US Army Reserve

CYBER

Private Public Partnership Initiative (P3i)

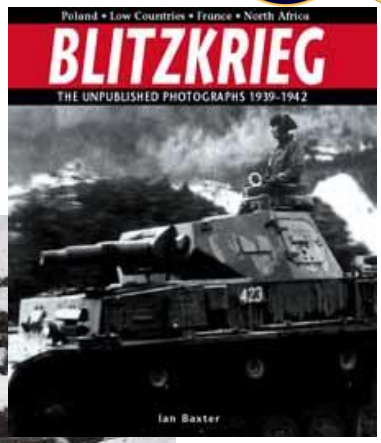
Overview

24 March 2015

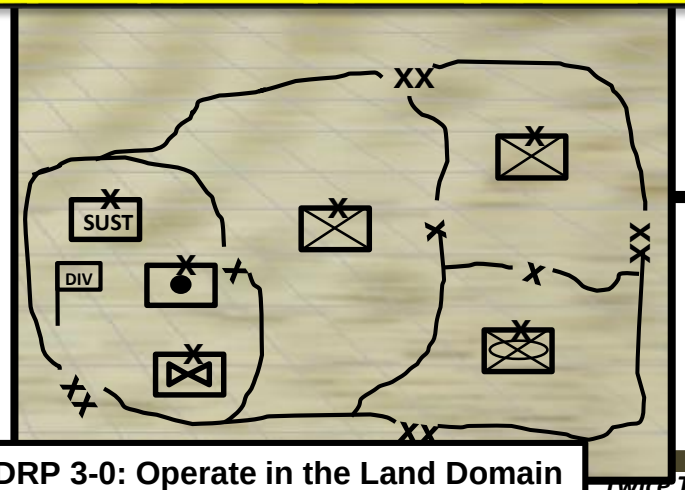
USAR Cyber Opportunity

Transforming the Force

1939
War
Transformed



"The inclusion of the cyberspace domain and the EMS greatly expands and complicates the operational framework transforming a limited physical battlefield to a global battlefield." – FM 3-38



ADRP 3-0: Operate in the Land Domain

Today
War
Transformed

FM 3-12 (TBP)/FM 3-38: Operate in the Cyberspace Domain / Electromagnetic Spectrum

Problem Statement

- **Background:** The US relies on information systems and data for almost every level of national power. US critical infrastructure and military operations are specifically at risk from Advanced Persistent Threats (nation-states, non- state actors, terrorists and criminal networks). The nature of cyber defense has shifted from passive defense, reliant on defense in depth and firewalls to active defense, with an emphasis on highly skilled and critical thinking cyber professionals. The demand for these individuals and units far outpaces the Cyber Soldier and unit inventory. The current DoD and Army school systems do not provide the through-put or advanced skills required for the USAR.

- **Problem Statement:**
  - National shortage of Cyber Security Professionals (50K in USG alone)
  - Significant Cyber Threat to Nation, DoD and Army
  - USAR Operational/Tactical shortfall (personnel, training, education, recruiting, retention)
  - Army demand for USAR Cyber capabilities is growing significantly
  - Army Reserve lacks approved innovative ways to generate equivalencies for cyber MOSQ/D
  - Army Reserve lacks Strategic Cyber Way Ahead

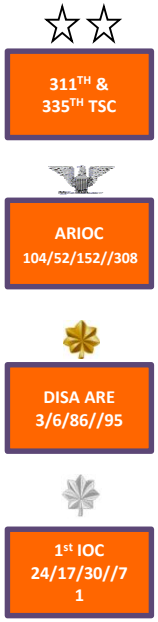
CAR Guidance-Intent-Endstate

- **Guidance and Intent:**
  CAR's #5 strategic priority: "Sustain and enhance Total Army Capability through employer partnerships and an innovative force mix that facilitates movement of Soldiers between active and reserve duty across a Continuum of Service."

- **Proposed Cyber P3i Endstate:**
  - G3/5/7 and USAR units enabled with inventory and skills
  - USAR Cyber personnel are recruited and retained to meet demand
  - USAR units meet readiness requirements for Cyber Defense
  - Cyber P3i enables innovative and effective training partnerships
  - Community relations with USAR is enhanced (Private and Public)
  - Cyber P3i integrated into USAR Cyber Strategic Way Ahead
  - Civil-Military equivalency program in place to generate MOSQ/D and Intermediate Cyber Core (ICC)
  - Army supports and values Cyber P3i effectiveness

FY14 USAR CYBER MISSION FORCE

Current USAR Cyber Force

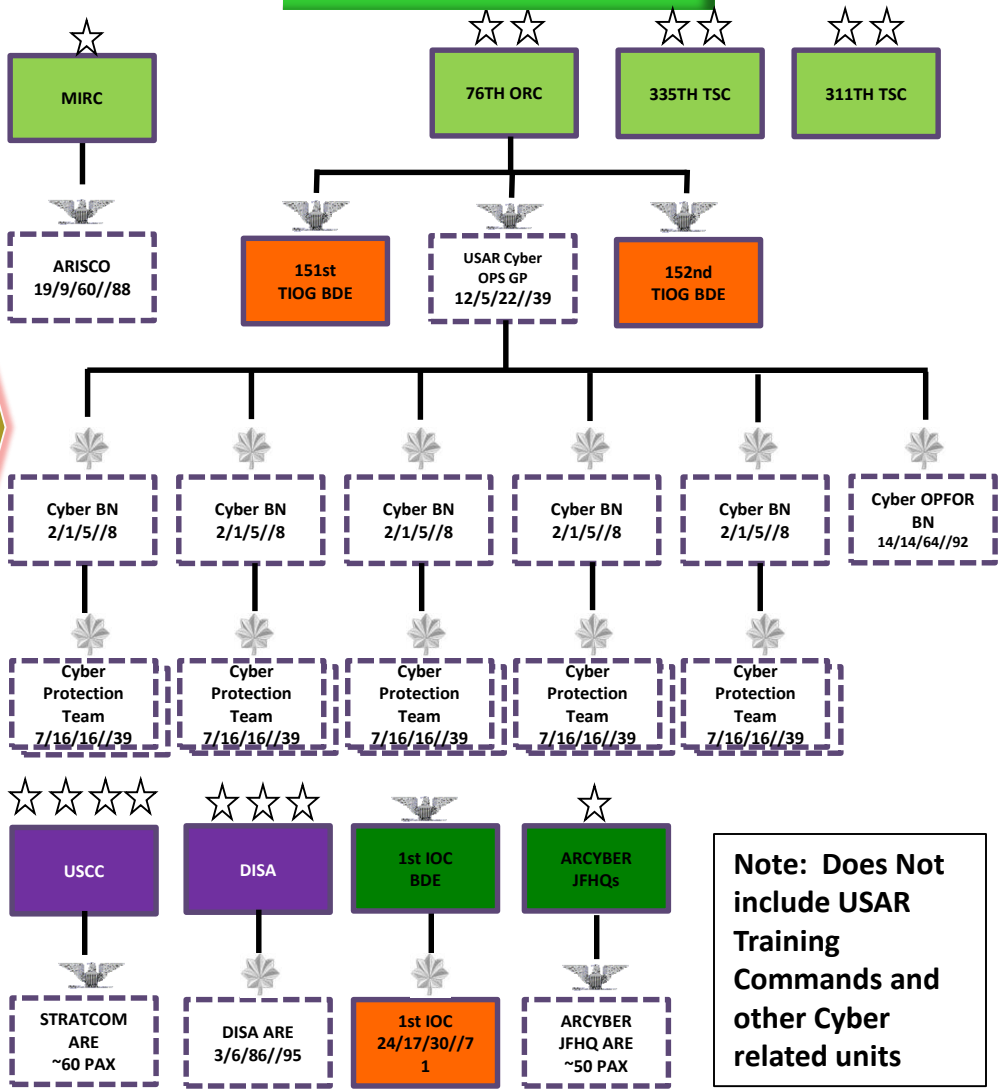


- **Army Reserve Concept For Cyber Force:**
  - To create 10x Cyber Protection Teams (39 PAX) and BN/BDE C^2 consisting of Cyber and MI soldiers
  - Provide a USAR Cyber OPFOR BN to supply cyber injects at USAR CSTP and surge support for 1st IOC WCCO and National Training Center Exercises
  - To create the ARISCO to provide Cyber targeting support to the 780th MI BDE
  - Create the multi-compo ARCYBER JFHQs which will provide intelligence and cyber planners for OCO and DCO missions
  - Transform the DISA ARE TDA into a CPT like structure which supports the DISA DoDIN Mission
- Soldiers identified for the Cyber Mission Force will begin training in both initial and functional cyber and intelligence courses.
- 335th and 311th TSCs continue to support the Southwest Asia and Pacific Regional Cyber Centers
- 151st and 152nd TIOGs have vulnerability scanning and OPSEC squads that support cyber missions

KEY

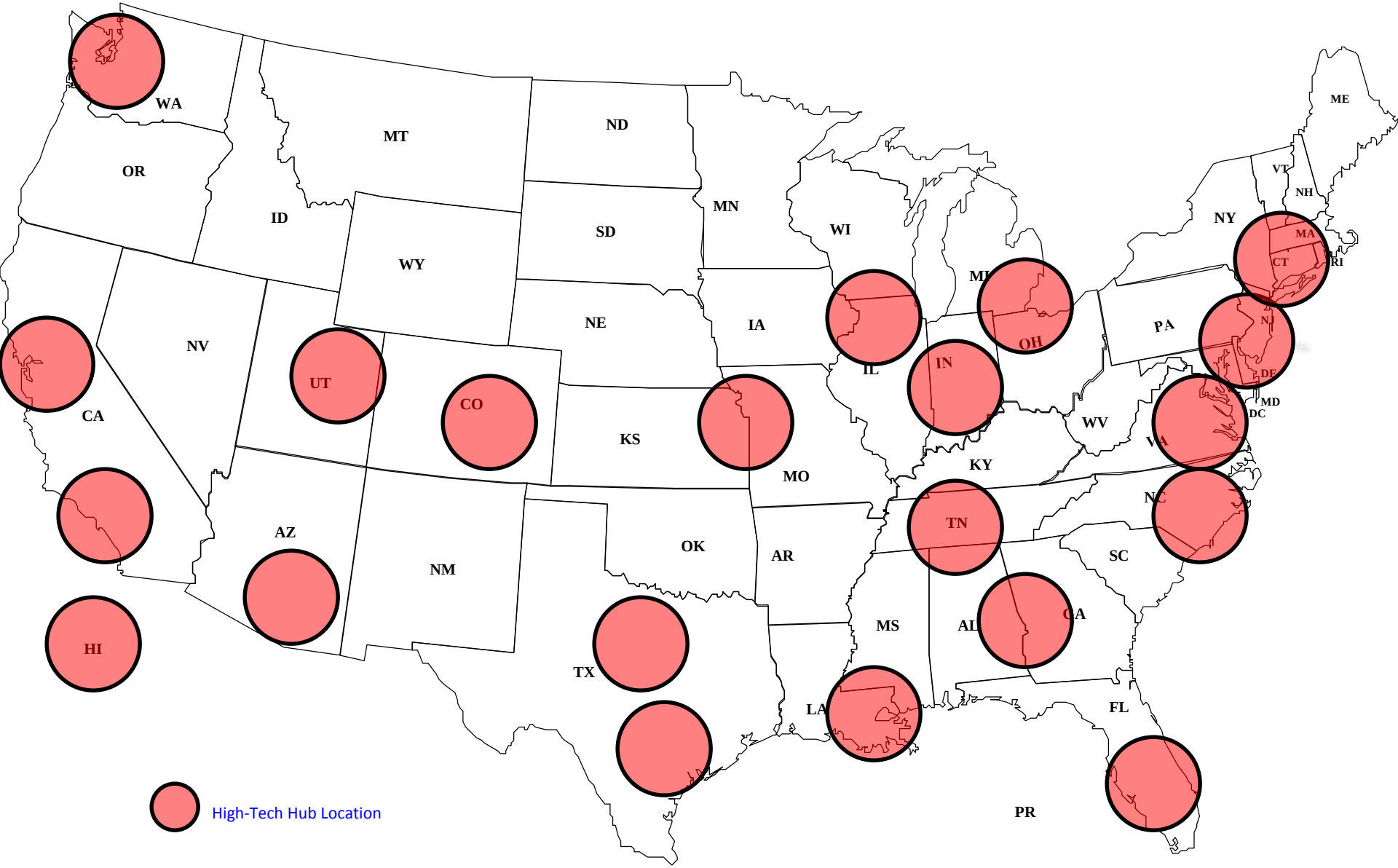
- CARRIER UIC
- IOC UNIT
- FOC UNIT
- USAR HQs
- Active Army HQs
- Joint Force HQ

Future USAR Cyber Force



Note: Does Not include USAR Training Commands and other Cyber related units

Current/Future Cyber Unit Similar Type Commands



USAR Cyber P3 Lines of Effort

Line of Effort 1: ACADEMIC NETWORKS: Develop University partnerships and networks of world class Cyber Security/ Cyber Engineering programs that can serve USAR Soldiers and transitioning Active Duty Soldiers in building foundational advanced Cyber skills, enhance existing cyber skills, and maintaining continuous professional education in the cyber career field.

Line of Effort 2: EMPLOYER NETWORKS: Develop comprehensive Employer Networks to support key program hypothesis that for Cyber Security Soldiers in the military cyber career field they must maintain advance cyber skills in civilian employment. Provide access points for USAR Soldiers and transitioning AC Soldiers into entry level, journeyman and master level cyber careers with the employer networks.

Line of Effort 3: COMMUNITY OUTREACH: Develop pilot Community Outreach programs from elementary, middle and High School to attract K-12 to Higher Education STEM programs, specifically Cyber Security and opportunities in the military/ USAR. This LOE will require strategic relationships with partner Universities and Employers and existing K-12 Cyber/STEM programs, such as Cyber Patriot (USAF Association).

Line of Effort 4: CYBER RESEARCH AND TRAINING INFRASTRUCTURE: Develop partnerships with University and Employer partners to design, build and operate Cyber Defense/ Cyber-Physical training/education and research infrastructure. This could include cyber labs, ranges, STX lanes and other training/education networks and programs that support Cyber immersion, collective training in Cyber-Physical, threat research and emulation allowing USAR Cyber forces to train as we fight (NTC/JRTC) – immersion real world closed exercise environments.

Line of Effort 5: STRATEGIC COMMUNICATION and OUTREACH: Internal and External communications to public, key external leaders and organizations and specifically internal USAR audiences – OUR SOLDIERS about the program, opportunities and benefits.

Cyber P3i – Linking Civilian/Military Careers

Employment Networks

USAR Cyber Capabilities/ Units

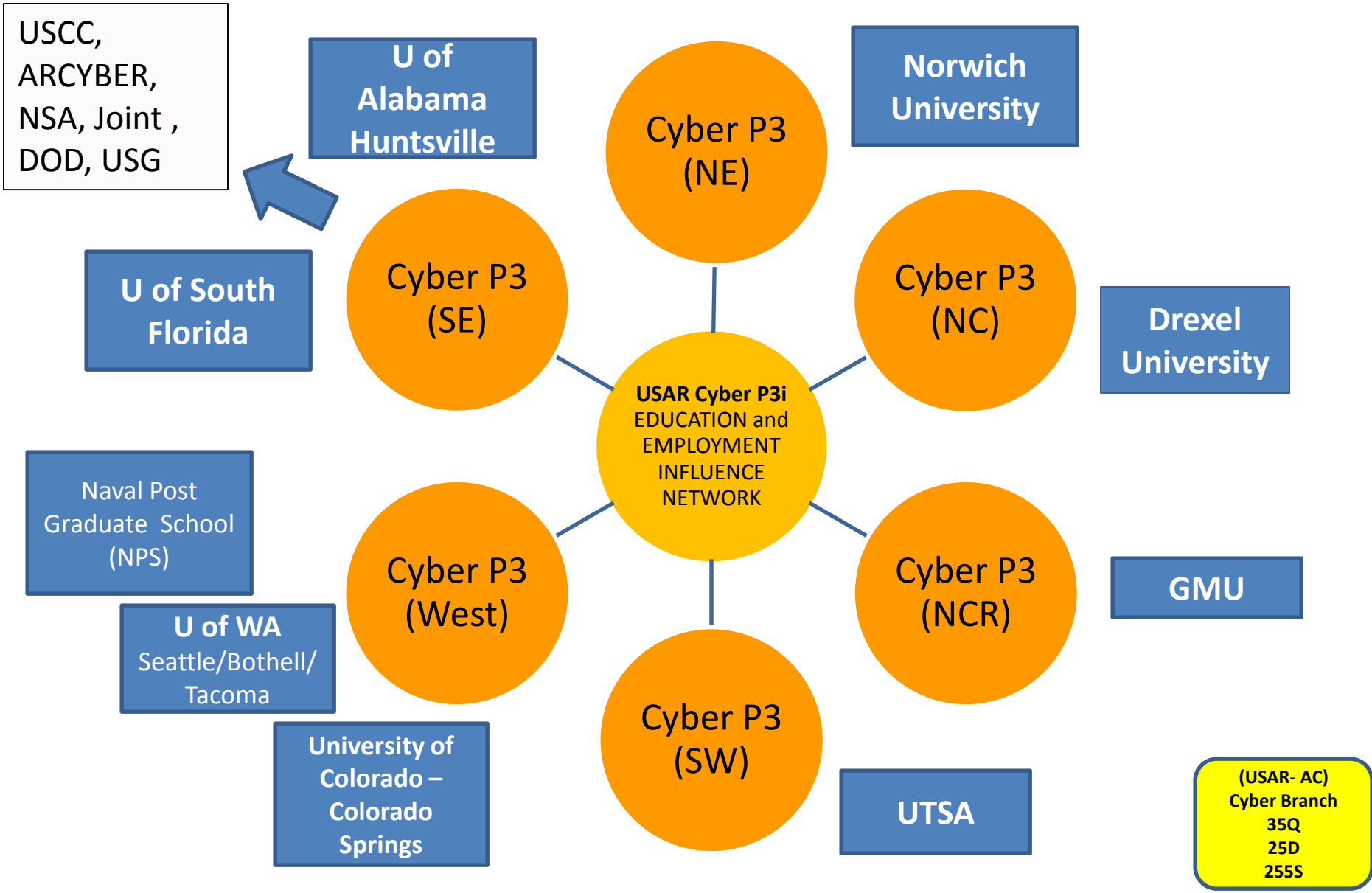
Enhanced Soldier Cyber Skills/KSAs

Academic Networks

USAR Soldier

Community Outreach

Regional USAR Cyber P3i (Academia)



University Selection Criteria

- Regionally Focused – co-located near USAR Cyber units/soldiers
- NSA/DHS Center for Academic Excellence (CAE) in Cyber Operations, Information Assurance or Cyber Research
- National Recognized Cyber program (Ponemon Survey)
- Cross-Discipline Programs (Business, Engineering, Computer Science etc)
- Diverse Cyber degree offerings (Bachelors, Masters, Certificates and PhD) in traditional, non-traditional and on-line
- Willingness to work with USAR

References:

- Ponemon Survey
- NSA CAE Schools

Initial University Selections

- **Selected Schools:**
  - **University of Texas/ San Antonio (UTSA)** Provost Letter of Intent – MOU - #1 School
  - **Norwich University** – All LOEs, AO visit scheduled for 27-29 OCT 14 pursue MOU - #2 School
  - **George Mason University**/ Letter of Intent pending – Same as UTSA/UW programs - # 7 School
  - **University of Washington (UW)** Cyber Security Director/ MOU - #10 School
  - **Naval Post Graduate School** – Cyber Scholarships/Fellowships (selected through put) # 27
  - **Drexel University/** Letter of Intent pending - Same as UTSA/UW programs - NSA CAE
  - **University of Colorado - Colorado Springs -** NSA CAE
  - University of South Florida (* partnership pending)
  - University of Alabama, Huntsville (*partnership pending)

- **Next Tier of Schools:**
  - **Already Engaged: (Phase II)**
    - **Texas A&M (College Station/ San Antonio**)/ Letter of Intent pending
    - **University of Massachusetts**
    - **University of Denver**
    - **Kansas State University**
    - **North Carolina State University**
    - **Auburn University**
    - **University of California Davis**

- To be engaged:

- **Georgia Tech**
- **Moorehead State**
- **Tuskegee**
- **U of Pittsburg**
- **Purdue University**
- **Virginia Tech**
- **VMI**

Employer Partners

- CALIBRE
- FBI
- Dynacorps
- URS/EA COM
- T-Mobile
- Verizon
- EMC
- Pro2Serve
- SABRE
- Microsoft
- Rack Space
- Chevron
- Parsons *
- Lockheed Martin *
- Palo Alto Networks *
- Hewlett Packard *
- JP Morgan Chase *
- Bank of America *
- Fox Entertainment *
- Northrop Grumman *

*** MOU in process**

Questions?