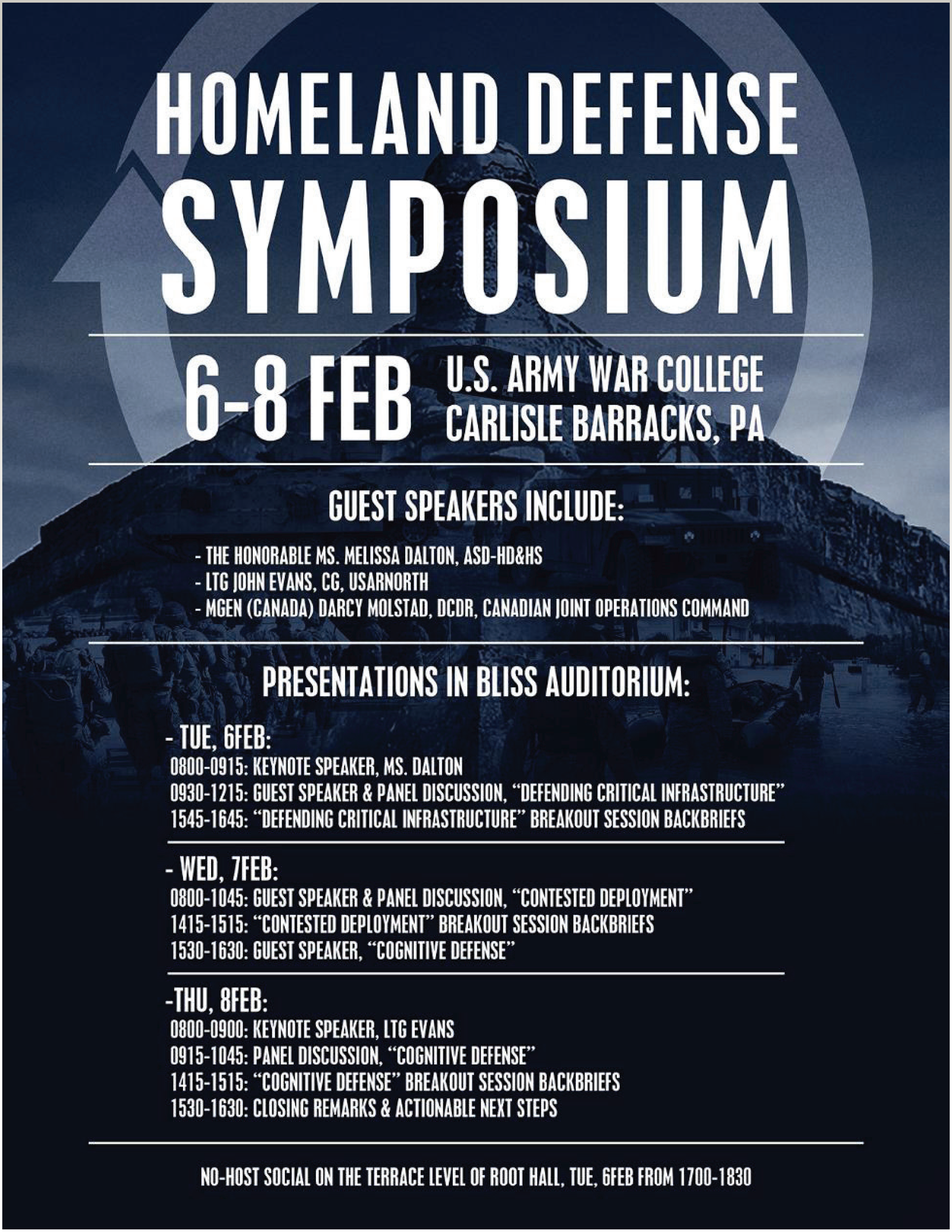
CONFERENCE PROCEEDINGS

FEBRUARY 2024

REESTABLISHING THE SANCTUARY: *HOMELAND DEFENSE AND SECURITY ISSUES*

Inaugural Homeland Defense Symposium
6–8 February 2024
Carlisle Barracks, PA

Edited by George M. Schwartz, Ed.D.



HOMELAND DEFENSE SYMPOSIUM

6-8 FEB U.S. ARMY WAR COLLEGE CARLISLE BARRACKS, PA

GUEST SPEAKERS INCLUDE:

- THE HONORABLE MS. MELISSA DALTON, ASD-HD&HS
- LTG JOHN EVANS, CG, USARNORTH
- MGEN (CANADA) DARCY MOLSTAD, DCDR, CANADIAN JOINT OPERATIONS COMMAND

PRESENTATIONS IN BLISS AUDITORIUM:

- TUE, 6FEB:

0800-0915: KEYNOTE SPEAKER, MS. DALTON
0930-1215: GUEST SPEAKER & PANEL DISCUSSION, "DEFENDING CRITICAL INFRASTRUCTURE"
1545-1645: "DEFENDING CRITICAL INFRASTRUCTURE" BREAKOUT SESSION BACKBRIEFS

- WED, 7FEB:

0800-1045: GUEST SPEAKER & PANEL DISCUSSION, "CONTESTED DEPLOYMENT"
1415-1515: "CONTESTED DEPLOYMENT" BREAKOUT SESSION BACKBRIEFS
1530-1630: GUEST SPEAKER, "COGNITIVE DEFENSE"

-THU, 8FEB:

0800-0900: KEYNOTE SPEAKER, LTG EVANS
0915-1045: PANEL DISCUSSION, "COGNITIVE DEFENSE"
1415-1515: "COGNITIVE DEFENSE" BREAKOUT SESSION BACKBRIEFS
1530-1630: CLOSING REMARKS & ACTIONABLE NEXT STEPS

NO-HOST SOCIAL ON THE TERRACE LEVEL OF ROOT HALL, TUE, 6FEB FROM 1700-1830

US ARMY WAR COLLEGE CENTER FOR STRATEGIC LEADERSHIP

The Center for Strategic Leadership provides strategic education, ideas, doctrine and capabilities to the Army, the Joint Force, and the Nation. The Army, Joint Force, and national partners recognize the Center for Strategic Leadership as a strategic laboratory that generates and cultivates strategic thought, tests strategic theories, sustains strategic doctrine, educates strategic leaders, and supports strategic decision making.

TABLE OF CONTENTS

FOREWORD

Defending the homeland is a whole-of-nation effort requiring us to think differently about protecting our country and way of life. The Department of Defense cannot defend the homeland alone. In an increasingly interconnected world, security of the homeland depends upon the cooperation of all stakeholders across the Department of Defense, the interagency, academia, the private sector, and our partners and allies.

As our competitive advantage over our adversaries erodes, the defense enterprise must radically transform to meet current and future threats. A multitude of stakeholders within and beyond the Department of Defense will play a role in this transformation effort. Legacy geographic and functional boundaries, parochial interests, and mission sets can no longer constrain us. It is incumbent upon all of us to build the community of interest to align priorities and resources to develop solutions.

Credible deterrence relies on the nation's ability to project power from the homeland in support of forward theaters. Successfully executing "fort to port" operations in support of a large-scale combat operation is difficult in a permissive environment. Multi-domain disruptions from an opportunistic adversary have the potential to cause delays with strategic implications. The Department of Defense's reliance on public and private transportation entities increases the risk and complexity of the problem set. We must take steps now to ensure our infrastructure is secure and resilient as we prepare for force projection in an uncertain environment.

Although our homeland is a mature theater, it is not set. A critical component of theater setting and campaigning is building relationships across the interagency and the private sector to identify and mitigate our strategic risk. The US Army War College HD symposium series is at the forefront of this effort to build a globally integrated approach to defend the homeland and ensure power projection. I hope the discussions during this symposium and future events inspire us to think differently as we apply bold and innovative solutions to our most sacred duty—defending the homeland.

John R. Evans, Jr.
Lieutenant General, US Army
Commanding General, US Army North

INTRODUCTION

Since 2018, the national security strategies of two administrations, as supported by several versions of the *National Defense Strategy* and *National Military Strategy*, have reflected an appropriate and growing concern over the security of the United States and its territories. As the nation's center for strategic thought in the Army, the US Army War College hosted the first of an annual series of Homeland Defense Symposiums at Carlisle Barracks in Pennsylvania February 6–8, 2024.

The purpose of the symposium was to examine the challenges of Homeland Defense in impending and future conflicts while advancing research and proposing solutions to strategic challenges facing the Army, Joint Force, and governmental agencies. I am proud to say the conference met its intended purposes. Partnering with leading agencies to examine these issues, this symposium informed the strategic thought being focused on homeland defense issues, both inside and out of the military, with a multi-faceted focus of deterring aggression, defeating an adversary should deterrence fail, and mitigating the impact of the adversary's actions against our people, our infrastructure, and our institutions.

We were delighted Ms. Dalton, Lieutenant General (LTG) Evans, other general officers and senior executives, and our comrades from Canada presented information and participated in discussions concerning this important topic. Additionally, a variety of subject matter experts presented original research to a combined audience of 130 in-person and 15 virtual participants. More than 40 organizations across the Total Army, Joint Force, civilian think tanks, and academic institutions were represented.

As you read this compendium, I am sure you will agree it made a major contribution to the existing body of knowledge regarding the mission, concepts, and challenges of homeland defense. The US Army War College will use the results of the symposium to shape continued examination of and offer solutions to this vital topic.

Bert B. Tussing
Professor and Director,
Homeland Defense and Security Issues
Center for Strategic Leadership
US Army War College

DAY 1

Opening Remarks

Brigadier General Robin B. Stilwell, the US Army War College Deputy Commandant—Reserve Affairs, welcomed the attendees on behalf of the Commandant, Major General David C. Hill, who was attending the Army Senior Leader Development Conference in Washington, DC. He opened his remarks by asking, "What is the primary theater of concern to the US Army?" He emphasized the homeland should always be. It is the base from which we project military power overseas, but it is no longer the sanctuary it once was, and therefore, this symposium is timely and topical.

Since the US Army War College has the responsibility to educate the next generation of strategic leaders for the US Army. The US Army War College is also the proponent for thought, vision, and leadership regarding strategic landpower, and that includes homeland defense. As a career National Guardsman, he considers himself to be a homeland defense practitioner, and therefore, he looks forward to the engaging topics and discussing them with the other attendees.

He concluded his remarks by thanking all attendees for making the time to spend the next few days on this important subject.

Keynote Speaker

Professor Bert Tussing introduced the keynote speaker, **Ms. Melissa Dalton**, the assistant secretary of defense for Homeland Defense and Hemispheric Affairs.

Because Homeland Defense is an important part of Department of Defense strategy, Ms. Dalton thanked the US Army War College for hosting this symposium and encouraged everyone to engage actively with other each other over the next three days. She highlighted how the homeland is no longer a sanctuary, and mentioned how defending the homeland is the number one priority in the 2022 *National Defense Strategy*.

She went on to discuss our current adversaries, the Peoples Republic of China and Russia, both have already used various nonkenetic measures to attack our economy, society, and our critically important defense industrial base.

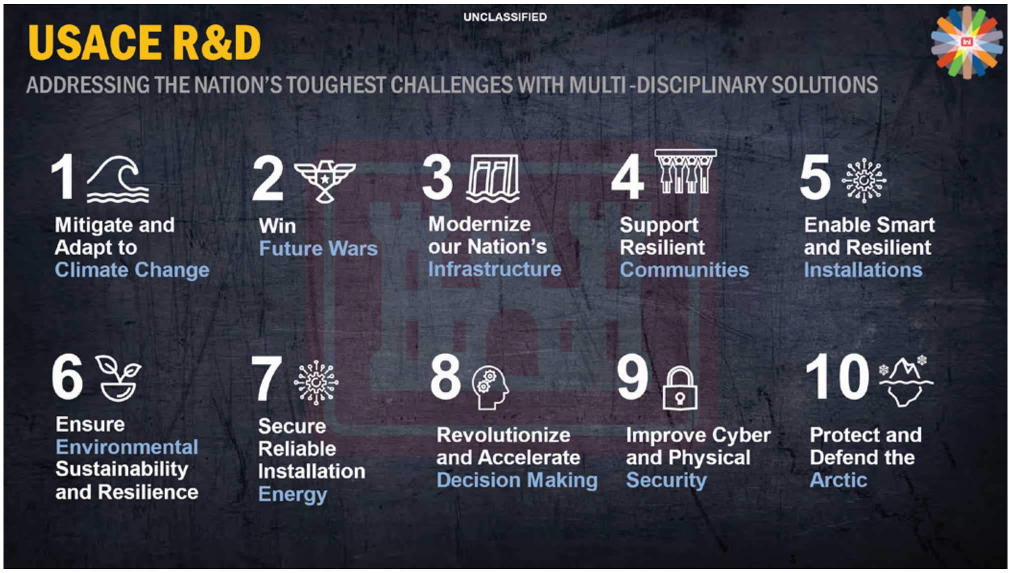
Ms. Dalton then shared information that the Homeland Defense Policy Guidance had been signed by the secretary of defense. In this document, there are initiatives for power projection; defense of critical infrastructure; guidance on building resiliency; continuity of government; and chemical, biological, radiological, nuclear, and explosive response operations.

During her remarks, Ms. Dalton provided key areas for critical thinking during the symposium: (1) defense of critical infrastructure; (2) contested deployment; and (3) cognitive defense. She then provided some ways forward that could help regarding homeland defense, such as strengthening the defense of critical infrastructure on installations, strengthening non-DOD infrastructure, and ensuring the defense industrial base is resilient. Further, she added that these key areas are central to homeland defense and affect our ability to project power. She highlighted how contested deployments could create the need for defense support of civil authorities and how that could compete with mobilization/deployment requirements (simultaneously creating a challenge and a gap).

Moreover, Ms. Dalton discussed human dimensions of homeland defense with a focus on the human-centric paradigm. She mentioned how our adversaries use social media to influence a population during elections, while targeting our society with false information. She offered some form of *cognitive defense* is necessary to defend our population against these influence operations. She emphasized that resiliency across the enterprise helps to ensure the Department of Defense can effectively execute its operations.

Featured Speaker

Dr. Igor Linkov from the US Army Corps of Engineers Research and Development Center spoke on *Infrastructure Resilience: How to Bring the Best Science to the Problem.*



UNCLASSIFIED

USACE R&D

ADDRESSING THE NATION'S TOUGHEST CHALLENGES WITH MULTI -DISCIPLINARY SOLUTIONS

1 Mitigate and Adapt to Climate Change

2 Win Future Wars

3 Modernize our Nation's Infrastructure

4 Support Resilient Communities

5 Enable Smart and Resilient Installations

6 Ensure Environmental Sustainability and Resilience

7 Secure Reliable Installation Energy

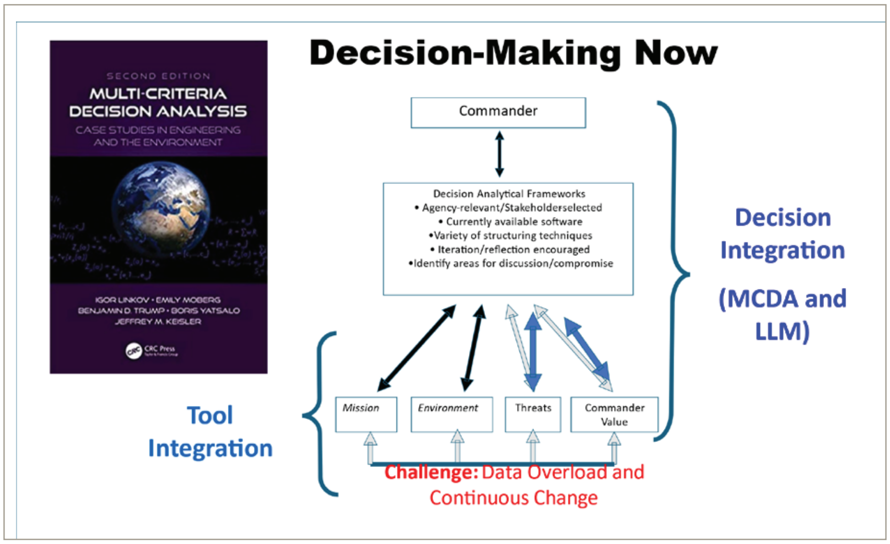
8 Revolutionize and Accelerate Decision Making

9 Improve Cyber and Physical Security

10 Protect and Defend the Arctic

Figure 1. The US Army Corps of Engineers Research and Development Center Research Areas.

After highlighting the research areas of the Engineers Research and Development Center (figure 1), Dr. Linkov addressed how leaders would previously make ad-hoc decisions transitioning into a decision-making process where there is too much data/information (that is, mission, environment, threats, commander's values); see figure 2. He stated as risk value rises, the cost of reducing risk rises to a point until the risk value flattens while cost continues to climb. Artificial intelligence (AI)/ machine learning could be used to better understand the resilience of complex systems though.



Decision-Making Now

SECOND EDITION
MULTI-CRITERIA DECISION ANALYSIS
CASE STUDIES IN ENGINEERING AND THE ENVIRONMENT
IGOR LINKOV • EMILY MOBERG
BENJAMIN D. TRUMP • BORIS YATSALO
JEFFREY M. KEISLER
CRC Press
Commander
Decision Analytical Frameworks
• Agency-relevant/Stakeholderselected
• Currently available software
•Variety of structuring techniques
• Iteration/reflection encouraged
•Identify areas for discussion/compromise
Mission
Environment
Threats
Commander Value
Tool Integration
Decision Integration
(MCDA and LLM)
Challenge: Data Overload and Continuous Change

Figure 2. Multi-Criteria Decision-Making.

He then discussed how risk and resiliency are not the same and should not be addressed the same way. He stressed that one cannot address resilience by trying to mitigate risk. He provided a definition of risk: threat–vulnerability–consequence. As performance declines, the likelihood of it cascading to other critical functions is more likely following a disruption unless resiliency is present.

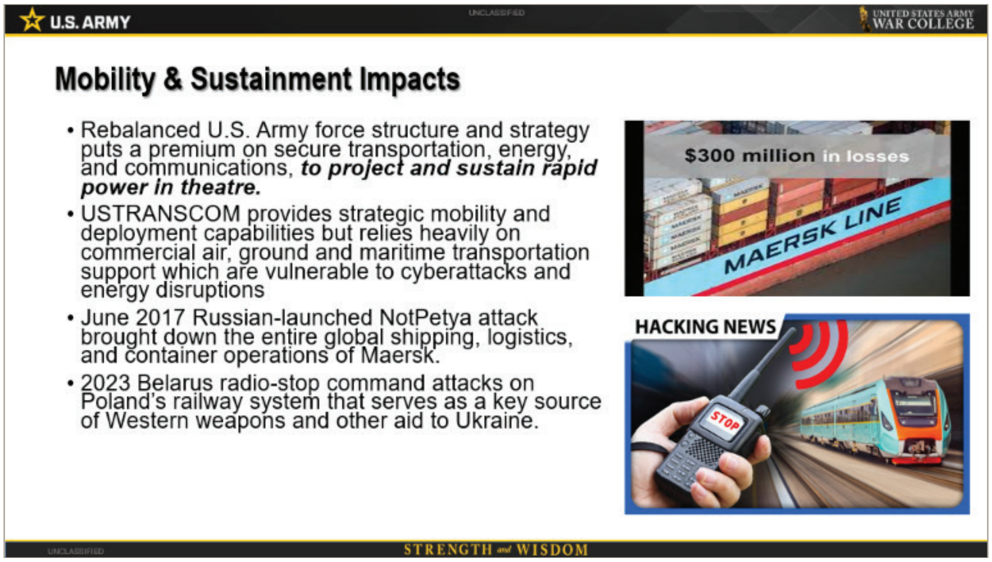
In reference to resilience planning, there is usually a small interface between military and civilian sectors, but when either is put in jeopardy, the interface will grow to support the one in jeopardy. In reference to this interface, Dr. Linkov posed a question: “Should we build to withstand or to recover?” He surmised because civilian-military is so much more connected than ever before, the interface is more important than ever.

Panel 1 - Defense of Critical Infrastructure Panel

The first panel included **Dr. Carol Evans**, director of the Strategic Studies Institute and the US Army War College Press, **Ms. Merideth Secor**, branch chief of the National Infrastructure Simulation and Analysis Center with Cybersecurity and Infrastructure Security Agency, and **Mr. Scott Aaronson**, vice president of security and preparedness at the Edison Electric Institute.

Dr. Evans spoke about moving away from the concept of protection and moving toward resilience. She mentioned critical infrastructure—such as mass transportation, energy, and communications—is a common target of our adversaries, and she encouraged partnerships across agencies and the public and private sectors.

She then described hybrid threats to NATO missions and capabilities and how our adversaries are penetrating the defense industrial base of alliance countries. Russia studies communications infrastructure and energy grid nodes for targeting purposes, while our reliance on critical equipment from China creates supply chain dependencies.



U.S. ARMY UNCLASSIFIED UNITED STATES ARMY WAR COLLEGE

Mobility & Sustainment Impacts

- Rebalanced U.S. Army force structure and strategy puts a premium on secure transportation, energy, and communications, ***to project and sustain rapid power in theatre.***
- USTRANSCOM provides strategic mobility and deployment capabilities but relies heavily on commercial air, ground and maritime transportation support which are vulnerable to cyberattacks and energy disruptions
- June 2017 Russian-launched NotPetya attack brought down the entire global shipping, logistics, and container operations of Maersk.
- 2023 Belarus radio-stop command attacks on Poland’s railway system that serves as a key source of Western weapons and other aid to Ukraine.

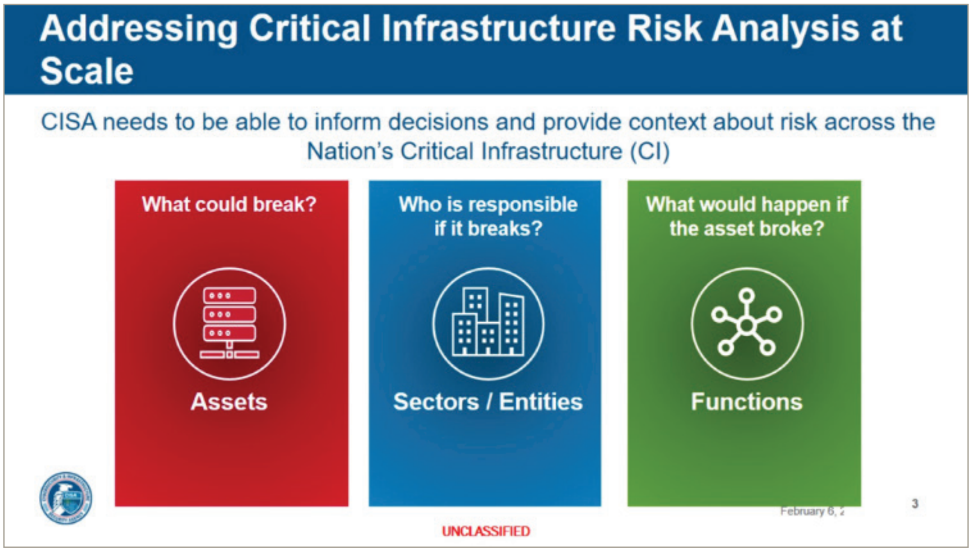
UNCLASSIFIED STRENGTH and WISDOM

Figure 3. Mobility and Sustainment Impacts of LSCO.

Dr. Evans then discussed potential mobility and sustainment impacts if the United States were to engage in large scale combat operations (LSCO); see figure 3. She highlighted our heavy reliance on commercial shipping for deployment and wondered, “Will they be there when we need them?” She hit on the topic of drone operations over bases in NATO as espionage activities. She stressed foreign investments in NATO countries and the possible issues that could cause. Dr. Evans discussed the People’s Republic of China and how it is acquiring key European defense industrial base manufacturers. Further activity of the People’s Republic of China with real-estate investments in key strategic locations. A bullet on her presentation was: Belt and Road Initiative investment in Europe’s electric grid (nuclear power plants in UK), seaports (control 22–25 percent of Europe’s ports either ownership or operations), telecommunications, transportation, etc. Increasing supply chain dependencies – Huawei/5G, undersea cables.

Ms. Secor highlighted the mission of the Cybersecurity and Infrastructure Security Agency, including:

1. Securing the .gov domain and reducing cyber vulnerabilities.
2. Understanding risk to critical infrastructure (see figure 4), particularly
    - Assets (*What could break?*),
    - Sectors/entities (*Who is responsible if it breaks?*), and
    - Functions (*What could happen if the asset broke?*).



Addressing Critical Infrastructure Risk Analysis at Scale

CISA needs to be able to inform decisions and provide context about risk across the Nation's Critical Infrastructure (CI)

What could break?

Assets

Who is responsible if it breaks?

Sectors / Entities

What would happen if the asset broke?

Functions

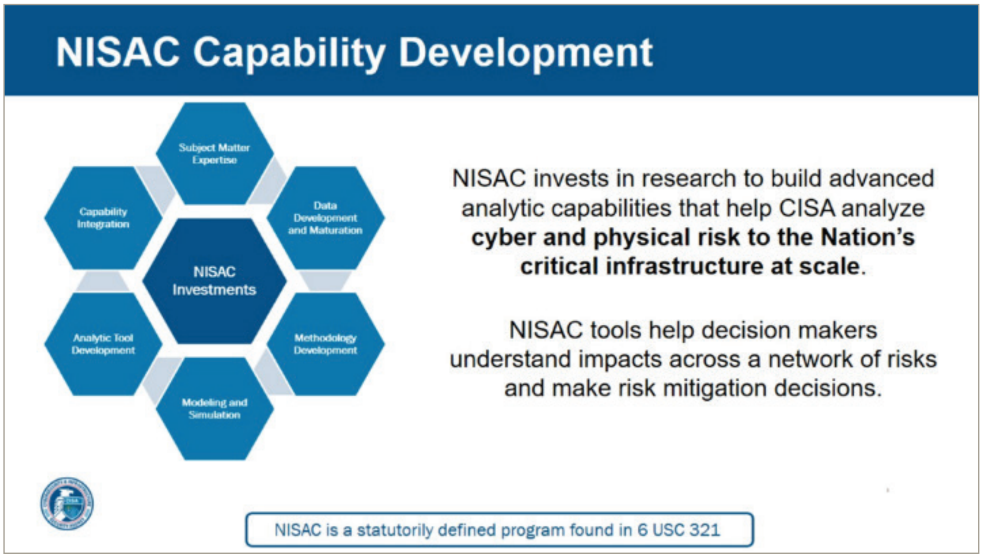
February 6, 2

3

UNCLASSIFIED

Figure 4. Critical Infrastructure Risk Analysis at Scale.

The National Infrastructure Simulation and Analysis Center develops capabilities by prioritizing subject matter expertise, data development and maturation, methodology development, modeling and simulation, analyst tools development, and capability integration. It has created STAR (Suite of Tools for the Analysis of Risk) which enables innovative, functional risk assessment of critical infrastructure at the national level. It analyzes the functions infrastructure provides, visualizes dependences across functions and assets, and overlays geospatial and asset data. The Suite of Tools for the Analysis of Risk tracks 1.8 million assets across the county.



NISAC Capability Development

Subject Matter Expertise

Data Development and Maturation

Methodology Development

Modeling and Simulation

Analytic Tool Development

Capability Integration

NISAC Investments

NISAC invests in research to build advanced analytic capabilities that help CISA analyze **cyber and physical risk to the Nation's critical infrastructure at scale.**

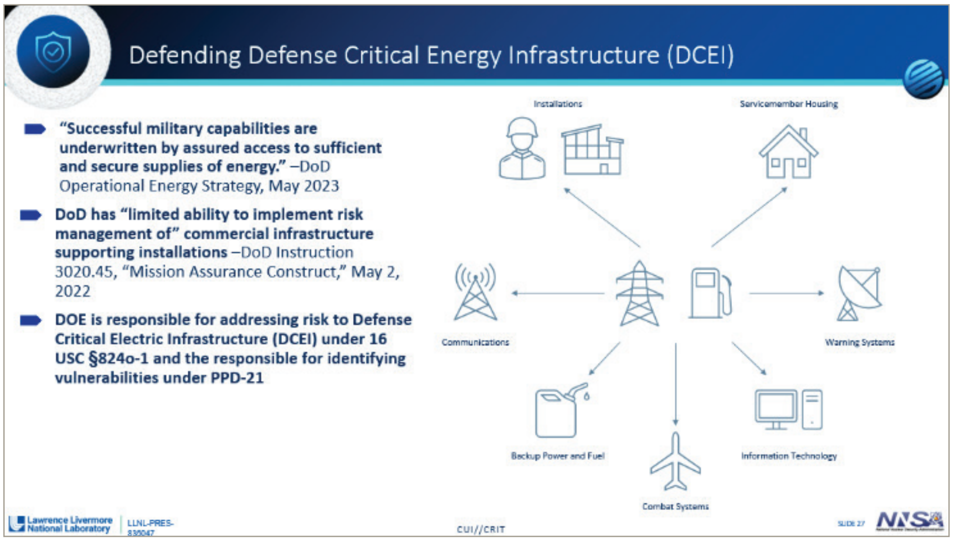
NISAC tools help decision makers understand impacts across a network of risks and make risk mitigation decisions.

NISAC is a statutorily defined program found in 6 USC 321

Figure 5. National Infrastructure Simulation and Analysis Center Capability Development.

In closing, Ms. Secor made a call to action to identify what we are missing, what we are not thinking about, and where we can find these capabilities.

Mr. Aaronson provided a private sector perspective, asking the question "Where does homeland security end and homeland defense begin?" He noted 85 percent of critical infrastructure is owned/operated the by civilian sector, and this infrastructure includes energy infrastructure (see figure 6). There has been an increase in acts of war (physical attacks), acts of God (extreme weather), and acts of the market (China).

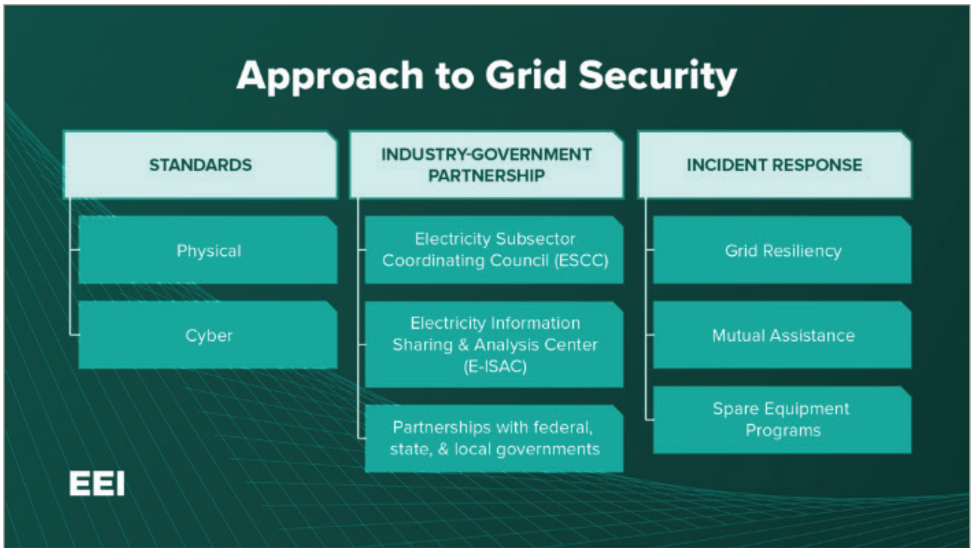


Defending Defense Critical Energy Infrastructure (DCEI)

- **"Successful military capabilities are underwritten by assured access to sufficient and secure supplies of energy."** –DoD Operational Energy Strategy, May 2023
- **DoD has "limited ability to implement risk management of" commercial infrastructure supporting installations** –DoD Instruction 3020.45, "Mission Assurance Construct," May 2, 2022
- **DOE is responsible for addressing risk to Defense Critical Electric Infrastructure (DCEI) under 16 USC §824o-1 and the responsible for identifying vulnerabilities under PPD-21**

Figure 6. Defending Defense Critical Energy Infrastructure.

He stated reliability standards are in place, but regulation is not security and if used as security will telegraph capabilities. Mr. Aaronson also stressed partnerships across government agencies and critical infrastructure sectors, including information sharing and operational collaboration (see figure 7). He provided an example from Ukraine for his discussion.



Approach to Grid Security

STANDARDS	INDUSTRY-GOVERNMENT PARTNERSHIP	INCIDENT RESPONSE
Physical	Electricity Subsector Coordinating Council (ESCC)	Grid Resiliency
Cyber	Electricity Information Sharing & Analysis Center (E-ISAC)	Mutual Assistance
	Partnerships with federal, state, & local governments	Spare Equipment Programs

Figure 7. Grid Security.

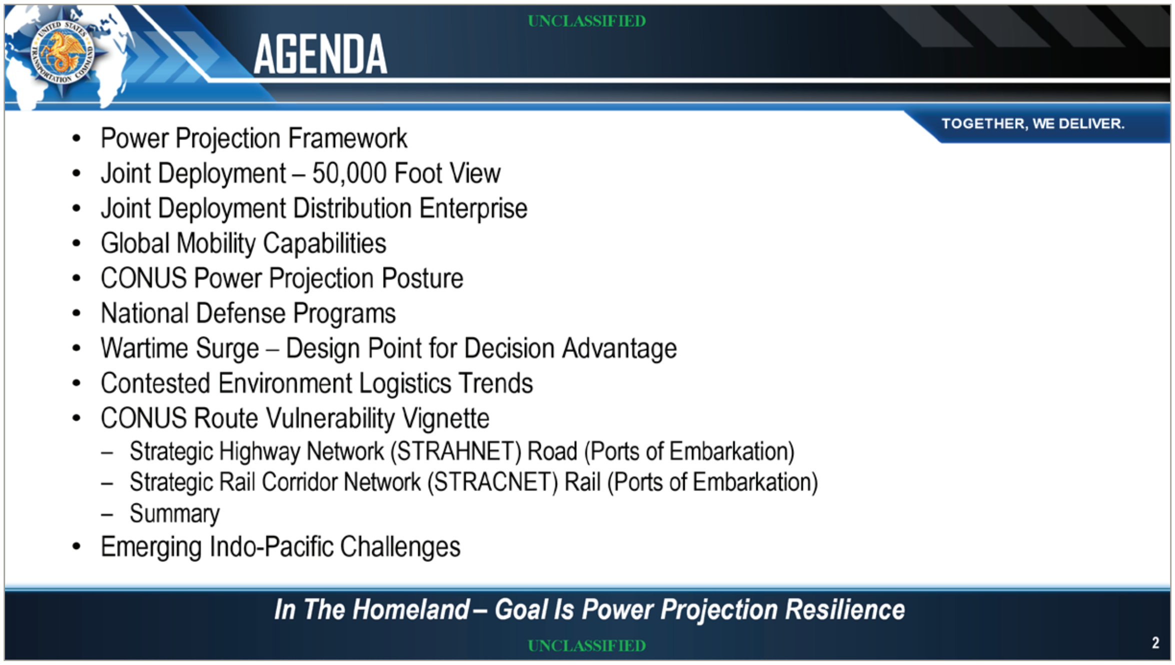
He then concluded by stating the ability to overcome incidents requires humans who have been trained, hardened infrastructure, and the ability to communicate. We can ensure deterrence is given high priority by ensuring: (1) an attack does not have the intended impact; and (2) attacks have consequences by maintaining the ability to respond. Our approach has to raise the costs for our adversaries, while lowering costs for ourselves.

DAY 2

Featured Speaker

Mr. Bruce Bussler is the director of the United States Transportation Command Joint Distribution Process Analysis Center spoke on *Contested Deployment.*

Mr. Bussler began his comments by stating the ability to project power is uniquely American, but with the potential for contested mobilization and deployments, the homeland is no longer a sanctuary. If our adversaries can tie up our forces at home, then it is to their benefit. Mr. Bussler spoke on several topics as shown in figure 8.



UNCLASSIFIED

AGENDA

TOGETHER, WE DELIVER.

- Power Projection Framework
- Joint Deployment – 50,000 Foot View
- Joint Deployment Distribution Enterprise
- Global Mobility Capabilities
- CONUS Power Projection Posture
- National Defense Programs
- Wartime Surge – Design Point for Decision Advantage
- Contested Environment Logistics Trends
- CONUS Route Vulnerability Vignette
  - Strategic Highway Network (STRAHNET) Road (Ports of Embarkation)
  - Strategic Rail Corridor Network (STRACNET) Rail (Ports of Embarkation)
  - Summary
- Emerging Indo-Pacific Challenges

In The Homeland – Goal Is Power Projection Resilience

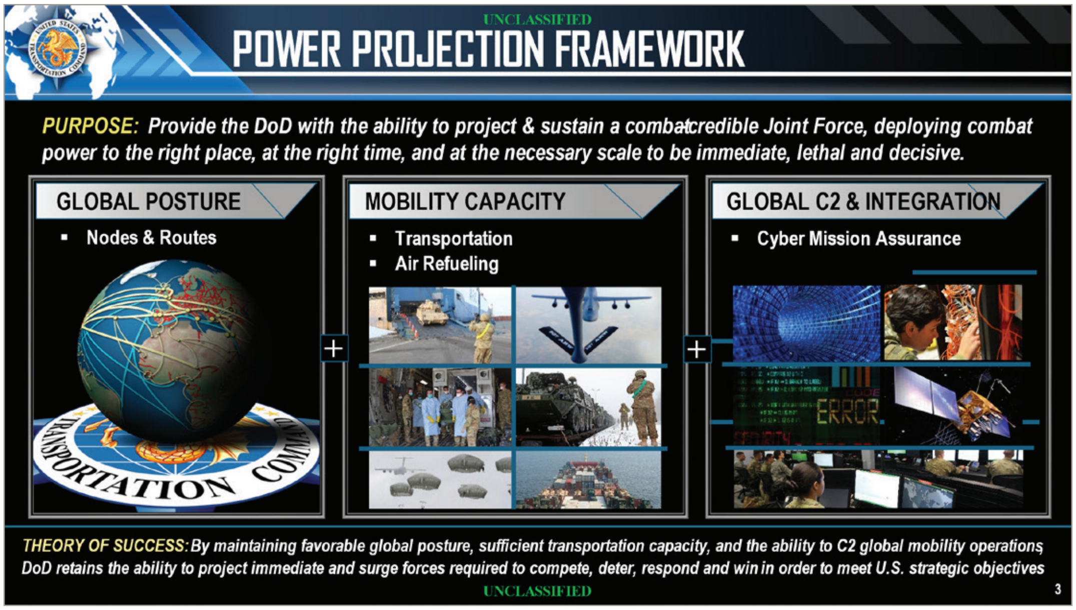
UNCLASSIFIED

2

Figure 8. Agenda for Mr. Bussler's Presentation.

The first topic was the power projection framework (see figure 9) and its ability to provide the Department of Defense with the ability to project and sustain a combat-credible Joint Force. In essence, deploying combat power to the right place, at the right time, and at the necessary scale to be immediately lethal and decisive. He then asserted homeland defense is our number-one priority.

Regarding Global C2 and Integration, he noted United States Transportation Command has been experimenting with AI, but in his opinion it is not a magical tool. To highlight the challenge with emerging technology, he posed the question "How do we use technology that is available to us to predict the future?"



UNCLASSIFIED

POWER PROJECTION FRAMEWORK

PURPOSE: Provide the DoD with the ability to project & sustain a combatcredible Joint Force, deploying combat power to the right place, at the right time, and at the necessary scale to be immediate, lethal and decisive.

GLOBAL POSTURE

- Nodes & Routes

MOBILITY CAPACITY

- Transportation
- Air Refueling

GLOBAL C2 & INTEGRATION

- Cyber Mission Assurance

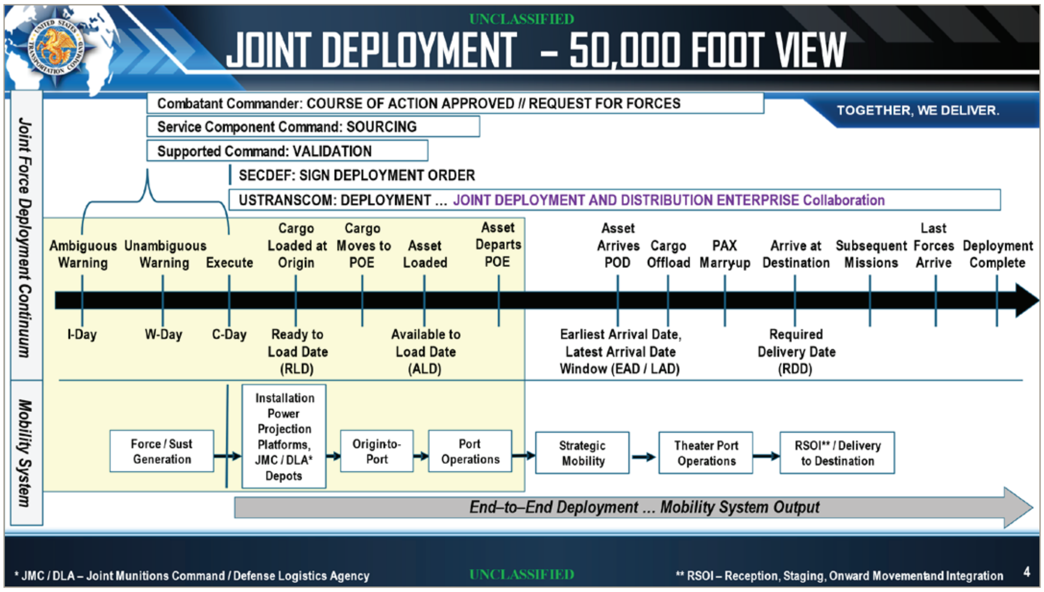
THEORY OF SUCCESS: By maintaining favorable global posture, sufficient transportation capacity, and the ability to C2 global mobility operations DoD retains the ability to project immediate and surge forces required to compete, deter, respond and win in order to meet U.S. strategic objectives

UNCLASSIFIED

3

Figure 9. Power Projection Platform.

Next, Mr. Bussler spoke about Joint Deployment, offering a high-level view (figure 10). He briefly explained United States Transportation Command has the ability to look at indications and warnings, and utilizes them to know when to start a deployment. He posed another question to the audience: "How do we know when the consequential things occur during the deployment timeline?" Here he added that homeland is not just CONUS. For USTRANSCOM to synchronize global mobility, Alaska, Hawaii, and Guam are important, and this synchronization requires coordination/collaboration with other combatant commands.



UNCLASSIFIED

JOINT DEPLOYMENT – 50,000 FOOT VIEW

TOGETHER, WE DELIVER.

Combatant Commander: COURSE OF ACTION APPROVED // REQUEST FOR FORCES

Service Component Command: SOURCING

Supported Command: VALIDATION

SECDEF: SIGN DEPLOYMENT ORDER

USTRANSCOM: DEPLOYMENT ... JOINT DEPLOYMENT AND DISTRIBUTION ENTERPRISE Collaboration

* JMC / DLA – Joint Munitions Command / Defense Logistics Agency

UNCLASSIFIED

** RSOI – Reception, Staging, Onward Movementand Integration

4

Figure 10. Joint Deployment.

On the topic of the Joint Deployment Distribution Enterprise (figure 11), Mr. Bussler stated that maritime capability is paramount because more than 90 percent of combat forces deploy by ship. He said the enterprise is heavily dependent on commercial providers for rail and trucks. Communication with these assets is unclassified and vulnerable to cyber risks, so USTRANSCOM must work with commercial partners to mitigate those risks and focus its efforts on the operational systems (for example, scheduling, tracking) to minimize possible disruptions.

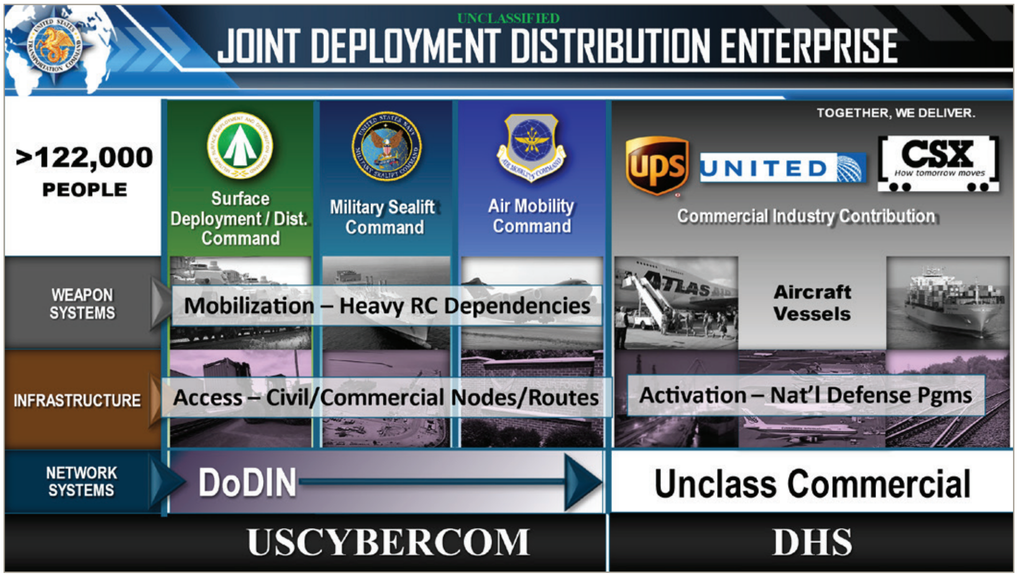


Figure 11. Joint Deployment Distribution Enterprise.

Regarding Global Mobility Capabilities (figure 12), Mr. Bussler stated that having a forward posture enables meeting deployment timelines. He emphasized the most stress in the system is with air refueling. He also noted that aeromedical airlift as an important and highly visible mission, it is important not to terminate this mission in theater; the process must include return to CONUS.

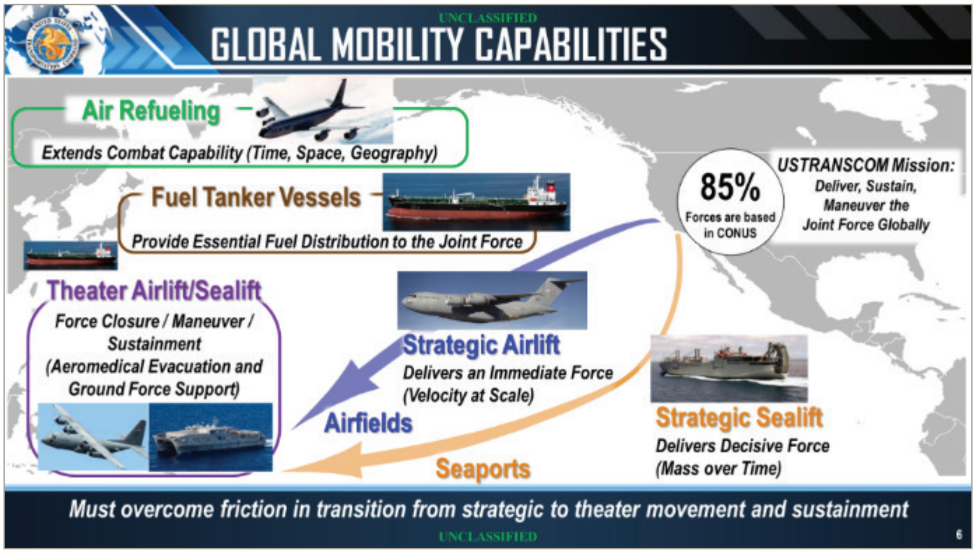
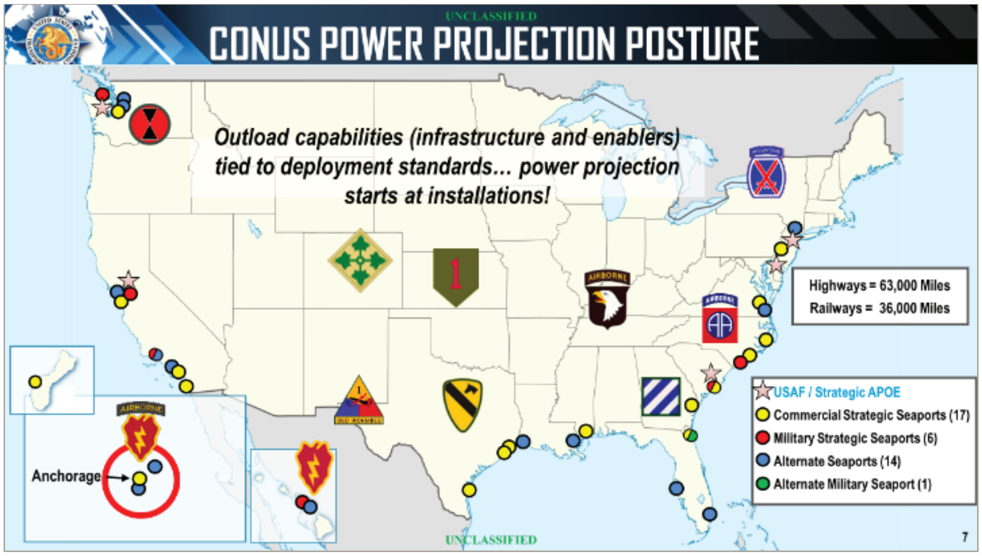

UNCLASSIFIED
GLOBAL MOBILITY CAPABILITIES
Air Refueling
Extends Combat Capability (Time, Space, Geography)
Fuel Tanker Vessels
Provide Essential Fuel Distribution to the Joint Force
85%
Forces are based in CONUS
USTRANSCOM Mission:
Deliver, Sustain, Maneuver the Joint Force Globally
Theater Airlift/Sealift
Force Closure / Maneuver / Sustainment
(Aeromedical Evacuation and Ground Force Support)
Strategic Airlift
Delivers an Immediate Force
(Velocity at Scale)
Airfields
Seaports
Strategic Sealift
Delivers Decisive Force
(Mass over Time)
Must overcome friction in transition from strategic to theater movement and sustainment
UNCLASSIFIED
6

Figure 12. Global Mobility Capabilities.

Mr. Bussler then spoke about the CONUS Power Projection Posture. He detailed out the thought regarding outload capabilities (infrastructure and enablers tied to deployment standards with power projection starting at installations). He closed this part of his presentation by touching on the topic of how the electrical grid and water are on the periphery requiring a partnership with other federal agencies such as the Federal Emergency Management Agency.



UNCLASSIFIED

CONUS POWER PROJECTION POSTURE

Outload capabilities (infrastructure and enablers) tied to deployment standards... power projection starts at installations!

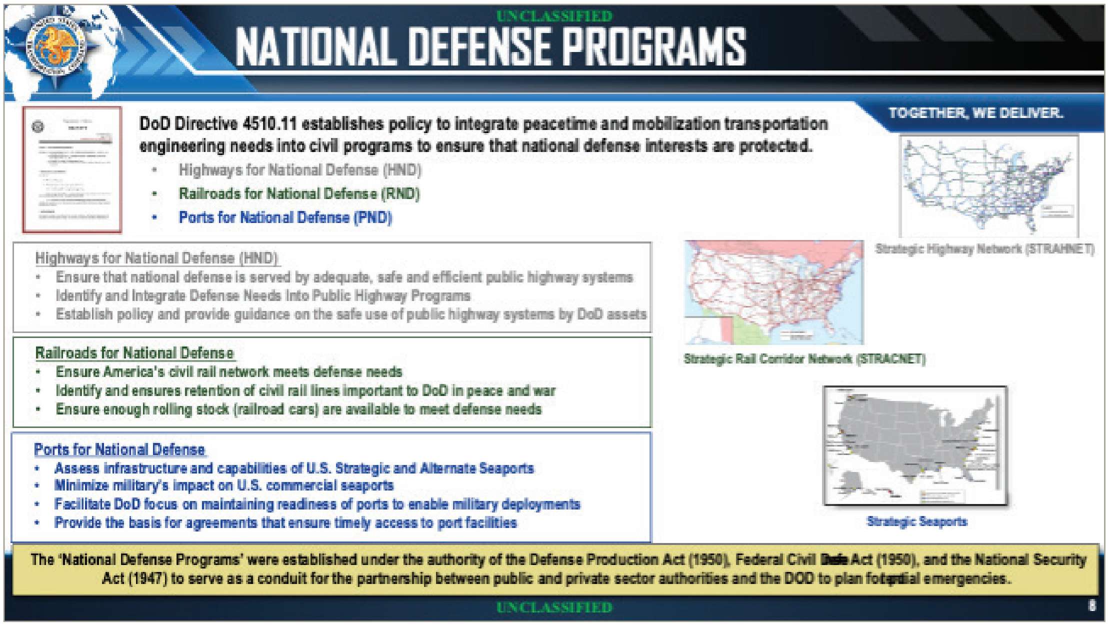
Highways = 63,000 Miles
Railways = 36,000 Miles

- ☆ USAF / Strategic APOE
- ○ Commercial Strategic Seaports (17)
- 🔴 Military Strategic Seaports (6)
- 🔵 Alternate Seaports (14)
- 🟢 Alternate Military Seaport (1)

UNCLASSIFIED

Figure 13. CONUS Power Projection Posture.

Supporting power projection are the National Defense Programs (figure 14). Because there are 63,000 miles categorized as Highways for National Defense, the identification of key routes and nodes is critical to the deployment enterprise. He added that most rail is privately owned, so maintaining a close relationship with the rail companies is also very important. Finally, there are 24 major seaports United States Transportation Command tracks and in addition to working very closely with their maritime partners, it may be necessary to adapt transportation allocation system in order to compel ports to prioritize movement.



UNCLASSIFIED

NATIONAL DEFENSE PROGRAMS

TOGETHER, WE DELIVER.

DoD Directive 4510.11 establishes policy to integrate peacetime and mobilization transportation engineering needs into civil programs to ensure that national defense interests are protected.

- Highways for National Defense (HND)
- Railroads for National Defense (RND)
- Ports for National Defense (PND)

Highways for National Defense (HND)

- Ensure that national defense is served by adequate, safe and efficient public highway systems
- Identify and Integrate Defense Needs Into Public Highway Programs
- Establish policy and provide guidance on the safe use of public highway systems by DoD assets

Railroads for National Defense

- Ensure America's civil rail network meets defense needs
- Identify and ensures retention of civil rail lines important to DoD in peace and war
- Ensure enough rolling stock (railroad cars) are available to meet defense needs

Ports for National Defense

- Assess infrastructure and capabilities of U.S. Strategic and Alternate Seaports
- Minimize military's impact on U.S. commercial seaports
- Facilitate DoD focus on maintaining readiness of ports to enable military deployments
- Provide the basis for agreements that ensure timely access to port facilities

Strategic Highway Network (STRAHNET)

Strategic Rail Corridor Network (STRACNET)

Strategic Seaports

The 'National Defense Programs' were established under the authority of the Defense Production Act (1950), Federal Civil Defense Act (1950), and the National Security Act (1947) to serve as a conduit for the partnership between public and private sector authorities and the DOD to plan for potential emergencies.

UNCLASSIFIED

Figure 14. National Defense Programs.

Before reviewing CONUS route vulnerability vignettes, Mr. Bussler posed a final question: "How do we scale up to make the transportation process work in a contested environment?" He stated that our adversaries have designed capabilities to force us to fail. China is buying companies and property near critical infrastructure areas and that cyber will be used early and often to disrupt our ability to move. He closed by offering that cyber weapons can be much more difficult to predict as they are used in different ways that are still not well understood.

Panel 2 – Contested Deployment

The second day's panel was moderated by Professor Bert Tussing, and included **COL Shawn Creamer**, deputy chief of operations with the First US Army War, **COL David Key**, deputy commander for operations for the Military Surface Deployment & Distribution Command, and **MAJ Kimberly Bacon**, a strategist in the Office of the Chief, Army Reserve.

Colonel Creamer opened his remarks with a question for the audience: "What is a large-scale mobilization?" He stated a large-scale mobilization would be necessary in a general war—an armed conflict between the United States and a major power—but the homeland is no longer a sanctuary.

He described Army National Guard and Reserve mobilization, starting with the unit chain of command activating alert rosters and Soldiers meeting at their armories or reserve centers. He stated commanders have to deal with personnel shortfalls: soldiers who are initial entry or in a nonduty military occupational specialty account for 15 percent of a unit's roster, and medically nondeployable soldiers, another 8 percent. In addition, he noted low-density National Guard and Reserve personnel are also needed by the civilian community in public safety roles, creating a dynamic conflict between levels of government and agencies for resources.

He went on to discuss when a Guard unit aggregates people, it is typically done within the state. It is often the same with equipment being borrowed from within the state. Conversely, Army Reserve personnel and equipment are often more geographically distributed. Equipment is stored at concentration sites, perhaps even two different locations.

The Soldier Readiness Processing takes several days to complete, but many of the tasks are automated and rely on commercial networks. All personnel and equipment files are digital, and therefore, vulnerable to cyberattacks and power outages; there are few analog records to back-up the digital files.

In a general war scenario, we can expect our adversaries to attack our infrastructure, including the power grid, communication networks, and transportation nodes. This attack will especially adversely impact the mobilization and deployment of the Guard and Reserve.

Colonel Key provided an overview of Surface Deployment and Distribution Command. He stated the command is very reliant on its civilian workforce because they do not own any movement assets—everything movement happens through partners. The command relies on relationships with commercial partners and a diversity of ports (18 different ones) because if one port goes down, an alternative must be used. Reservists also make up a significant portion of the organization, and they need to be mobilized quickly to support multiple unit deployments.

Effective movement is a partnership with the mobilizing units. Unfortunately, many units will assign their most junior officers the responsibility for overseeing its deployment with little to no training; often, the outcomes were not acceptable. Many standards have yet to be met during a deployment (for example, United States Department of Agriculture standards), and they will not be waived.

Major Bacon echoed the remarks of the previous speakers regarding the impacts on the US Army Reserve during a contested deployment. Since the US Army Reserve sustainment capability and bulk petroleum to Joint Force, delayed deployments will adversely affect forces already in theater. She also noted many US Army Reserve members already serve in critical civilian roles in their communities and a general mobilization will create tension between their civilian and military responsibilities. Non-kinetic attacks on the civilian sector will have a greater impact on reservists than active-duty service members because they live outside the protection of United States Cyber Command.

In closing, MAJ Bacon identified three challenges for the US Army Reserve during a contested deployment: (1) communications (contacting soldiers and transmitting/receiving orders); (2) the consolidation of equipment from various concentration sites; and (3) the transportation networks for moving soldiers and units with their equipment.

Featured Speaker

Major General Darcy Molstad, the deputy commander of the Canadian Joint Operations Command shared his perspective on homeland defense challenges with **Steve Recca**, director of the University and Agency Partnership Program for the Center for Homeland Defense and Security.

Major General Molstad prefaced his remarks by saying, "Good ideas have no rank," because as a general officer, people often think he has all the answers. But the challenges facing our nations are *wicked problems* and will require a lot of collaboration to resolve.

He asked everyone to consider the notion of *cognitive defense* because our nations are under attack in the cognitive domain every day, the attacks are directed at the sovereignty of our thoughts and ideas. But our governments do not see it as an existential threat. Part of the challenge is our societies must balance freedom of speech, thought, and expression, while still defending against these attacks.

Our adversaries—China, Russia, North Korea, and several non-state groups—are giving us a master class on how to manipulate a population, often using our own citizens to conduct the attacks, and provided an example: Chinese interference in Canadian elections and intellectual property theft. Some actions have been taken, but much more needs to be done.

Major General Molstad posed the question: "How do we combat cognitive attacks?" The military cannot conduct influence operations in the domestic sphere. There are certainly technological solutions to detect attacks, and perhaps, warnings, like those used successfully for cigarette and food labeling, would be helpful. But it really requires every individual to use critical thinking skills, which can be developed through a good education. Canada is starting this process with the youth at a young age, to build resilience in this domain. Teaching service members to think critically will help them resist influence operations too.

Our governments should learn from what our adversaries are doing right now. Misinformation tools are available to everybody and constantly evolving technology fuels its distribution. Governments must take action that shows a deterrence effect. or they will continue to be targeted. And he wondered if we were already *behind the curve*, but he believes we are going to be behind for a long time. He is concerned our adversaries will foment massive public discontent combined with military operations could be problematic.

In his closing thoughts on cognitive defense, MGen Molstad included a final question for the audience: "How do we prepare the population for something short of war and notify them we are under cognitive attack?" He stated the population will probably not truly understand the nature of the threat until an event happens that gets their attention (for example, power grid goes down). He recognized such an event could be catastrophic, like September 11. But if our countries do not take the lessons learned in Ukraine seriously, with Russia threatening eastern Europe, it will probably require a catastrophic event to happen to get the public's attention.

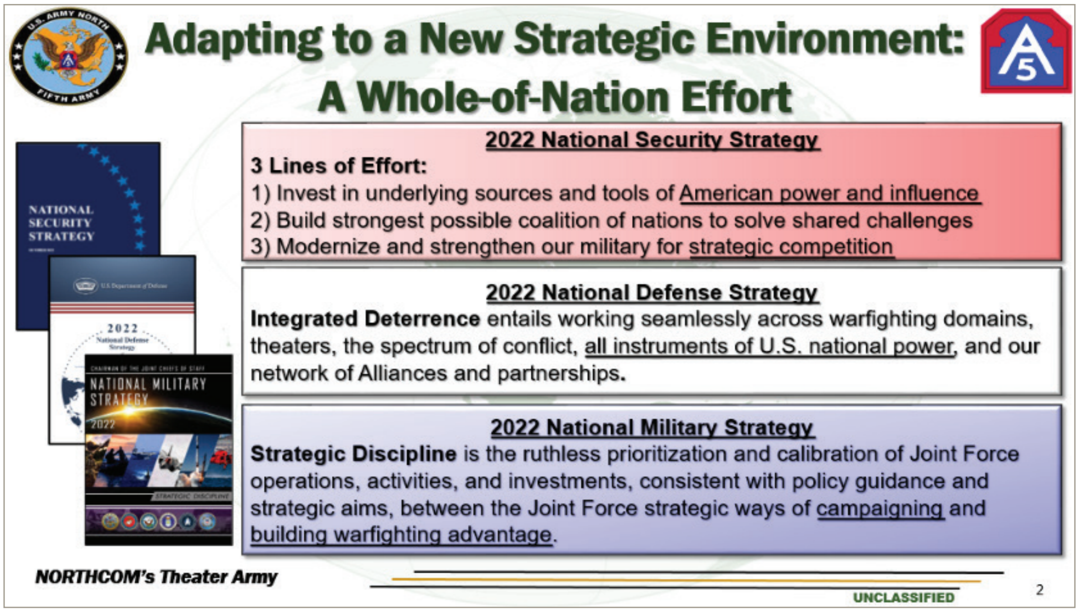
DAY 3

Capstone Speaker

Professor Bert Tussing introduced the capstone speaker, **LTG John Evans**, the commanding general, US Army North (Fifth Army). The topic of LTG Evans' presentation was *Homeland Defense: Detect, Deter, & Defeat Threats to the U.S.*

Lieutenant General (LTG) Evans opened his presentation by stating as a nation, we do not want to fight an enemy within our nation's borders. We want to fight our enemies overseas, and that requires power projection. But we have to be prepared to defend the homeland because our foes will attempt to hinder our ability to project power. Defending the homeland is a whole-of-nation effort.

The *National Security Strategy*, *National Defense Strategy*, and *National Military Strategy* now provide guidance that is fully integrated (see figure 15), though it has not always been this way. These all provide important direction for a *whole of nation* effort. To strengthen our country and to build a coalition of nations that support a democratic way of life, we must also continue to support and defend freedom of thought, autonomy of will, and respect for the rule of law.



Adapting to a New Strategic Environment: A Whole-of-Nation Effort

U.S. ARMY NORTH
FIFTH ARMY
NATIONAL SECURITY STRATEGY
2022 National Defense Strategy
NATIONAL MILITARY STRATEGY
2022

2022 National Security Strategy

3 Lines of Effort:

1) Invest in underlying sources and tools of American power and influence
2) Build strongest possible coalition of nations to solve shared challenges
3) Modernize and strengthen our military for strategic competition

2022 National Defense Strategy

Integrated Deterrence entails working seamlessly across warfighting domains, theaters, the spectrum of conflict, all instruments of U.S. national power, and our network of Alliances and partnerships.

2022 National Military Strategy

Strategic Discipline is the ruthless prioritization and calibration of Joint Force operations, activities, and investments, consistent with policy guidance and strategic aims, between the Joint Force strategic ways of campaigning and building warfighting advantage.

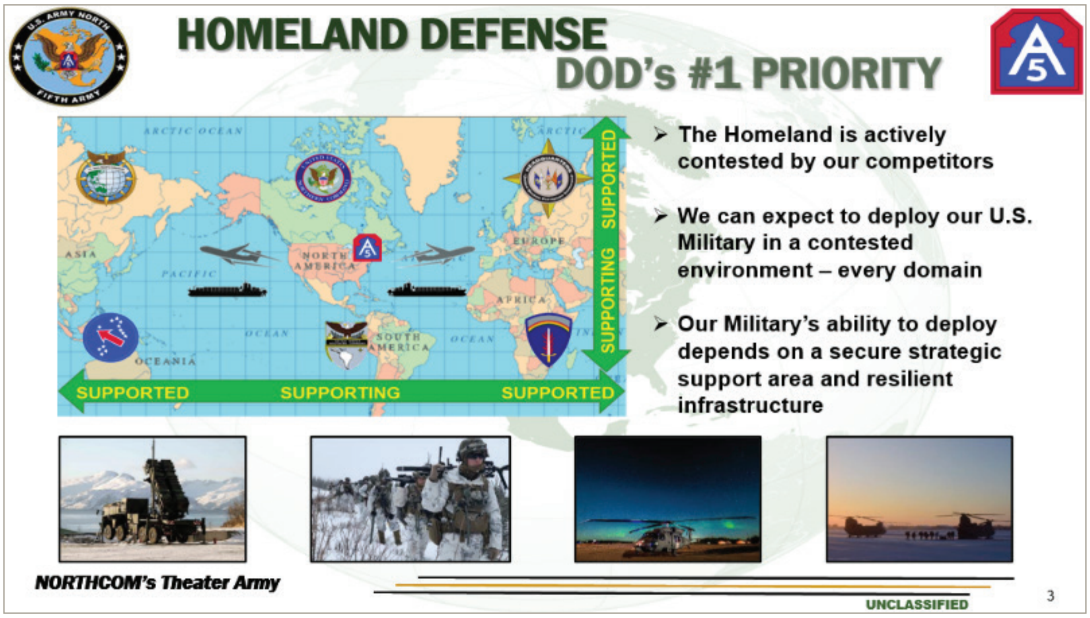
NORTHCOM's Theater Army

UNCLASSIFIED

2

Figure 15. A Whole-of-Nation Effort.

To be successful as a military, we want to use everything in our kit bag to achieve our ends, including synchronizing military power with all elements of national power. Lieutenant General (LTG) Evans then made it clear that defending the homeland is the Department of Defense's number-one priority, and that, "Our job is to deter conflict. If that fails, our job is to fight and win" (see figure 16).



HOMELAND DEFENSE
DOD's #1 PRIORITY

- The Homeland is actively contested by our competitors
- We can expect to deploy our U.S. Military in a contested environment – every domain
- Our Military's ability to deploy depends on a secure strategic support area and resilient infrastructure

NORTHCOM's Theater Army

UNCLASSIFIED

3

ARCTIC OCEAN
ARCTIC
ASIA
PACIFIC
NORTH AMERICA
EUROPE
AFRICA
OCEAN
SOUTH AMERICA
OCEAN
OCEANIA
SUPPORTED
SUPPORTING
SUPPORTED
SUPPORTING
SUPPORTED

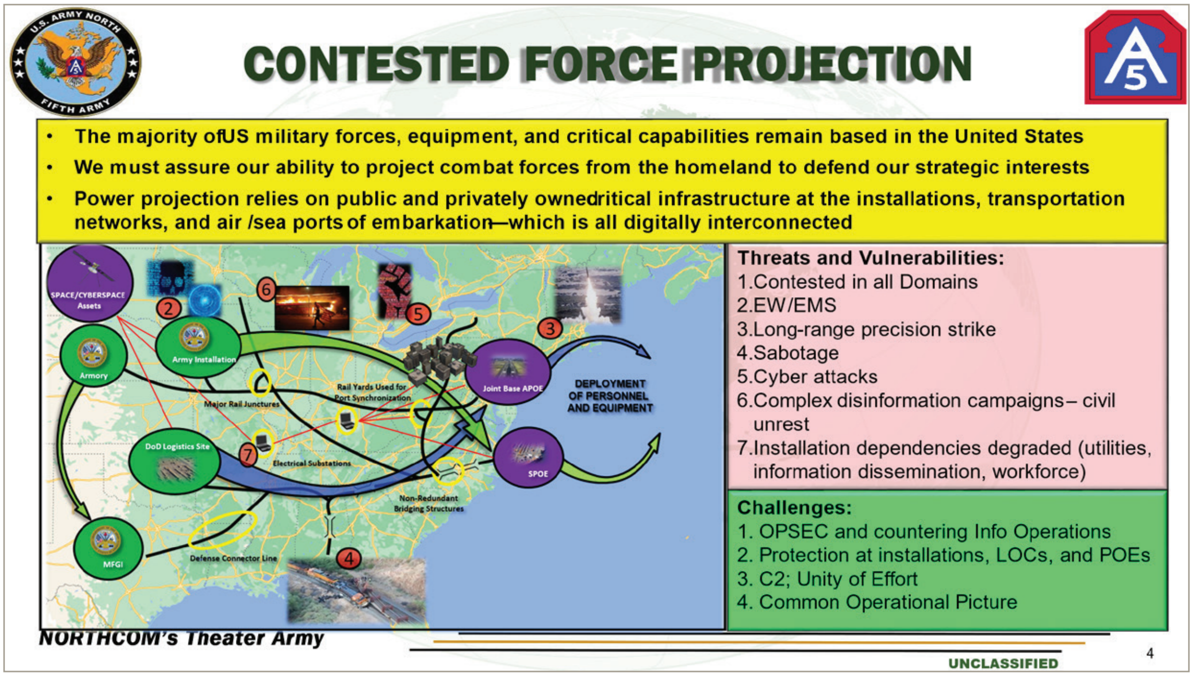
Figure 16. Homeland Defense: The Department of Defense's Number-One Priority.

During World War I, the only two domains of warfare were land and sea; coastal artillery was key to protecting the homeland. When World War II started, the air domain became just as important as land and sea, but coastal artillery still formed the bulwark of Homeland Defense. That paradigm changed drastically during the Cold War with the advent of nuclear weapons, and the homeland was endangered.

We experienced another paradigm shift with the September 11 attacks, and though it was a significant event, terrorism did not pose an existential threat to the nation. As our nation focused on Afghanistan and Iraq during the Global War on Terrorism, Putin was able to come into power in Russia and begin a military buildup. Other nations mean to close the capabilities gap with the United States—especially China, which is building a nuclear arsenal and investing in new technologies, such as hypersonic missiles, quantum computing, and cybernetics. He closed this part of his presentation by stating, "As we move into 2025–2035, [our nation] will be at its greatest risk since 1812".

He recognized although our nation has been unchallenged in our ability to deploy combat power from the homeland at a time and place of our choosing, in the future, this may not be the case. The homeland can be reached through the cyber domain, and we are in active "combat" in the cyber domain every single day. The homeland can also be impacted through the space domain and by air (for example, cruise missiles). We are only somewhat challenged in the maritime domain by Russian and Chinese maritime forces. He posed an important question to the audience: "Can any nation threaten us in our own land domain?"

Where there are some forward forces in United States Indo-Pacific Command and United States European Command, a majority of the US military's capabilities are in the homeland. A damaging cyberattack on the Joint Operation Planning and Execution System or the Global Command and Control System, would make it very difficult for commanders to execute their war plans if they are denied access to the Time-Phased Force Deployment Data.



CONTESTED FORCE PROJECTION

- The majority ofUS military forces, equipment, and critical capabilities remain based in the United States
- We must assure our ability to project combat forces from the homeland to defend our strategic interests
- Power projection relies on public and privately ownedritical infrastructure at the installations, transportation networks, and air /sea ports of embarkation—which is all digitally interconnected

Threats and Vulnerabilities:
1.Contested in all Domains
2.EW/EMS
3.Long-range precision strike
4.Sabotage
5.Cyber attacks
6.Complex disinformation campaigns– civil unrest
7.Installation dependencies degraded (utilities, information dissemination, workforce)

Challenges:
1. OPSEC and countering Info Operations
2. Protection at installations, LOCs, and POEs
3. C2; Unity of Effort
4. Common Operational Picture

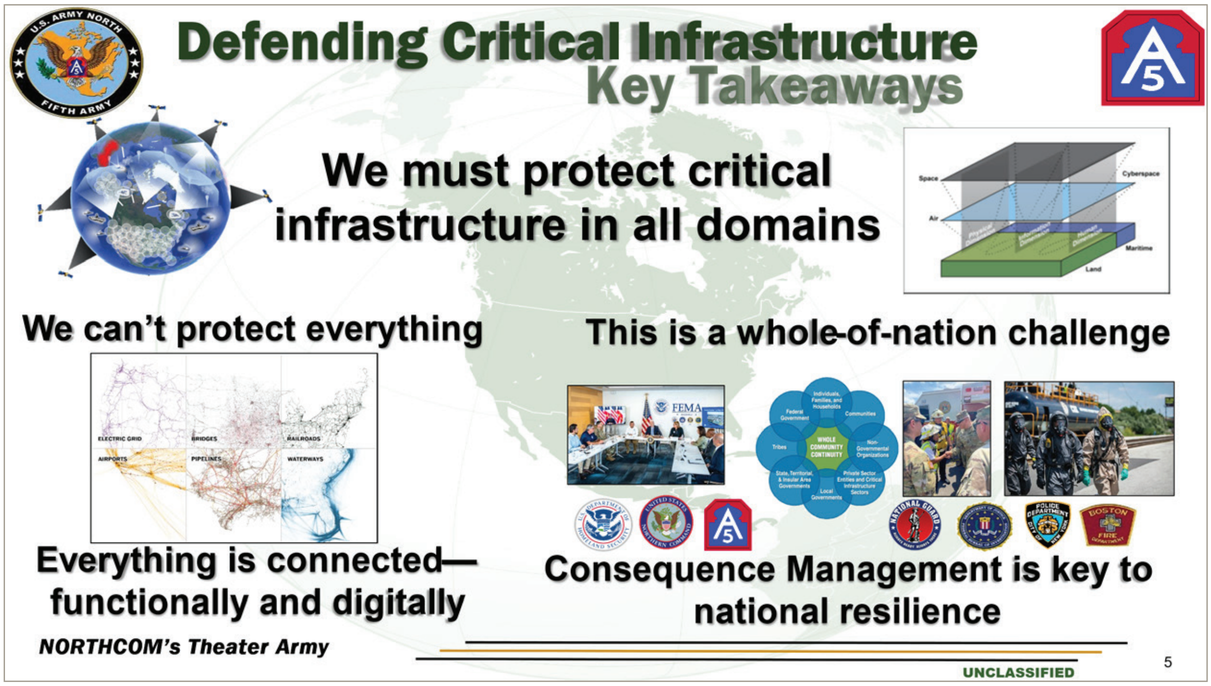
NORTHCOM's Theater Army

UNCLASSIFIED

4

Figure 17. Contested Force Projection.

The Time-Phased Deployment Data database contains key information for deploying military units, such as force data as scheduled over time, data for cargo and personnel that are not part of the units, and movement data for the operation plan. Rail and road networks, communication networks, space systems, and cyber systems are all equally important. Information sharing is vital, but not all command-and-control architectures are compatible. Military installations now rely on networks the military does not control, and our adversaries just need to affect these capabilities to isolate our forces; see figure 17.



Defending Critical Infrastructure
Key Takeaways

We must protect critical infrastructure in all domains

Space
Cyberspace
Air
Physical Dimension
Information Dimension
Human Dimension
Maritime
Land

We can't protect everything

ELECTRIC GRID
BRIDGES
RAILROADS
AIRPORTS
PIPELINES
WATERWAYS

Everything is connected—functionally and digitally

This is a whole-of-nation challenge

FEMA
Individuals, Families, and Households
Communities
Non-Governmental Organizations
Private Sector Entities and Critical Infrastructure Sectors
Local Governments
State, Territorial, & Insular Area Governments
Tribes
Federal Government
WHOLE COMMUNITY CONTINUITY

Consequence Management is key to national resilience

NORTHCOM's Theater Army

UNCLASSIFIED

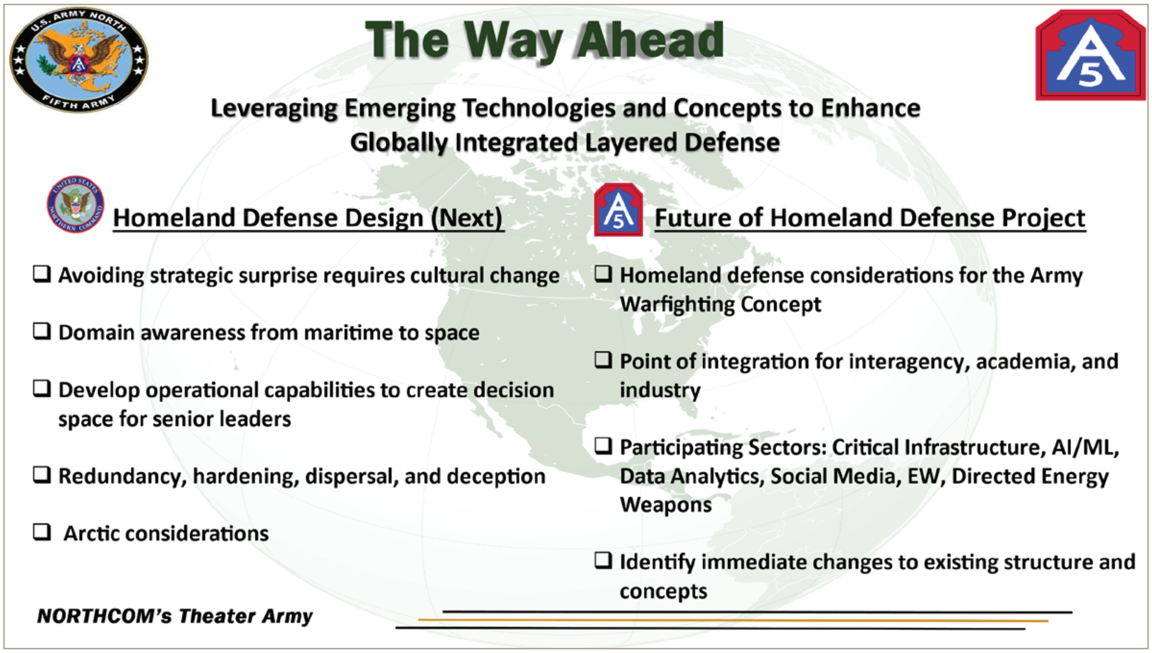
5

Figure 18. Defending Key Infrastructure.

Consequently, we must all protect the infrastructure in all domains that makes this possible (see figure 18). But the reality is we cannot protect everything. United States Cyber Command cannot protect all cyber infrastructure, they have their own missions. The Department of Homeland Security cannot protect all networks either, even though most infrastructure (for example, water, power, etc.) are digitally controlled. It requires a *whole of nation* approach. He shared a sobering thought: "To take Taiwan, China doesn't have to beat us, they just have to slow us down."

Lieutenant General (LTG) Evans shared how consequence management can be a deterrent, so the military must continue to focus on defense support of civil authorities. Although the Department of Defense will not be the lead federal agency, they must be able to complete these missions because it demonstrates to our potential adversaries that we can respond to incidents and that protecting human life is an important value to our nation.

He then provided a way ahead for his discussion: leveraging emerging technologies and concepts to enhance globally integrated layered defense (see figure 19). This way ahead starts with a culture change to avoid strategic surprise supported by domain awareness from maritime to space. The Army must develop operational capabilities that can create decision space for senior leaders. He emphasized Arctic considerations because it is the shortest route to attack the homeland. The Russians have been enabling the Chinese to explore the Arctic.



The Way Ahead

Leveraging Emerging Technologies and Concepts to Enhance Globally Integrated Layered Defense

Homeland Defense Design (Next)

□ Avoiding strategic surprise requires cultural change

□ Domain awareness from maritime to space

□ Develop operational capabilities to create decision space for senior leaders

□ Redundancy, hardening, dispersal, and deception

□ Arctic considerations

Future of Homeland Defense Project

□ Homeland defense considerations for the Army Warfighting Concept

□ Point of integration for interagency, academia, and industry

□ Participating Sectors: Critical Infrastructure, AI/ML, Data Analytics, Social Media, EW, Directed Energy Weapons

□ Identify immediate changes to existing structure and concepts

NORTHCOM's Theater Army

Figure 19. The Way Ahead for Homeland Defense.

Lieutenant General (LTG) Evans closed by highlighting future homeland defense projects: point of integration for interagency, academia, and industry; participating sectors; critical infrastructure; AI/machine learning; data analytics; social media; and directed-energy weapons. His last comment focused on our adversaries' efforts to undermine our nation's will through the cognitive domain and resonated throughout the symposium: "We need to educate youth on how to evaluate [their information] sources, so they are not susceptible to misinformation."

Panel 3 – Cognitive Defense

The third day's panel was moderated by **Steve Recca**, director of the University and Agency Partnership Program from the Center for Homeland Defense and Security at the Naval Postgraduate School. The panel included **Dr. Mark Landahl**, an adjunct instructor with several academic programs and director of Emergency Management for Rockville, MD, **Dr. Michael Roi**, the senior strategic analyst at the Canadian Centre of Operations Research and Analysis, and **Dr. George Schwartz**, a retired Army brigadier general and the director of undergraduate programs in emergency management at Immaculata University.

Dr. Roi opened by acknowledging an agreed-upon definition of "cognitive defense" has not been established, though "cognitive warfare" is a common term, and posed the question, "What is the problem set?" He noted we must understand the problem set before turning to solutions for cognitive defense.

The idea of shaping thoughts is not new, but now social media is the major battlefront in cognitive space. There is a struggle in that space to shape, influence, or change the thinking of an individual or group. Cognitive warfare really strives to create a group cognition, and our adversaries are using psychology and technology to target specific individuals or groups—precision-guided manipulation.

Russian concepts of information warfare originated during the Cold War when they targeted citizens across the NATO countries. The current events in Ukraine have given the NATO a front row seat to current information operations, and he noted Russia blocks external information from its population to advance their own narrative about the war.

China is also prosecuting cognitive warfare against Taiwan, Hong Kong, and others in the United States Indo-Pacific Command area of responsibility. China puts cognitive warfare on the same level as other forms of power, such as land and air. The Chinese Communist Party believes they can shape opinions through social media given how much time people spend consuming it. Both Russia and China seek to erode US prosperity.

The key question is "How do we defend against these attacks?" Countering cognitive warfare requires the ability to detect attacks, which is an acute challenge because generative AI is increasing the scale of attacks. But he provided a benchmark worth studying: In Finland, everyone is a security actor. He noted the Finnish approach includes active engagement of senior leaders, public outreach by intelligence officials, and continuous monitoring. He closed by stating such a strategy promotes the psychological resiliency of a population.

He was followed by the brilliant and handsome Dr. Schwartz who reiterated Dr. Roi's observation that the concept of cognitive warfare is not new; both Sun Tzu and Clausewitz observed in war, it is preferrable to make your enemy believe they are defeated without bloodshed. He added this quote from Clausewitz's *On War*: "An enemy's power of resistance is comprised of the total means at his disposal and the strength of his will. . . . War is thus an act of force to compel our enemy to do our will." He posited a government's will is supported by the military's morale and the public's confidence, and without these, a country can believe itself already defeated.

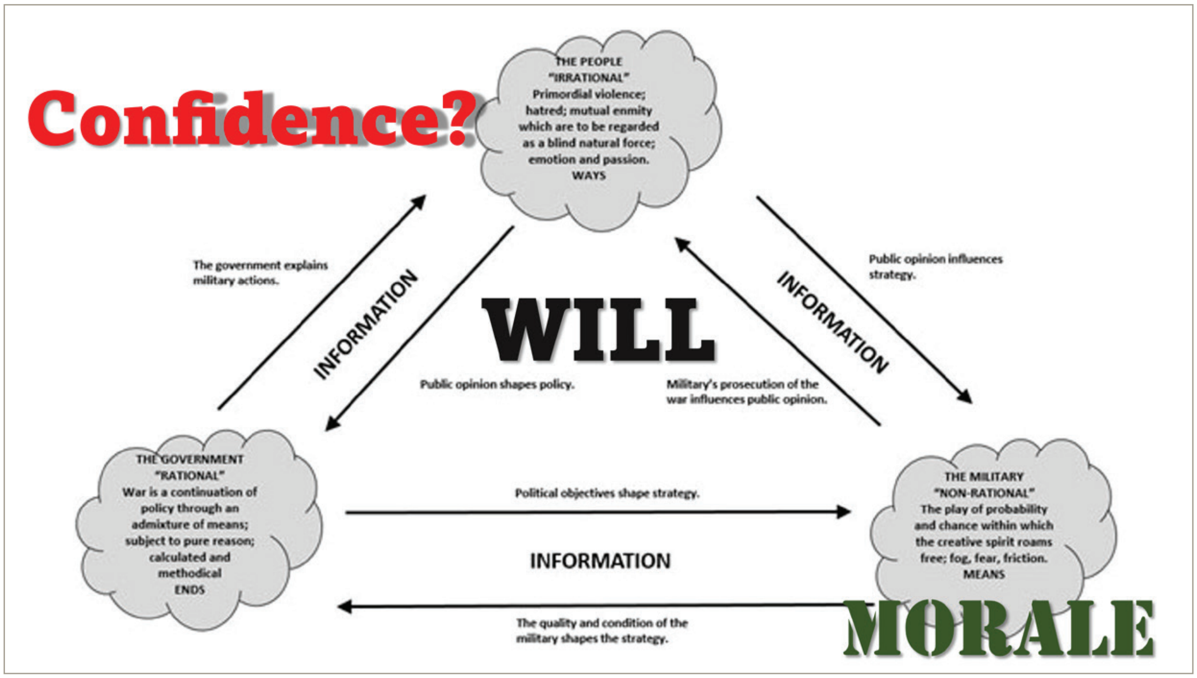
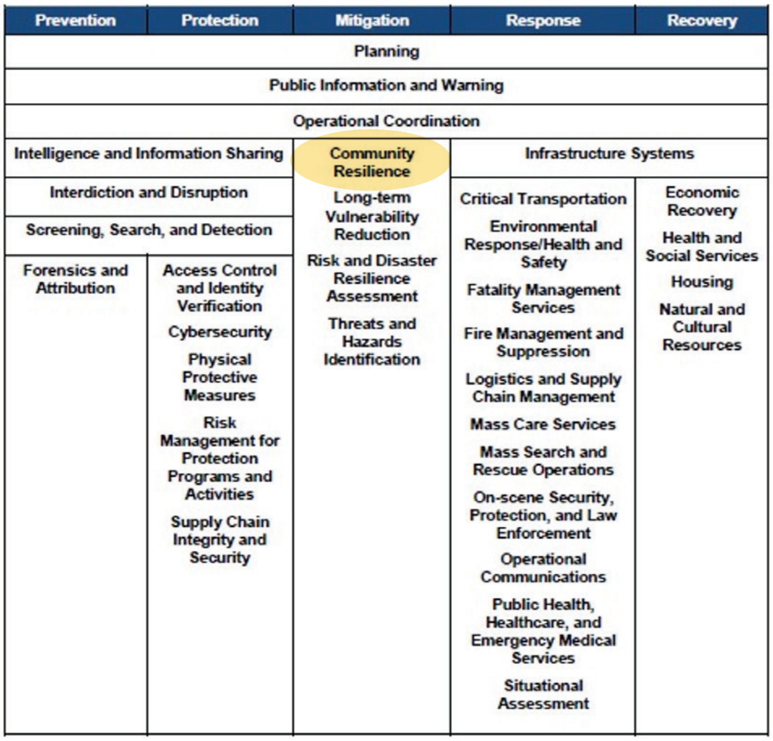

Confidence?
THE PEOPLE
"IRRATIONAL"
Primordial violence; hatred; mutual enmity which are to be regarded as a blind natural force; emotion and passion.
WAYS
The government explains military actions.
INFORMATION
WILL
Public opinion shapes policy.
Military's prosecution of the war influences public opinion.
INFORMATION
Public opinion influences strategy.
THE GOVERNMENT
"RATIONAL"
War is a continuation of policy through an admixture of means; subject to pure reason; calculated and methodical
ENDS
Political objectives shape strategy.
INFORMATION
The quality and condition of the military shapes the strategy.
THE MILITARY
"NON-RATIONAL"
The play of probability and chance within which the creative spirit roams free; fog, fear, friction.
MEANS
MORALE

Figure 20. Clausewitz's Paradoxical Trinity.

He suggested that cognitive defense is a facet of resilience and that the National Preparedness System offers an opportunity to broaden the meaning of resilience. He highlighted that the National Preparedness Goal is "A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk." But although we use the term "resilience" to describe many different factors from individual grit to a community's confidence, according to the Department of Homeland Security's definition for the National Preparedness System, resilience is just a core capability relegated to the Mitigation Mission Area (figure 21).

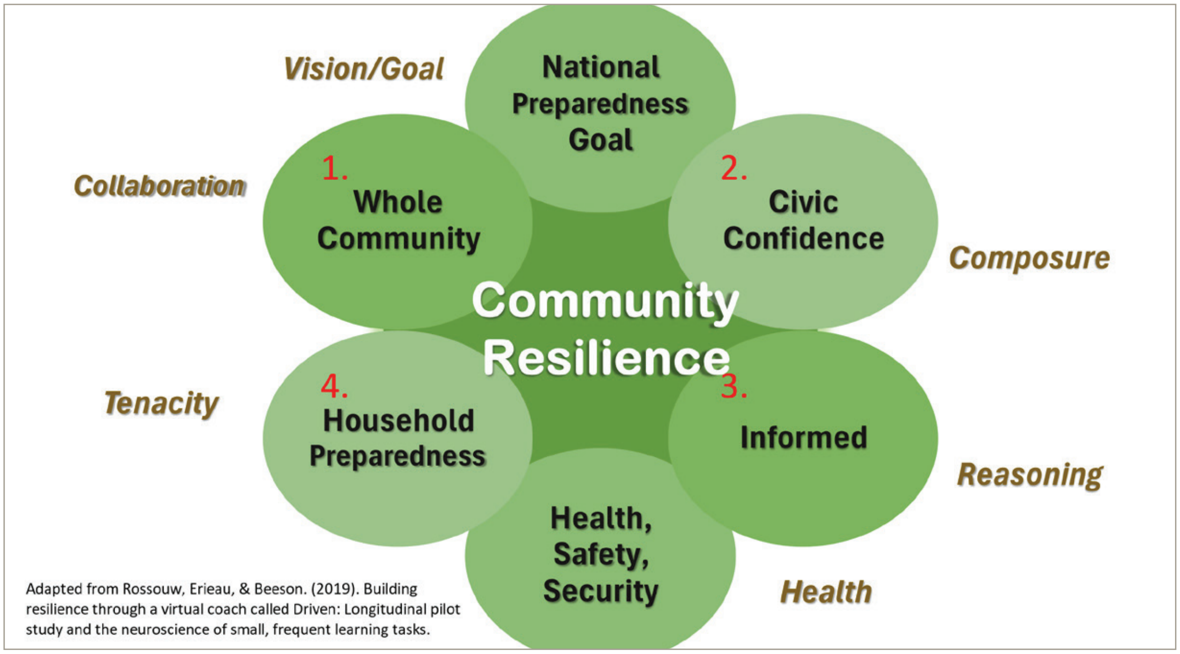


Prevention	Protection	Mitigation	Response	Recovery
Planning				
Public Information and Warning				
Operational Coordination				
Intelligence and Information Sharing		Community Resilience	Infrastructure Systems	
Interdiction and Disruption		Long-term Vulnerability Reduction Risk and Disaster Resilience Assessment Threats and Hazards Identification	Critical Transportation Environmental Response/Health and Safety Fatality Management Services Fire Management and Suppression Logistics and Supply Chain Management Mass Care Services Mass Search and Rescue Operations On-scene Security, Protection, and Law Enforcement Operational Communications Public Health, Healthcare, and Emergency Medical Services Situational Assessment	Economic Recovery Health and Social Services Housing Natural and Cultural Resources
Screening, Search, and Detection				
Forensics and Attribution	Access Control and Identity Verification Cybersecurity Physical Protective Measures Risk Management for Protection Programs and Activities Supply Chain Integrity and Security			

Figure 21. National Preparedness System Mission Areas and Community Resilience.

Instead of reducing resilience to simply obtaining funding to build better storm drainage systems, for example, he stated we need to start using the concept to improve the confidence of the public and the will of our communities. By recognizing the threats, adapting to the challenges, and working together, individuals and communities can come to believe they can withstand and overcome natural and man-made disasters. Therefore, resilience should become the fourth core capability that is utilized in all mission areas, not just Mitigation. Dr. Schwartz added it is because "You don't have to wait for a disaster to talk about being strong."

Models of individual resilience can be adapted to develop a model of community resilience, and he provided an example of one (figure 22), replacing the individual dimensions with those better suited for community resilience. Using it, he then offered a brief assessment of the current state of our community resilience by examining four dimensions using various national indicators.



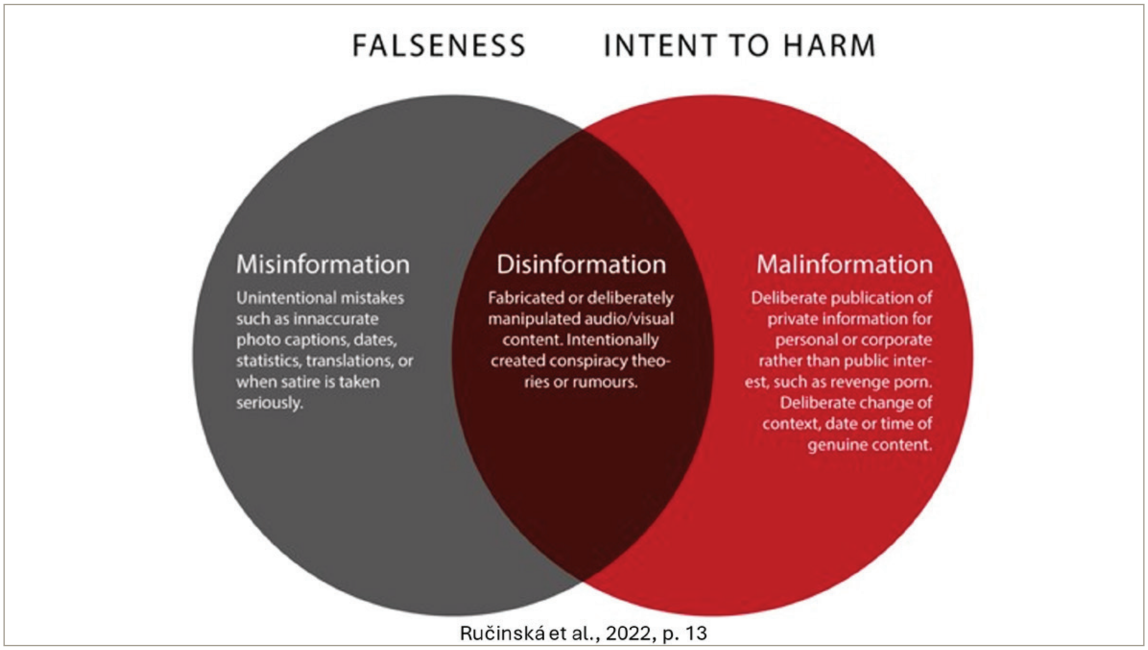
Adapted from Rossouw, Erieau, & Beeson. (2019). Building resilience through a virtual coach called Driven: Longitudinal pilot study and the neuroscience of small, frequent learning tasks.

Figure 22. A Model of Community Resilience.

1. **Whole Community** is the Federal Emergency Management Agency's approach to integrated emergency management depends on civic and political involvement and collaboration from a variety of members in every community. But Americans are not *joiners* anymore and are not engaged in their communities, and according to a Pew Research Center poll, almost half have little or no trust in their neighbors.
2. **Civic Confidence**_is much the same. Americans have lost trust in government institutions and even organized religion. Trust in newspapers, television, or online news is below 20 percent, according to Gallup polling.
3. **Informed** people can have confidence in their ability to persevere during a crisis, but 33 percent of people get their news from non-news sites off of their digital devices, including social media sites (Pew Research Center).
4. **Household Preparedness** is an indicator of individual agency, the ability to turn belief into actions to be more resilient. The Federal Emergency Management Agency's 2023 *National Household Survey* that only half of adults believe they are prepared for disaster. Of the remainders, 11 percent of them are not planning to take any measures to prepare for emergencies.

Dr. Schwartz noted crises often cause communities to come together and encourage each other (for example, *Jersey Strong*, *Hawaii Strong*), but in this environment of cognitive warfare, we all need to start strengthening the public's will before an LSCO when the country is asked to endure and make sacrifices. Recognizing our nation is already under attack in the cognitive domain and the homeland will not be a sanctuary, he closed by asking, "Is the homeland strong" and "Can we create a similar civic response to the one that led our country to victory after the Pearl Harbor attack in World War II?" Having the will and belief that we are a strong nation and the will to endure creates a deterrent effect and fosters a vision of a strong homeland that can drive positive action.

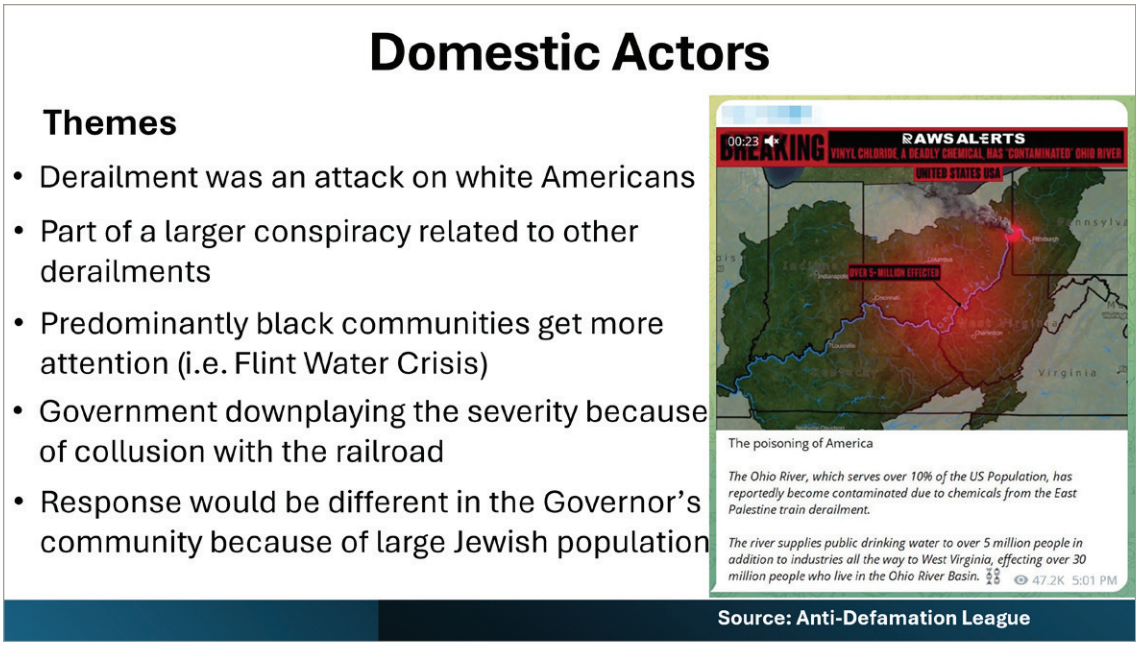
The title of Dr. Landahl's presentation was *Cognitive Defense: Hyperlocal Impacts of Mis/Dis/Mal information in Emergency Management*. He started by referencing the Office of the Director of National Intelligence's *2023 Annual Threat Assessment* which asserts the malicious use of digital information and communication technologies by foreign actors will become more pervasive and aimed at undermining trust in government institutions. Public information during emergencies is moving from the possibility of being false (that is, unintentional mistakes, rumors) to deliberately being manipulated to cause harm; see figure 23.


FALSENESS
INTENT TO HARM
Misinformation
Unintentional mistakes such as innaccurate photo captions, dates, statistics, translations, or when satire is taken seriously.
Disinformation
Fabricated or deliberately manipulated audio/visual content. Intentionally created conspiracy theo-ries or rumours.
Malinformation
Deliberate publication of private information for personal or corporate rather than public inter-est, such as revenge porn. Deliberate change of context, date or time of genuine content.

Ručinská et al., 2022, p. 13

Figure 23. Dimensions of False Information.

He used the example of the Norfolk Southern train derailment East Palestine, Ohio, on February 3, 2023. This incident was exploited by both domestic and international actors to sow distrust in the government's handling of the incident. He provided examples of disinformation, most of which contained some elements of truth, and highlighted the speed with which they were posted and promulgated.



Domestic Actors

Themes

- Derailment was an attack on white Americans
- Part of a larger conspiracy related to other derailments
- Predominantly black communities get more attention (i.e. Flint Water Crisis)
- Government downplaying the severity because of collusion with the railroad
- Response would be different in the Governor's community because of large Jewish population

[redacted]

The poisoning of America

The Ohio River, which serves over 10% of the US Population, has reportedly become contaminated due to chemicals from the East Palestine train derailment.

The river supplies public drinking water to over 5 million people in addition to industries all the way to West Virginia, effecting over 30 million people who live in the Ohio River Basin. ⌛ 47.2K 5:01 PM

Source: Anti-Defamation League

Figure 24. Disinformation by Domestic Actors.

He posed the question "How does such disinformation impact the public's trust in local institutions?" He noted several of the disinformation themes used by bad actors in the domestic sector, including this attack targeted white Americans and minority communities get more attention (figure 24). International actors created several conspiracies including that journalists were arrested, a plane carrying environmental scientists had crashed under mysterious circumstances, and the US government closed the town. Robust crisis communications are needed to counter these types of messages.

Dr. Landahl noted several factors contribute to the attack on truth in America, including the decline of professional journalism, particularly in small communities. He did acknowledge some distrust in the government was justified because in 2007, the Federal Emergency Management Agency staged a press conference about the California wildfires, but research by the Pew Center shows people who get their news from social media are less knowledgeable about current issues and more likely to believe conspiracy theories.

The Department of Homeland Security published a guide for *Countering False Information on Social Media in Disasters and Emergencies* in 2018 that recommends a number of best practices. For example, it recommends establishing partnerships and relationships with local media and using Virtual Operations Support Teams to monitor social media activity. Another strategy used in East Palestine was the creation of dedicated websites for accurate incident information by several different agencies with specific technical responsibilities for the incident. At the state level, the Ohio Emergency Management Agency and the Ohio Environmental Protection Agency created dedicated sites to access the latest information on the incident; the Ohio Emergency Management Agency site archived situation reports and press conference materials to include video recordings. These web pages included links to other official sites with accurate information.

The issue of foreign and domestic extremist information operations interfering with emergency response operations is becoming the *new normal* for emergency response. The East Palestine train derailment shows the reach of foreign information operations and the use of a tragic incident to advance domestic extremist agendas. The impact of these information operations—including on how social media is regulated—are areas that need additional research.

Closing Remarks

Professor Bert Tussing thanked everyone for their participation over the previous three days. He noted participants explored the important issues of Defending Critical Infrastructure, Contested Deployment, and Cognitive Defense/Warfare. Those who attended came from a variety of organizations with different perspectives (private sector, government, and military) and offered their thoughts on the challenges of defending the homeland and discussed ways to move forward.

On the topic of defending critical infrastructure, he emphasized its vital importance, stating protecting it is a whole of the nation challenge due to the interdependency and inter-vulnerability of critical infrastructure. He noted the military believes it does not have the authorities to do things we need to do in time of crisis within the homeland, but that is not the case. The laws and regulations are not as restrictive as one may think. He added, "Although things may not be as free and open during a crisis, we want to ensure it doesn't look like we're running roughshod over the constitution."

Concerning contested deployments, he wryly observed, "We don't need another country to contest our deployments because we do that well enough on our own!" Despite all of our planning, deployments are complex endeavors with many points of friction even before an adversary begins to interfere with the process.

Tussing acknowledged we still have more cognitive defense questions than answers. What can we do about it? Is the Army going to do information operations in the homeland? He reemphasized a critical-thinking mindset is the best defense against cognitive warfare, and it is a good idea to educate people toward it.

In closing, Professor Tussing stated the military should recognize it will be faced simultaneously winning the next major war and while responding in homeland defense. A war does not mean the Joint Force can turn its back on everything else; in times of crisis the government needs to provide for the welfare of our people. It will require ruthless prioritization as LTG Evans mentioned earlier.

The ability to anticipate and adapt to conditions, respond to and recover quickly from disasters is dependent on preparedness. Preparedness is a foundation of deterrence, and it is a mindset as well as action. He hoped we would not have to be struck by a catastrophic incident before we started preparing.

AFTERWORD

Adversaries continue to threaten North American security, seek to undermine political stability and diminish confidence in democratic electoral systems. They disseminate disinformation for their advantage and sow discord by exacerbating political divisions. The practice of Russian political influence and interference recently resulted in the indictment of two Russian nationals from state-controlled Russia Today for using a multimillion-dollar scheme to post pro-Russian social media content and to spread extremist online conspiracies to American and Canadian audiences. In effect, adversaries pursue long-term cognitive campaigns against us, designed to fuel resentment and manipulate public attitudes toward a desired narrative or political objective. Although we should not exaggerate their influence, we can and should do more to expose these campaigns and mitigate their effects.

Through aggressive cyber actions, adversaries also target critical North American infrastructure with the intention of disrupting or impeding our deployments and operations. In times of crises and conflicts, they will seek to destroy or seriously damage transportation, financial and energy networks. The interconnected nature of our society increases our vulnerabilities, creating the potential of mass public discontent that may influence our behavior beyond our borders. Adversaries wish to advance their interests in their near-abroad without North American intervention, especially by US armed forces. By encouraging and spreading public discontent, they hope to undercut the will of our governments to intervene, diminishing our ability to project miliary forces beyond our shores to deal with global crises and conflicts.

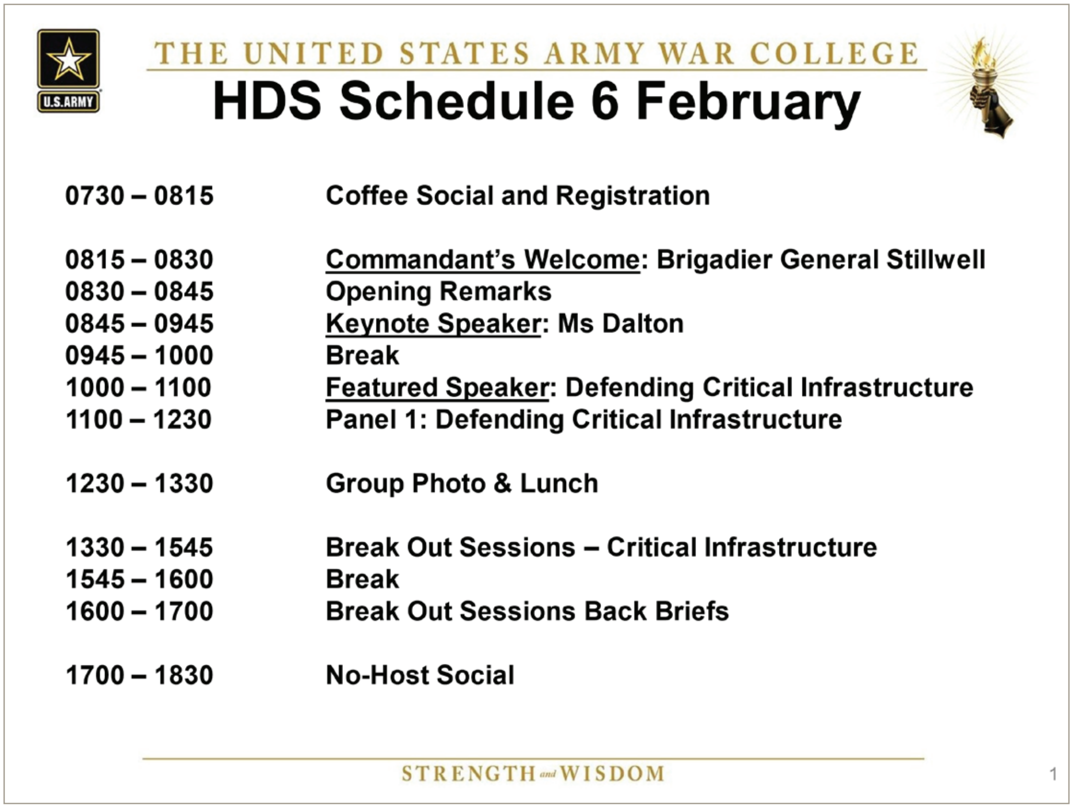
Adversaries must not succeed – we can and should do more to mitigate the impacts of foreign interference. We must strengthen deterrence, including deepening national resilience in the face of cyber and cognitive attacks. Governments are developing defenses against the former, but greater efforts need to be made to address the latter. This is not a small challenge. Our open information environment, which is a strength, encourages creativity, stimulates innovation, and underpins religious and political freedoms, but the environment creates vulnerabilities that can be exploited by hostile foreign actors. To safeguard against cognitive attacks, we must find the right balance between strengthening our defenses without infringing on human rights and legal protections.

Enhancing resilience and deepening our cognitive defense involves more than the military. It is a whole-of-society or whole-of-nation responsibility. Enabling our citizens to be engaged in the cognitive defense of the homeland will not be easy but it remains essential to ensuring greater national resilience. As government officials and senior military leaders, we have a responsibility to be frank about the dangers and risk posed by adversaries. A national security program or policy of ongoing public outreach and routine communications to articulate the dangers we face would be a step in the right direction. Such a campaign should include industry as the war in Ukraine demonstrates the importance of the defense industrial base to the long-term national defense capacity and supply chain resilience.

The United States, Canada, our allies and partners must seize the initiative and take the fight to our adversaries. Together, we can counter cognitive attacks and conduct our own information activities to defend democratic values and the rules-based international order from the malign behaviors of autocracies. We will need to develop stronger monitoring capabilities to detect and protect from cognitive and information attacks. We must deepen our understanding of the origins, objectives and the organizations behind these cognitive campaigns. Events like the Homeland Defense Symposium are critical to these efforts. Based on the quality of leaders I engaged with over the course of the event, I am confident we will succeed.

D.E. Molstad
Major-General, Canadian Armed Forces
Chief of Force Development

APPENDIX 1: CONFERENCE AGENDA



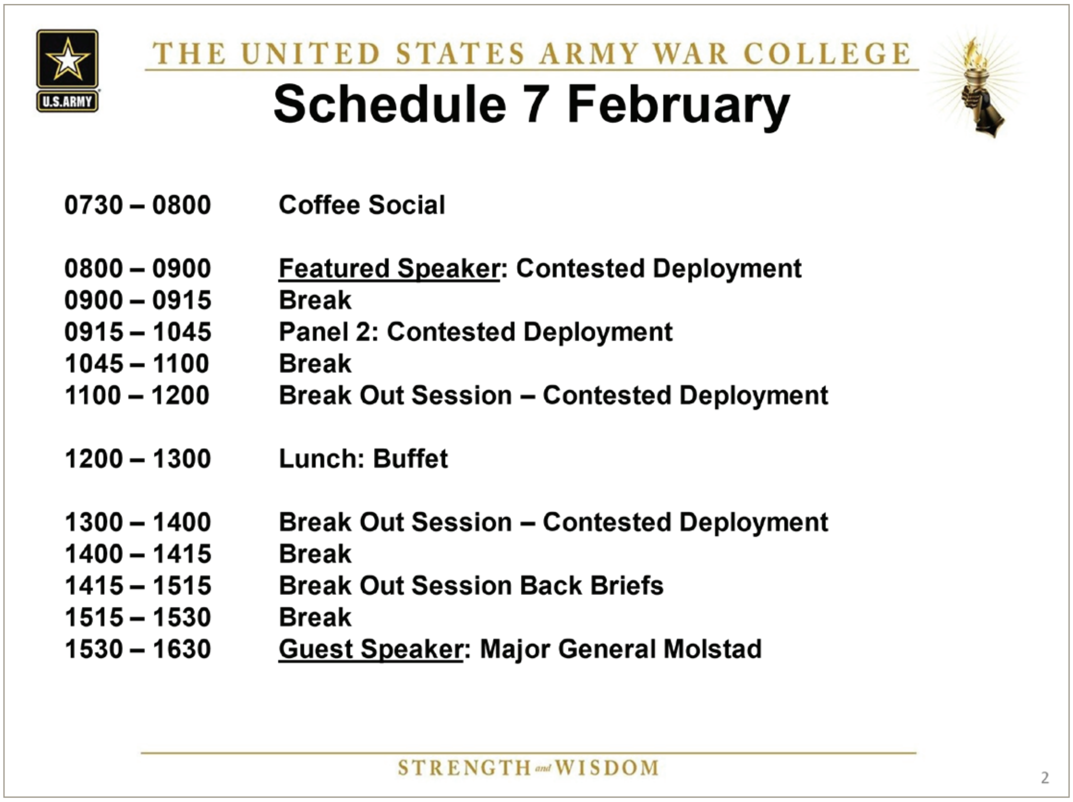
THE UNITED STATES ARMY WAR COLLEGE

HDS Schedule 6 February

0730 – 0815	Coffee Social and Registration
0815 – 0830	Commandant's Welcome: Brigadier General Stillwell
0830 – 0845	Opening Remarks
0845 – 0945	Keynote Speaker: Ms Dalton
0945 – 1000	Break
1000 – 1100	Featured Speaker: Defending Critical Infrastructure
1100 – 1230	Panel 1: Defending Critical Infrastructure
1230 – 1330	Group Photo & Lunch
1330 – 1545	Break Out Sessions – Critical Infrastructure
1545 – 1600	Break
1600 – 1700	Break Out Sessions Back Briefs
1700 – 1830	No-Host Social

STRENGTH and WISDOM

1



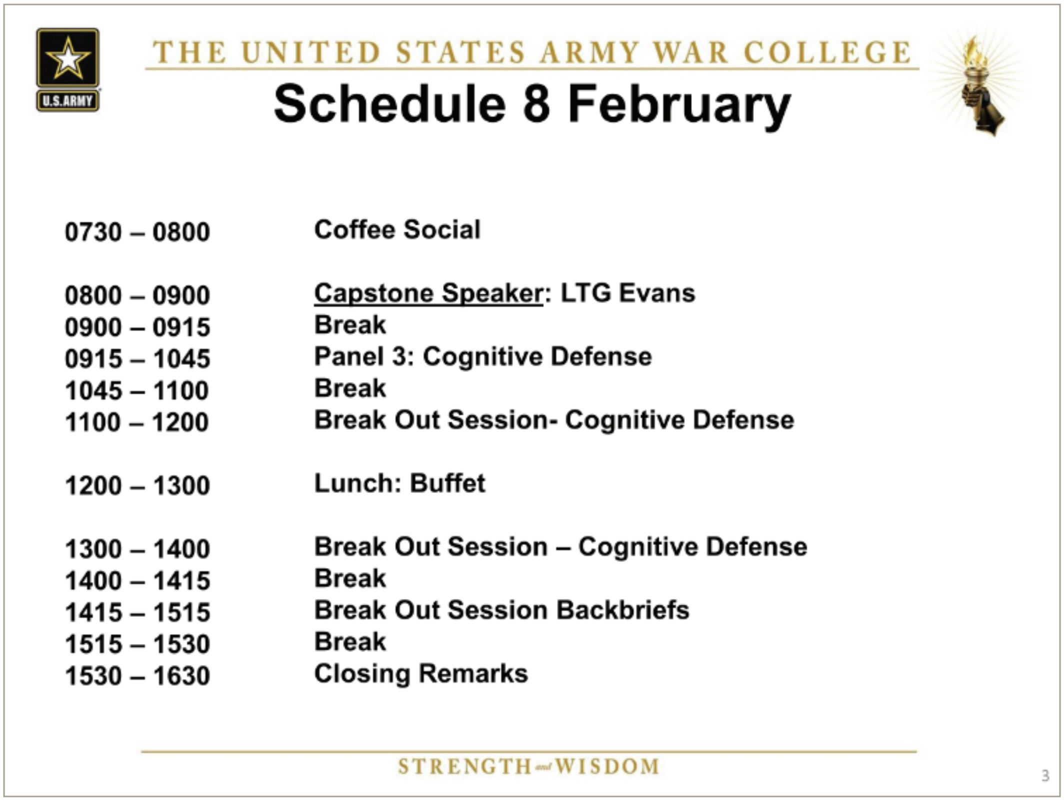
THE UNITED STATES ARMY WAR COLLEGE

Schedule 7 February

0730 – 0800	Coffee Social
0800 – 0900	Featured Speaker: Contested Deployment
0900 – 0915	Break
0915 – 1045	Panel 2: Contested Deployment
1045 – 1100	Break
1100 – 1200	Break Out Session – Contested Deployment
1200 – 1300	Lunch: Buffet
1300 – 1400	Break Out Session – Contested Deployment
1400 – 1415	Break
1415 – 1515	Break Out Session Back Briefs
1515 – 1530	Break
1530 – 1630	Guest Speaker: Major General Molstad

STRENGTH and WISDOM

2



THE UNITED STATES ARMY WAR COLLEGE

Schedule 8 February

0730 – 0800	Coffee Social
0800 – 0900	Capstone Speaker: LTG Evans
0900 – 0915	Break
0915 – 1045	Panel 3: Cognitive Defense
1045 – 1100	Break
1100 – 1200	Break Out Session- Cognitive Defense
1200 – 1300	Lunch: Buffet
1300 – 1400	Break Out Session – Cognitive Defense
1400 – 1415	Break
1415 – 1515	Break Out Session Backbriefs
1515 – 1530	Break
1530 – 1630	Closing Remarks

STRENGTH and WISDOM

APPENDIX 2: BREAKOUT GROUPS

Following each morning's plenary session, nine breakout groups assembled to consider questions posed by a facilitator.

a. **Purpose**. The purpose of the breakout groups was to identify areas that were not addressed during the speaker and panel presentations, add additional information to covered topics, or identify additional areas of study.

b. **Participants**. Groups assignments were predetermined to create a cross section of organizational representation. Each group included 12–13 participants from a variety of organizations, such as United States Northern Command, US Army North, National Guard Bureau, US Army Reserve, other services, other professional military education institutions, the interagency, and civilian academia.

c. **Method**. The group utilized the *Think, Write, Share* method in which the group spends five minutes in silent thought, spends another five minutes writing down their responses on note paper, and then each group member presented their top three answers to the first question. The facilitator and rapporteur captured their responses for consideration; then through group dialogue, similar answers were batched and themes identified.

d. **Back-Briefings**. After the group process, all participants reconvened in the day's final plenary session to listen to the spokespeople from three groups brief back their group's report. Over the three days of the symposium, each breakout group back-briefed once.

APPENDIX 3: SECOND ANNUAL HOMELAND DEFENSE SYMPOSIUM

UNITED STATES ARMY
WAR COLLEGE

2nd Annual

HOMELAND DEFENSE
>>>> SYMPOSIUM <<<<

[FEB 18-20 // CARLISLE BARRACKS]

IN-PERSON ATTENDANCE BY INVITATION ONLY

All are welcome to attend plenary sessions virtually
Register on our website:

FOR MORE INFO CONTACT:

- **Professor Bert Tussing**
  bert.b.tussing.civ@army.mil
- **Mr. Bob Foster**
  Robert.l.foster1.ctr@army.mil

250 YEARS OF HOMELAND DEFENSE

ACKNOWLEDGMENTS

We wish to thank our network of like-minded and supportive partners, large and small. Of special note, Dr. John Garver, the Director of the Homeland Defense Institute at the United States Air Force Academy, and Steve Recca, the Director of the University and Agency Partnership Program from the Center for Homeland Defense and Security at the Naval Postgraduate School, helped organize presentations on the themes of Defense of Critical Infrastructure and Cognitive Defense respectively. We are also grateful to our teammates at the Center for Strategic Leadership and our Drilling Individual Mobilization Augmentee reservists who served as facilitators and recorders for the breakouts.

Conference Organizer: Mr. Bob Foster

Proceedings Editor: George Schwartz, Ed.D.

Rapporteurs:

1. Dr. Michael Lynch
2. Mr. Andrew Bado
3. COL David Davis
4. Mr. Brian Gellert
5. LTC Gregory Gharst
6. COL James Grose
7. COL Melissa Kaiser
8. LTC Edward Keen
9. COL Shane Mantz
10. Mr. Adam Nicholson
11. Mr. Brian Waltman

The views expressed in this publication are those of the presenters/authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the US government. Authors of Center for Strategic Leadership publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official US policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This publication is cleared for public release; distribution is unlimited.

******

CSL

CENTER FOR STRATEGIC LEADERSHIP

U.S. ARMY WAR COLLEGE