



UNITED STATES MILITARY ACADEMY
WEST POINT.



Defending the Nation in Cyberspace

Colonel Jon Brickey
Army Cyber Institute, West Point

The opinions expressed herein are those of the author, and are not necessarily representative of those of the Department of Defense, the United States Army, or the Army Cyber Institute.

"Momentum non vertendum" - Irreversible Momentum



Vision

To develop intellectual capital and impactful partnerships that enable the nation to outmaneuver our adversaries in cyberspace.

Mission

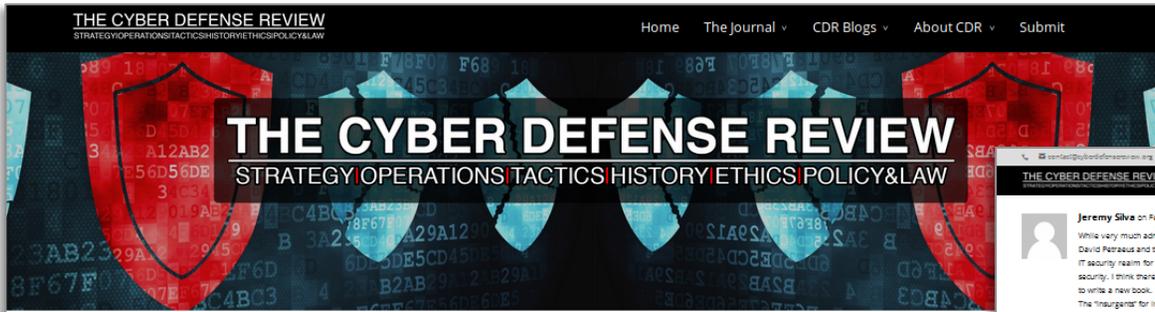
The ACI is a national resource for research, advice and education in the cyber domain, engaging Army, government, academic, and industrial cyber communities in impactful partnerships to build intellectual capital and expand the knowledge base for the purpose of enabling effective Army cyber defense and cyber operations.

Values

Excellence – Do everything well and people will trust us
Partnership – Non-competitive, results-driven team effort
Innovation – Think outside the box, avoid groupthink
Candor – Remain tribe-agnostic and be an honest broker



The Honorable John McHugh with LTG Caslen and COL Conti at the ACI Ribbon-Cutting Ceremony on 3 Oct 2014



Welcome!

Welcome to The Cyber Defense Review, a forum for current and emerging research on cyber operations. This joint effort between the Army Cyber U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER) grew out of a shared recognition of the need for a professional publication focus strategy, operations, tactics, history, ethics, law and policy in the cyber domain. The Cyber Defense Review (CDR) is positioning itself as the leading print journal for issues related to cyber for military, industry, professional and academic scholars, practitioners and operators interested providing important research to advance the body of knowledge in an inherently multi-disciplinary field. The CDR provides an unclassified venue for content an online journal with longer more thoroughly researched articles and a blog with short engaging thought pieces to stir rapid discussion within the community. We publish original, unpublished, relevant and engaging contributed content from across the community.

The CDR will initially be an online-only offering, designed for the timely publication of well-researched articles to facilitate dynamic multi-disciplinary within this community. We will simultaneously begin accepting articles for the Cyber Defense Review print journal. The print journal will be a peer-publication for robust original, unpublished work to facilitate meaningful discussion. Please see the link to our Call for Papers under the Submit menu.

The CDR is designed to spur debate and serve as a platform where conventional wisdom can be supported and/or questioned. The CDR will consist of our diverse community across military services, academic disciplines, technical communities, and backgrounds to cross-pollinate ideas with the solving tomorrow's problems today. It serves as a marketplace that rewards sound logic, creativity, and innovative solutions to the problems faced military, national, and global cybersecurity community.

Please explore our offerings, provide feedback and contribute. Check back often as we will be adding articles and blog posts regularly. Join the community.

Signed,

MajGen D. J. O'Donohue
Commander, MARFORCYBER

COL Gregory Conti
Director, Army Cyber Institute

THE CYBER DEFENSE REVIEW

Home The Journal CDR Blogs About CDR Submit

Jeremy Silva on February 20, 2015 at 8:30 am Reply

While very much admittedly a newcomer to the COIN FM (just finished "The Insurgents: David Petraeus and the Plot to Change the American Way of War"), but having been in the IT security realm for a while, I am really interested in the COIN application to the cyber-security. I think there is a good deal that can apply, but there may be yet another reason to write a new book.

The "insurgents" for instance, are an incredibly diverse group, ranging from loose activist groups to incredibly well funded groups.

Tactics do not change weekly, but change almost by the minute especially with cyber-criminal syndicates who employ legions of staff to create zero-day attacks for a burgeoning marketplace.

Also what is the goal of the COIN operation? It is continuous and there is no true population to sway (maybe worldwide).

I am really fascinated by this adaptation and hope more discussion is generated on the subject.

Dave Cruoe on February 19, 2015 at 9:05 pm Reply

All,

To which I submit that the collateral damage is far more expansive than the damage any specific attack or counterattack, or the unintended spread of such, inflicts.

The potential collateral damage is in the information that the defense provides to the defender in the form of technique, code, application &c. information and knowledge are absolutely critical elements to manage, along with the literal code impact of any deployment.

R.E. Campbell on February 18, 2015 at 4:01 pm Reply

I am not military and am retired IT worker. While I was trained in a number of cyber security areas, I felt that the core problem was with the software infrastructure and the diverse products that made it up.

To follow your example, this was like fighting to defend a conflagration of software products where you have little power to change or otherwise affect the behavior of the individual units and their relationship to the population of users. This was a perfect environment for different attacks by many enemies. David Rice's 2007 book, "Geekonomics" spelled out some of the costs of this defective software infrastructure. Until that is addressed, the war will continue...with casualties. I wish you success.

Wesley Parish on February 18, 2015 at 1:38 am Reply

I read a statement a few years ago to the effect that the US problem in Vietnam was that it had plenty of perimeter but no hinterland, while the Vietnam side had no perimeter but plenty of hinterland. Consequently counterinsurgency couldn't last as long as the insurgency ...

I can see the merit of the counterinsurgency analogy, but I think its only relevant to specific parts of the problem. What if one has an unreliable team member on your side? And cyber attack paths can be difficult to trace. And - another analogy - "cyber weaponry", like land mines and discarded ammunition, can last for quite a long time in the wild, as long as they have a host environment.

Submit a Comment

Your email address will not be published. Required fields are marked *

Name *

Email *

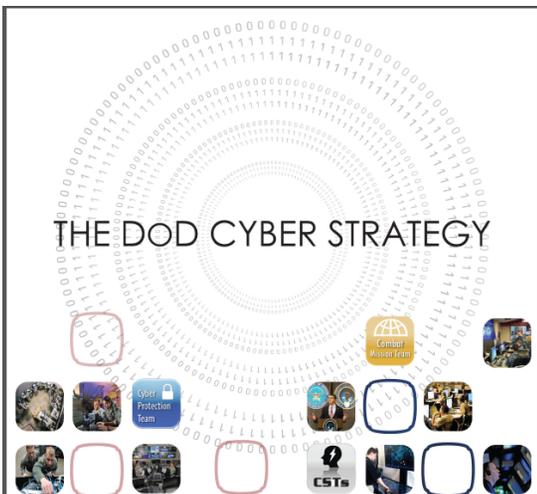


- DoD Cyberspace Strategy & Vision
- Cyber Education & Training
- Partnerships
- Research



Strategic Goals

- I. Build and maintain ready forces and capabilities to conduct cyberspace operations.....
- II. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions
- III. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence.
- IV. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.....
- V. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.





- Joint Training Standards
- Service Courses
- Army
 - New Branch, Cyber School
 - Cyber Leader Development Program
- Non-military Education: growing options
- Industry Training: many options



- DOD Cyberspace Strategy
- International
- Interagency
- Industry & Academia
 - Defense Innovation Unit - Experimental (DIUx)
 - US Army Reserve P3i
 - Army Cyber Institute



Leveraging Partnerships

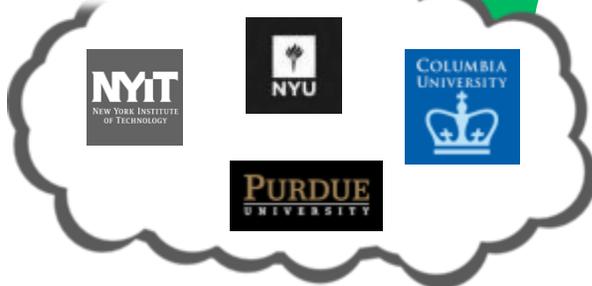
Government



Industry



Academia



31+ productive or emerging partners

Some examples of how the ACI is currently leveraging partnerships

- **FBI Cyber Center (NYC):** table-top cyber exercise for all NYC
- **Columbia University (NYC):** determining what future cyber policy and laws should be
- **Citi Group (NYC):** cyber talent management best practices
- **Cubic Corporation:** research the intersection of cyber and kinetic operations and training
- **ARCYBER:** Cyber Talks
- **MARFORCYBER:** Cyber Defense Review (journal)
- **Purdue University:** history of cyber operations



- ACI top 3: Big Data, Internet of Things, Cyber Operations at the Army Tactical Level
- Cyber Immediate Response Authority
- Cyber Escorts (like Naval Escorts)

