



U.S. ARMY CYBER COMMAND / U.S. 2ND ARMY

ARMY CYBER

- [Home](#)
- [Organization »](#)
- [News »](#)
- [History](#)
- [Support »](#)
- [Jobs »](#)

Cyber Chatter



[Subscribe to RSS Feed](#)

Army Cyber News

Army Cyber News

- **Lao officials train to fight cyber crime**
[JUL 04, 2013 - Asia One] Training has begun for IT engineers set to join the Lao Computer Emergency Response Team (LaoCERT), the country's first body dedicated to fighting cyber crime.
- **Digital Conflict**
[JUL 03, 2013 - Defense Systems - blog] How we train the next generation of officers who will lead our cyber forces is an emerging issue for the U.S. military. I previously covered some technical cyber training programs back in February 2011, but I did not address cyber training at the officer's level.
- **Army reservists unequipped for drive against cyber war**
[JUL 04, 2013 - Click Liverpool] Britain's Territorial Army are woefully unprepared to combat online terrorism - according to a leading UK IT entrepreneur.
- **Sentences for cyber crime and snooping to be tougher across EU**
[JUL 04, 2013 - Reuters] EU lawmakers agreed on Thursday to toughen criminal penalties across the European Union for cyber attacks, especially those that include harming critical national infrastructure and hijacking computers to steal sensitive data.
- **UK teams with defense and telecom companies on cyber security**
[JUL 05, 2013 - Reuters] Nine of the world's biggest weapon makers and telecoms providers are teaming up with Britain to bolster the country's cyber security, aiming to tackle the increasing threat of hacking and other such attacks.
- **Israeli cyber security firm Seculert raises \$10mIn in funding**
[JUL 08, 2013 - Reuters] Seculert, an Israeli cyber security firm, said on Monday that it has raised \$10 million in financing from Sequoia Capital and Norwest Venture Partners.
- **Cyber Attacks Continue To Threaten Critical Infrastructure**
[JUL 02, 2013 - Subnet] Cyber attacks are becoming increasingly prevalent for utilities, creating a growing need for vigilant cyber security policies to defend the nation's critical infrastructure.
- **NSA Revelations Raise Doubts About Passage Of Cybersecurity Legislation**
[JUL 02, 2013 - Homeland Security News Wire] U.S. officials say the revelations about the National Security Agency's(NSA) domestic surveillance programs could make it harder for lawmakers to pass a cybersecurity bill. Critics of the House cybersecurity bill, known as the Cyber Intelligence Sharing and Protection Act (CISPA), which was passed earlier this year (it is still being debated in the Senate), argued the bill could lead to private information falling into the hands of the NSA.
- **Can State And Local Govs Benefit From The U.S. Commerce Department's Cybersecurity Program?**
[JUL 05, 2013 - Government Technology] <http://www.govtech.com/security/Can-State-and-Local-Govs-Benefit-from-the-US-Commerce-Departments-Cybersecurity-Program.html> Data breaches are inevitable. As Michigan CSO Dan Lohrmann noted earlier this year, small security breaches occur in government more often than many people are aware of -- and then there are the large, widely publicized breaches, most recently in California, the Washington State Courts and last year at the South Carolina Department of Revenue.

Army Cyber Command hosts the Under SecArmy

Under Secretary of the Army Dr. Joseph W. Westphal visited the U.S. Army Cyber Command Headquarters at Fort Belvoir, Va., Jan. 10, to gain situational awareness and ensure the Army is correctly prioritizing, balancing and integrating resources to support the mission of this newly-established and mission-critical organization.



SOUNDOFF!

U.S. Cyber Command held a joint cyberspace training exercise during the first week in November, primarily conducted at the Air Force Red Flag Facility at Nellis Air Force Base, Nev. The exercise brought together approximately 300 cyber and IT professionals.



Fort Belvoir Celebrates U.S. Army Birthday

Lt. Gen. Rhett A. Hernandez (Commander, U.S. Army Cyber Command) speaks at the U.S. Army 236th birthday celebration

- Port Of Baltimore Is Vulnerable To Cyber Attack, Brookings Study Says**
 [JUL 05, 2013 - The Baltimore Sun] U.S. commerce "would grind to a halt in a matter of days" in the aftermath of a crippling cyberattack that the nation's ports — including Baltimore — are ill-prepared for, according to a new Brookings Institution report.
- For months it has been an entertaining parlor game in the nation's capital: guessing what will happen**
 [JUL 03, 2013 - Baltimore Business Journal] Cyber security job growth, particularly in the Fort George G. Meade area, has made the Baltimore region one of the hottest office markets in the nation, according to a report issued this week by Cassidy Turley.
- The future of U.S. Cyber Command**
 [JUL 03, 2013 - National Interest.org] For months it has been an entertaining parlor game in the nation's capital: guessing what will happen next with U.S. Cyber Command, the military organization designed to defend the country's networks and attack its adversaries. The topic will increasingly be in the spotlight as the head of that command, General Keith Alexander, is also the director of the National Security Agency, which is beset by revelations of cyber snooping —possibly a damaging link if the crisis does not blow over.
- Talking to China on the cyber threat**
 [JUL 07, 2013 - Financial Times, editorial] Senior officials from the US and China will meet in Washington this week for the latest round of their high-profile Strategic and Economic Dialogue. Following last month's summit between President Barack Obama and Chinese leader Xi Jinping, there is much for both sides to discuss. The US wants the new Chinese leadership to take a tougher line over North Korea's nuclear programme.
- Security experts reveal cyber attack threat to Olympics**
 [JUL 08, 2013 - Independent] Security experts have revealed that they received suggestions of a cyber attack targeted at the opening ceremony of last summer's Olympic Games.
- Ex-FBI chief Louis Freeh warns of cyber threats**
 [JUL 07, 2013 - Politico] United States intelligence officials must do a better job analyzing the mountains of global Internet, telephone and financial data they already collect to thwart the cyber terrorists of tomorrow, according to former FBI director Louis Freeh.

Change of Command

Lt. Gen. Rhett A. Hernandez assumed command of the U.S. Army Cyber Command during a ceremony officiated by Army Vice Chief of Staff Gen. Peter W. Chiarelli.

Lt. Gen. Rhett A. Hernandez

[External Link Disclaimer](#)

