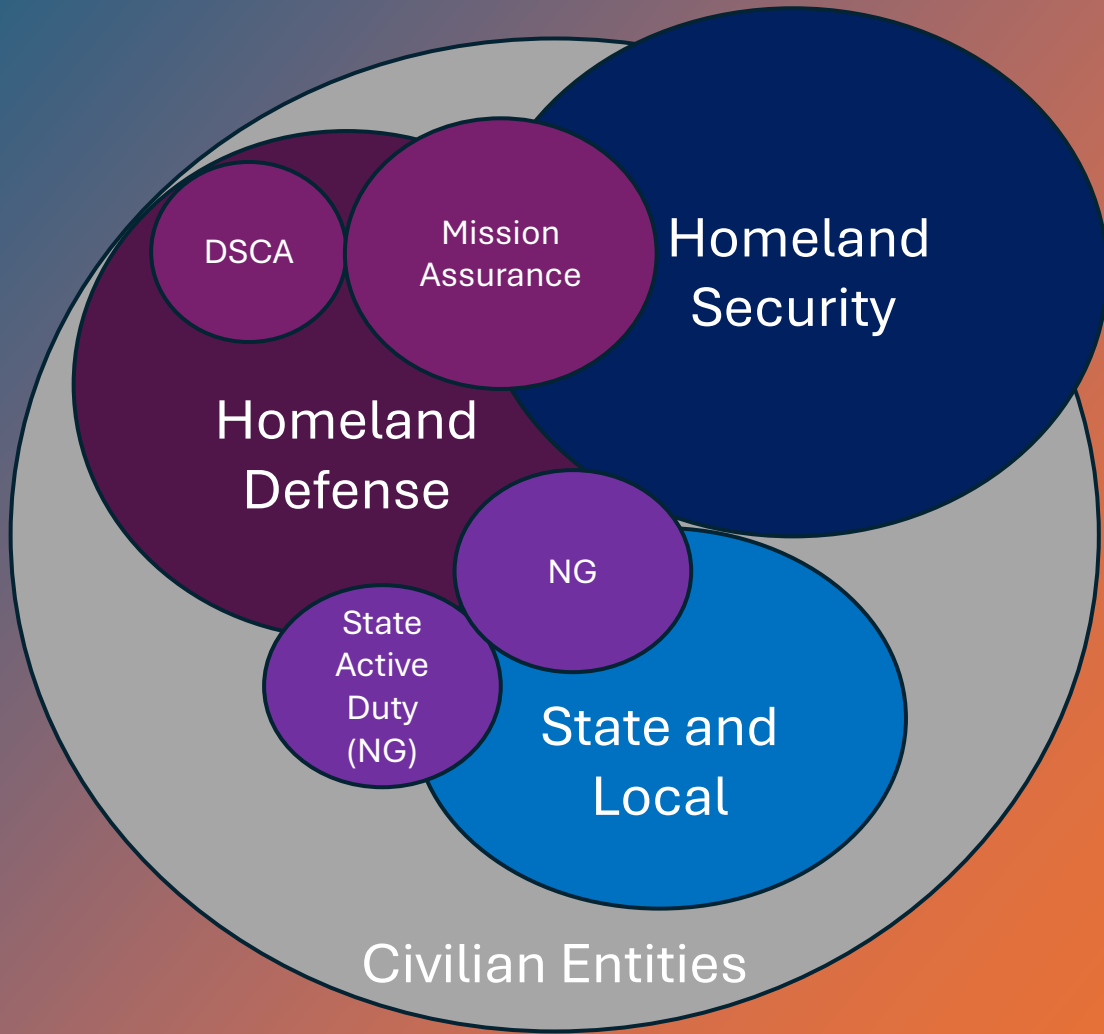# Kentucky National Guard Cyber Resilience Initiative
Closing the Homeland Security Gap

MG Haldane Lamberton

The Adjutant General

LTC Dayna Sanders

Cyber Program Manager/Deputy G6

What Gap?

- **Homeland Security:** National effort to prevent, reduce vulnerability, minimize damage, and recover from **terrorist** attacks.

- **Homeland Defense:** Deter, prevent, defeat, and mitigate **threats** to the nation and aid civil authorities in times of crisis.

...tivates Minnesota National Guard Following Sa...

...n Walz today issued an [executive order] activating cyber protection assets from t...
...a cyberattack on the city of Saint Paul.

...ing alongside the City of Saint Paul to restore cybersecurity as quickl...
...tional Guard's cyber forces will call...

China's new underwater tool cuts deep, exposing vulnerability of vital network of subsea cables

Story by John Calabrese • 1w • ⏱ 5 min read

Why Now?

...sophisticated Cyber Actor(s) Ta...
...perational Technology

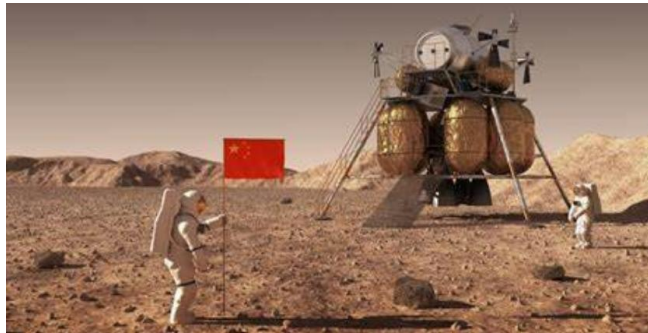...olar Power System Vulnerabilities Co...
Blackouts

James Coker
Deputy Editor, Infosecurity Magazine
Follow @ReporterCoker

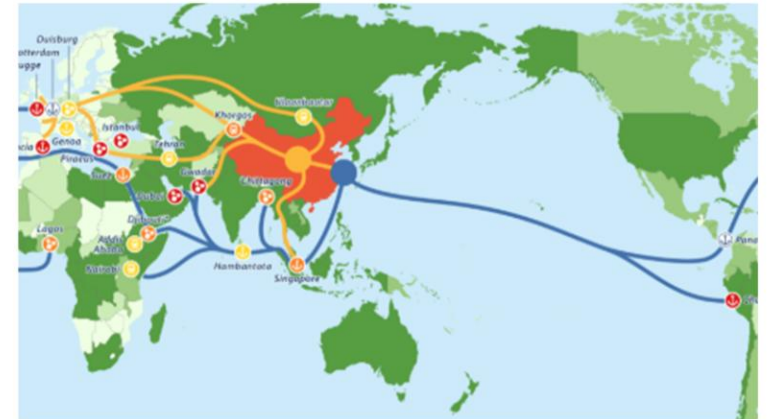...se Date: May 06, 2025

The kit drops fileless malware into legitimate software already in place, such as system tools.

Malicious activity is executed, while hidden in plain sight, providing remote access, stealing data, or disrupting operations.

Map of the States members of the BRICS
(Brazil, Russia, India, China, South Africa and proposed BRICS members)

- Brazil
- Russia
- India
- China
- South Africa

- Nicaragua
- Argentina
- Senegal
- Nigeria
- Algeria
- Egypt
- Saudi Arabia
- Iran
- Afghanistan
- Kazakhstan
- United Arab Mirates
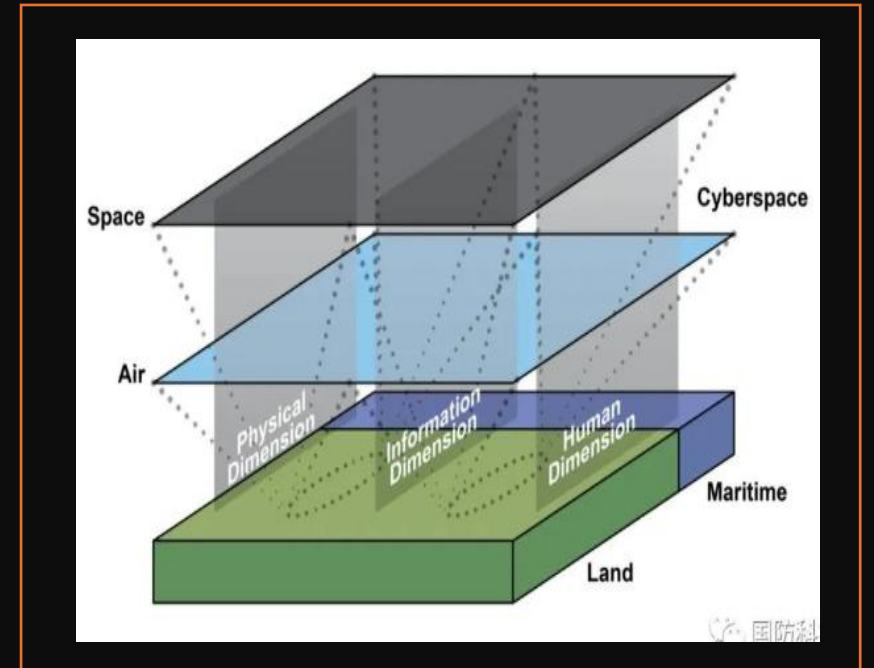- Indonesia

Proposed BRICS members

The Reality: *Everything* Short of Kinetic is a Battlefield

Reframing Our Approach

- Not Just a Military Problem: Whole of Government and Industry Problem

- Foreign and Domestic Focus

- Leverage Science AND Art

- Free vs Controlled Data Flow: Is it worth the risk?

- Collective Effort : Eliminate Current Silos

- Expanded Authorities

What Now?

INCREASE TRUST

SHARE CYBER CAPABILITIES

DECREASE RISK TO INFRASTRUCTURE

Together, We Secure Kentucky

Emergency Support Function (ESF) 17: Cybersecurity

- In the event of a significant cybersecurity incident, ESF17 provides a **centralized entity** for responding to a cyber incident that affects the Commonwealth of Kentucky.
- ESF 17 provides a means of defining, specifying, and maintaining the functions and resources required to ensure timely and consistent actions, communications, and response efforts.
- ESF 17 ensures appropriate coordination and inclusion of necessary state, federal, and local agencies, and private industry, to minimize the impact of a cybersecurity incident.
- Lead Agency: Kentucky Office of Homeland Security

KYCRI MISSION STATEMENT

The Kentucky National Guard Cyber Resilience Initiative (KY CRI) builds trust, cyber resiliency, and shared cyber capabilities and knowledge across public and private sectors through operating along four lines of effort.

What We Do

Federal Mission: provide cyber capability to combatant commands as required. Support Department of Defense Information Network (DODIN) compliance requirements to enable operations and readiness across KY.

Domestic Operations: train, advise, and assist requests to provide an enhanced defensive cyber capability to critical infrastructure owners.

Community Outreach: conduct engagements in the community to increase awareness of National Guard cyber capabilities and foster disaster preparedness.

Partnership Building: partner with academic government, private organizations and partner nations to exchange knowledge and information.

KYNG CAPABILITIES

- Army and Air National Guard Cyber and Signal assets
    - Satellite Tele-Communications
    - HF Radio
    - Mobile Internet Connectivity (Mobile & Satellite)
- Many members of the KYNG hold cyber/IT positions in their civilian jobs. They combine an intimate knowledge of leading-edge technologies from the private and public sector with a deep appreciation of cyber attacker's tradecraft that comes from a combination of civilian and military experiences.

Building a Cyber Network for the Future

Train	Advise	Assist
• Provide Education to Technical Workforce • Host Table Top Exercises for users, managerial, or technical staff • Provide user training specific to cyber practices	• Provide Advice and Recommendations on Cybersecurity Practices • Recommendations for Hardening Physical, Network, or System Environments	• Provide On-Site Assistance During Cyber Incidents • Provide Cyber Assessments to Better Secure Networks and Data

CYBER BLUEGRASS 2025

November 4-6 2025 – Boone National Guard Center, KY, Murray State University Campus, and University of Louisville School of Engineering.

- Training: Training is available 27-31 October

- Lead Organizations: Murray State University, The University of Louisville, & KYNG

- Host on Murray State University Cyber Range Environment

- **The goal of Cyber Bluegrass is to leverage** partners and resources across multiple public and private entities to establish a framework for cyber related disaster preparedness and response across FEMA Region 4 through building trust, cyber resiliency, and shared cyber capabilities and knowledge.

Support Requests

Requests for Support under a **declaration of emergency** come from local Emergency Managers through the KYEM system of record, WebEOC

Request for support **NOT** under a declaration of emergency are routed directly to the KYNG Cyber Initiatives Team. We will work with KYEM to ensure requirements are input into WebEOC.

kyngcyberinitiatives@army.mil