The Interim Years of Cyberspace

Robert M. Lee

Twitter: @RobertMLee

RobertMichael.Lee@Gmail.com

Intro

- AF Cyberspace Operations Officer
- Germany
- AF ISR Agency

CYA

The opinions and statements expressed by Robert M. Lee are his own and do not represent or constitute an opinion of the United States Government, Department of Defense, or AF.

Takeaways

- Lessons Learned from Airpower
- Interim Years of Cyberspace
- Cyber Capabilities vs FUD
- Sphere of Influence

Lessons Learned from Airpower

Interim Years of Airpower

- Time between WWI and WWII
- Airshows and developments
- Advocates and pioneers

The Bomber Always Gets Through

Vectored Approach

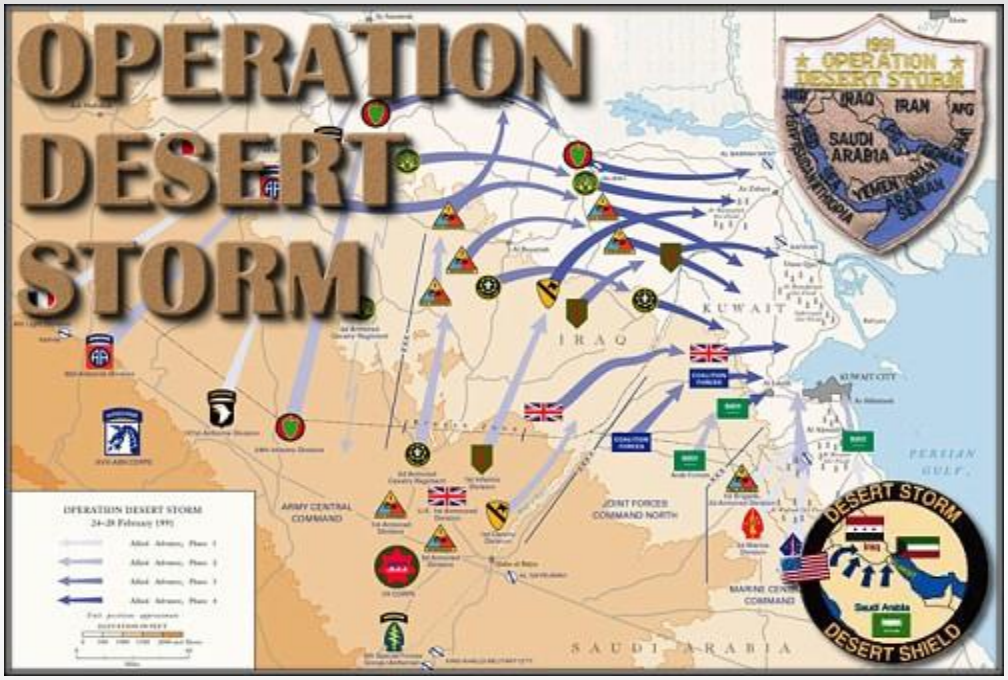
Capabilities can = Statements


Blur the Lines of War

Education and Tactics

Aspects of the Interim Years of Cyber

Interim Years of Cyberspace



- Cyber capabilities for multiple decades
- Nation-states testing capabilities/strategies
- Non nation-state actor involvement
- Ongoing nation-state operations

U.S. general: We hacked the enemy in Afghanistan

By Raphael Satter, Associated Press

Updated 8/24/2012 9:25 PM

The U.S. military has been launching cyberattacks against its opponents in Afghanistan, a senior officer says, making an unusually explicit acknowledgment of the oft-hidden world of electronic warfare.

By Gerald Herbert, AP

Lt. Gen. Richard Mills speaks during christening ceremonies for the USS Somerset at the Huntington Ingalls Industries shipyard in Avondale, La.

Marine Lt. Gen. Richard P. Mills' comments came last week at a conference in Baltimore during which he explained how U.S. commanders considered cyber weapons an important part of their arsenal.

"I can tell you that as a commander in Afghanistan in the year 2010, I was able to use my cyber operations against my adversary with great impact," Mills said. "I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations."

Mills, now a deputy commandant with the Marine Corps, was in charge of international forces in southwestern Afghanistan between 2010 and 2011, according to his official biography. He didn't go into any further detail as to the nature or scope of his forces' attacks, but experts said that such a public admission that they were being carried out was itself striking.

"This is news," said James Lewis, a cyber-security analyst with the Washington-based Center for Strategic and International Studies. He said that while it was generally known in defense circles that cyberattacks had been carried out by U.S. forces in Afghanistan, he had never seen a senior officer take credit for them in such a way.

"It's not secret," Lewis said in a telephone interview, but he added: "I haven't seen as explicit a statement on this as the one" Mills made.

Pentagon spokesman Lt. Col. Damien Pickart declined to elaborate on Mills' comments, saying in an email that "for reasons of security . we do not provide specific information

“I can tell you that as a commander in Afghanistan in the year 2010, I was able to use my cyber operations against my adversary with great impact. I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire to affect my operations.”
- Marine Lt. Gen. Richard P. Mills

www.cbsnews.com/8301-18563_162-57353420/panetta-cyber-warfare-could-paralyze-u.s/

28 comments

47

Like

Panetta: Cyber warfare could paralyze U.S.

By **Scott Pelley**

"The reality is that there is the cyber capability to basically bring down our power grid to create…to paralyze our financial system in this country to virtually paralyze our country."
- US Secretary of Defense Leon Panetta

…, the Pentagon established …yber command to wage war and defend America's …r systems. It's a top priority for Secretary of Defense Leon Panetta. In an interview for "60 …" CBS Evening News anchor Scott Pelley spoke with Panetta while he was touring the …ast last month, flying in a command post that's rigged to conduct nuclear war if need be. The Secretary told CBS News cyber war is one of his biggest worries.

Panetta: The reality is that there is the cyber capability to basically bring down our power grid to create ... to paralyze our financial system in this country to virtually paralyze our country. And I think we have to be prepared not only to defend against that kind of attack but if necessary we are going to have to be prepared to be able to be aggressive when it comes to cyber efforts as well. We've got to develop the technology, the capability, we've got to be able to defend this country.

Panetta to Pelley: Iran will not be allowed nukes
60 Minutes: Cyber War, sabotaging the System
Pentagon: Cyber warfare skills inadequate
North Korea waging cyber warfare?

Pelley: Is it fair to characterize your cyber command as currently engaged in battle every day?

Panetta: That's one of the interesting questions. What constitutes an act of war when it comes to cyber warfare? Countries use cyber as a way to exploit information. I think the Chinese use it as a way to gain information in the business arena. But if a cyber effort were made that, in fact, crippled this country or paralyzed this country or hit a major grid system then you have to ask the question does this constitute an act of war?

WE ARE ANONYMOUS

Because none of us are as cruel as all of us.

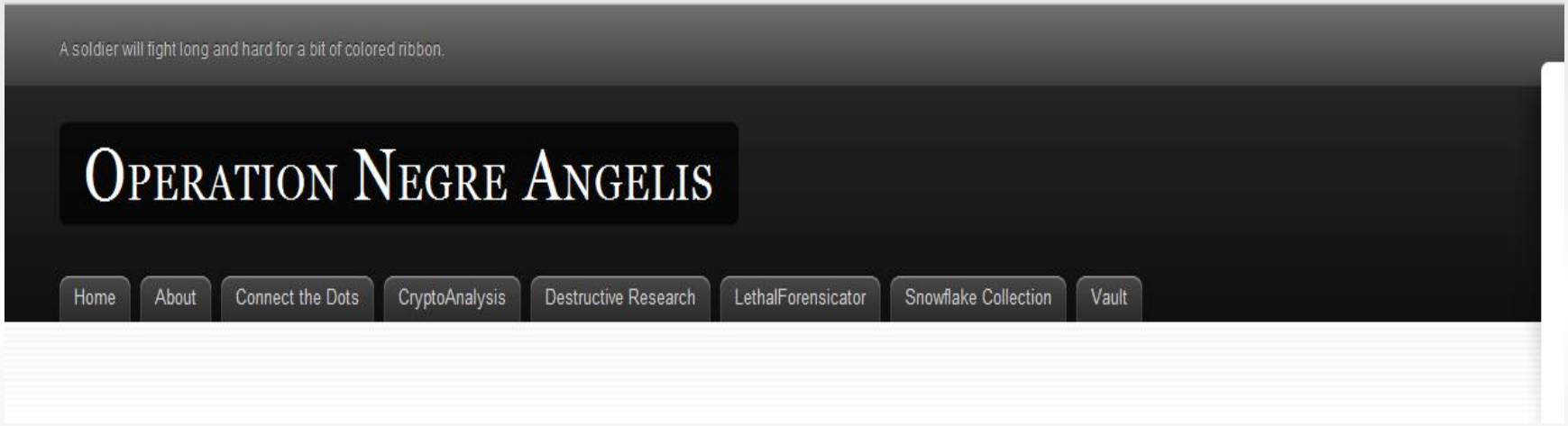
HACKERS FOR CHARITY.ORG

Jester

@th3j35t3r Everywhere

Hacktivist for good. Obstructing the lines of communication for terrorists, sympathizers, fixers, facilitators, oppressive regimes and other general bad guys.

http://th3j35t3r.wordpress.com



OperationONA@Gmail.com

Google | Take Action

+1 164k

Home **What's at stake** What you can do Past actions **Make your voice heard**

What's at stake?

A free and open world depends on a free and open Internet.

The Internet empowers everyone — anyone can speak, create, learn, and share. It is controlled by no one — no single organization, individual, or government. It connects the world. Today, more than two billion people are online — about a third of the planet.

Important Issues During Interim Years

- Understanding/deciding authorities, legalities, definitions, and limitations
- Military, commerce, social media, etc. roles
- Internet privacy concerns and rights
- Regardless of your views on the subject matter this is a critical time for cyberspace

Civ-Mil Sharing

- Varied expertise focused
- Innovative solutions and revolutionary ideas
- Threat Intelligence
- Protection of basic rights and principles

The Seriousness of the Future

Realism vs. FUD


JUST LIKE CSI:
ENHANCE ALL THE IMAGES
memegenerator.net

Buy My *Insert Latest Tech of Day*

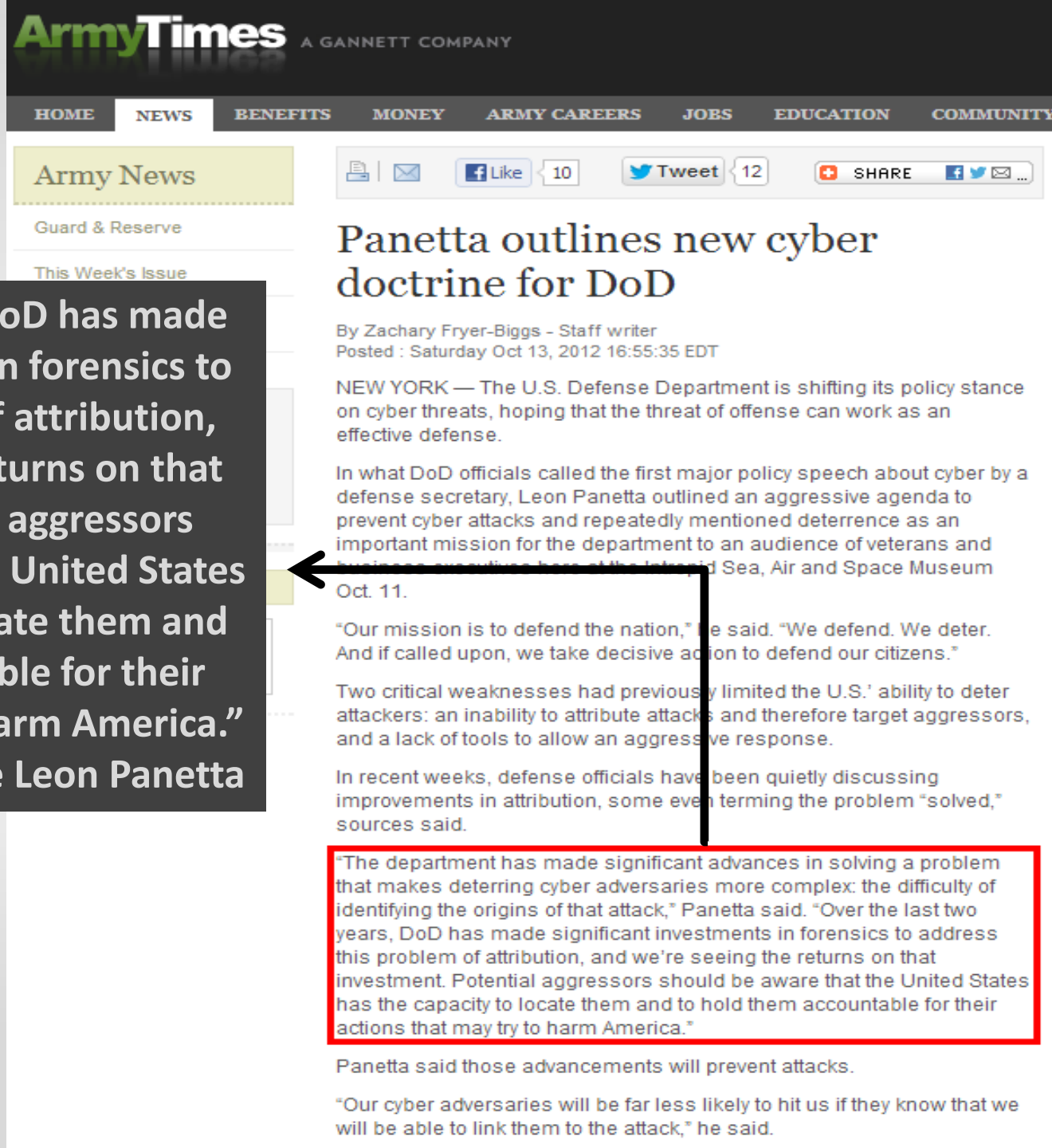
- Not all technologies are created equally
  - "It's easy to install and practically protects the network itself!"
- Attackers do their homework, defenders must as well
- Plenty of people make a business on FUD
- Are there really this massive spike in "APT"? Is this something new?

More Threats or Better Analysts?

Education, tools, & skill increases = More Discoveries

Nation-states testing capabilities = More Threats

"In the last two years, DoD has made significant investments in forensics to address this problem of attribution, and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capability to locate them and to hold them accountable for their actions that may try to harm America."
- US Secretary of Defense Leon Panetta



ArmyTimes A GANNETT COMPANY

HOME | NEWS | BENEFITS | MONEY | ARMY CAREERS | JOBS | EDUCATION | COMMUNITY

Army News

Guard & Reserve

This Week's Issue

Like 10 Tweet 12 SHARE

Panetta outlines new cyber doctrine for DoD

By Zachary Fryer-Biggs - Staff writer
Posted : Saturday Oct 13, 2012 16:55:35 EDT

NEW YORK — The U.S. Defense Department is shifting its policy stance on cyber threats, hoping that the threat of offense can work as an effective defense.

In what DoD officials called the first major policy speech about cyber by a defense secretary, Leon Panetta outlined an aggressive agenda to prevent cyber attacks and repeatedly mentioned deterrence as an important mission for the department to an audience of veterans and [illegible] Sea, Air and Space Museum Oct. 11.

"Our mission is to defend the nation," he said. "We defend. We deter. And if called upon, we take decisive action to defend our citizens."

Two critical weaknesses had previously limited the U.S.' ability to deter attackers: an inability to attribute attacks and therefore target aggressors, and a lack of tools to allow an aggressive response.

In recent weeks, defense officials have been quietly discussing improvements in attribution, some even terming the problem "solved," sources said.

"The department has made significant advances in solving a problem that makes deterring cyber adversaries more complex: the difficulty of identifying the origins of that attack," Panetta said. "Over the last two years, DoD has made significant investments in forensics to address this problem of attribution, and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America."

Panetta said those advancements will prevent attacks.

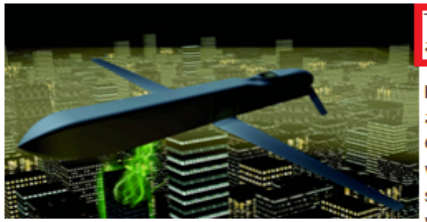
"Our cyber adversaries will be far less likely to hit us if they know that we will be able to link them to the attack," he said.

Capabilities We Know Of…

- Bronze Night – 2007
- Aurora - 2009
- Stuxnet – 2010
- DuQu – 2011
- Flame – 2012
- Shamoon – 2012
- APT1 (Mandiant Report) - 2013

Nation-State Weapons

- Not single purposed
  - UAVs/F16s/F35s/etc
  - Multiple payloads
  - F35 features include:
"ground attack, air defense missions, and reconnaissance"



The U.S. Air Force is developing network weapons to attack aircraft.

Electronic warfare specialists know the technology is already a double-edged sword, however. The Chinese, a senior service official says, are already working hard on, and in some cases fielding, similar systems to attack high-value aircraft used for early warning, electronic surveillance, command and control, and intelligence.

The Air Force is pursuing "cyber-methods to defeat aircraft," Gen. Norton Schwartz, the service's chief of staff, told attendees at the 2012 Credit Suisse and McAleese Associates Defense Programs conference in Washington March 8. But Lt. Gen. Herbert Carlisle, the deputy chief of staff for operations, says the same threat to U.S. aircraft already is "out there."

Ashton Carter, deputy secretary of defense, is pushing both offensive and defensive network-attack skills and technology. "I'm not remotely satisfied" with the Pentagon's cyber-capabilities, Carter says.

"The Russians and the Chinese have designed specific electronic warfare platforms to go after all our high-value assets," Carlisle says. "Electronic attack can be the method of penetrating a system to implant viruses. You've got to find a way into the workings of that [target] system, and generally that's through some sort of emitted signal."

The Chinese have electronic attack means — both ground-based and aircraft-mounted — specifically designed to attack E-3 AWACS, E-8 Joint Stars and P-8 maritime patrol aircraft, he says.

Schwartz revealed no other details, but several years ago the service tested the "Suter" system, which used a data stream filled with algorithms to invade an integrated air defense (IAD) system through its antennas. The data-stream, generated by an EC-130 Compass Call electronic-attack aircraft, was able to capture the enemy pictures, take over the network as system administrator and tap into di launchers through their wireless communication links. Changes to or effe of the enemy IAD system were monitored by an RC-135 Rivet Joint sign aircraft.

A fielded version of the system was used by Compass Call aircraft in Ira to tap into wireless telephone systems used to control improvised explo However, the EC-130 is a large, slow aircraft that does not fly at high a vulnerable to anti-aircraft guns and missile fire. So the task has become network invasion device small enough to fit into a stealthy aircraft — m unmanned, strike or reconnaissance — that can penetrate to a useful t attack enemy electronics and networks.

New U.S. aircraft like the F-22, F-35, EA-18G and F/A-18E/F now carry active electronically scanned array (AESA) radars that are being considered as part of an electronic-attack/network-invasion capability. However, different versions of the AESA arrays are being tailored to better fit the cyber/electronic attack mission. Some will go on unmanned designs like Boeing's Champ cruise missile, Raytheon's MALD-J jamming missile and a line of Mk.-82 bomb shapes to carry out the electronic attack role. Other designs will be tailored for the Suter-like, network-invasion task.

3/23/2012 3:02 PM CDT

Recent Photos View all photo galleries

"The Air Force is pursuing cyber-methods to defeat aircraft"
- Gen. Norton Schwartz

Selected Videos View all video galleries


LHT Budapest
2:36


Hot Jobs: Four Young Professionals
3:00


Jetman Yves Rossy
2:31

"The Russians and the Chinese have designed specific electronic warfare platforms to go after all our high-value assets. Electronic Attack can be the method of penetrating a system to implant viruses."
- Deputy Secretary of Defense Ashton Carter

Hypothetical Attack Scenario

Industrial Control Systems

Certificate Authorities

Cyber Espionage

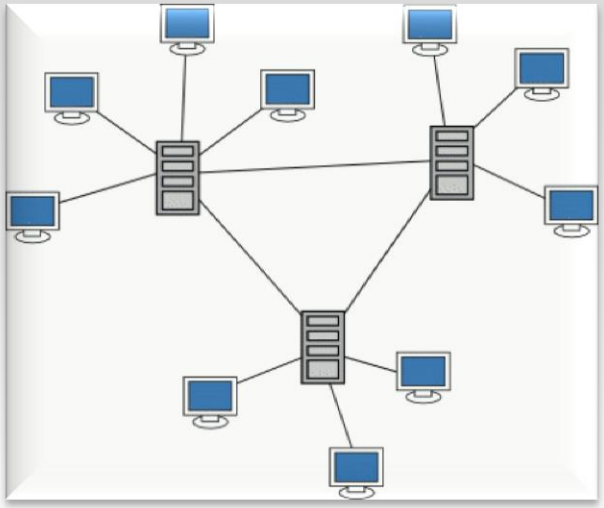
Information Stealing

Industrial Factory

University/Corporate Research Laboratories/AV Companies

Cyber Attack

Disruption of Communication



Key Internet Nodes/ISPs

Key Electrical Power Grids

Satellite Communication Network

Military Conflict

Nation vs. Nation

Non Nation vs Nation

Missile Radar/SAM Sites/Warning Systems

Mobile C2 and Attack/Defense A/C

Coastal Defenses

Your Role

- Education must be the long term goal
- Communicate to leadership in their terms
- Use your Sphere of Influence

A soldier will fight long and hard for a bit of colored ribbon.

Operation Negre Angelis

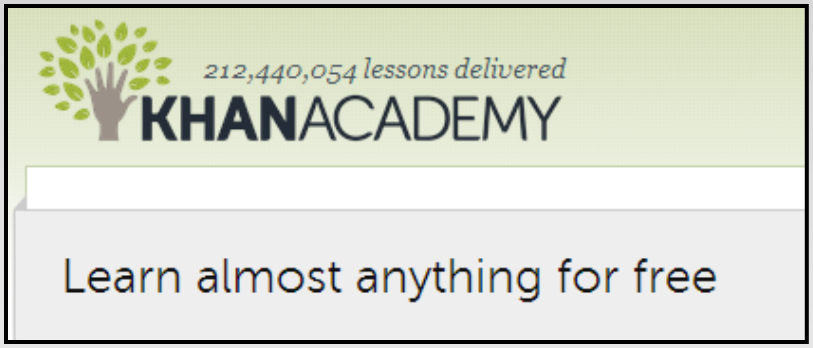
Home | About | Connect the Dots | CryptoAnalysis | Destructive Research | LethalForensicator | Snowflake Collection | Vault

Jester

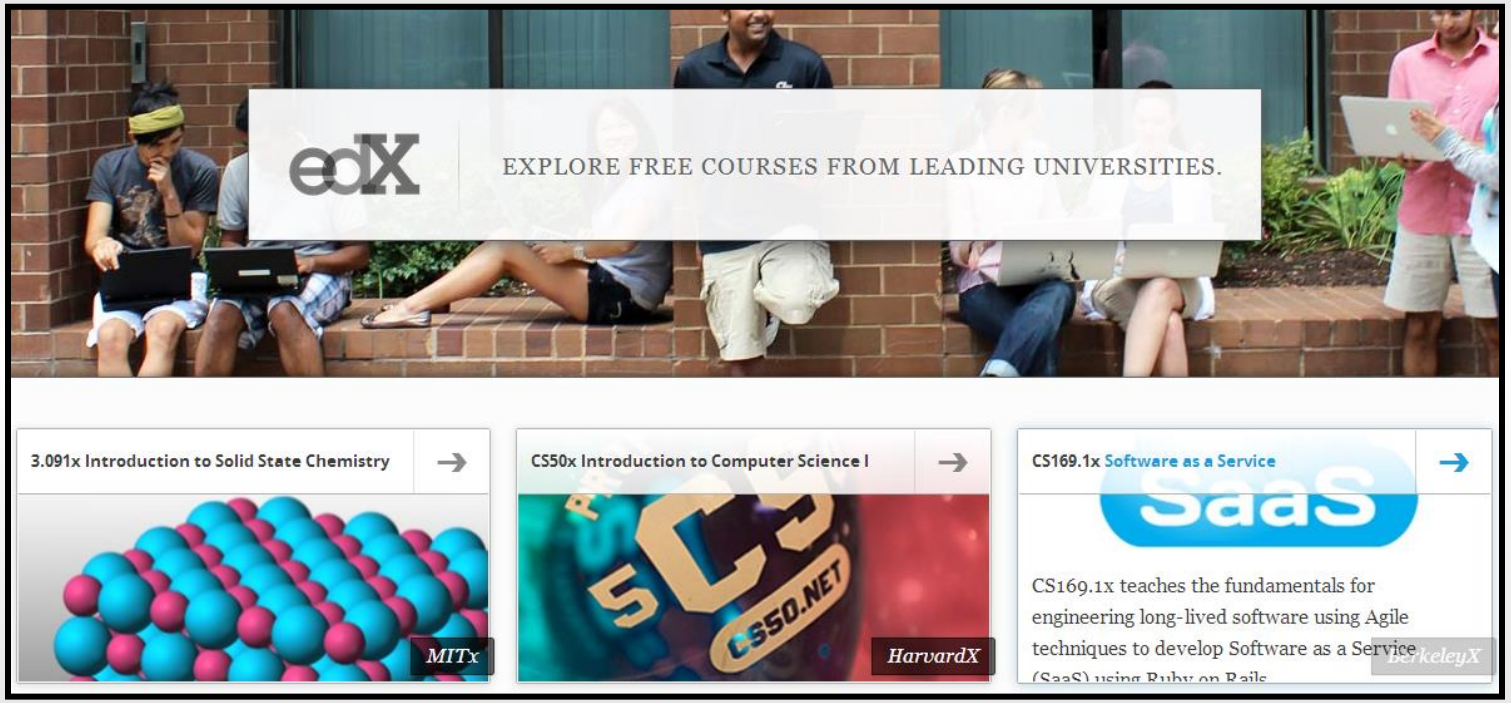
@th3j35t3r Everywhere

Hacktivist for good. Obstructing the lines of communication for terrorists, sympathizers, fixers, facilitators, oppressive regimes and other general bad guys.

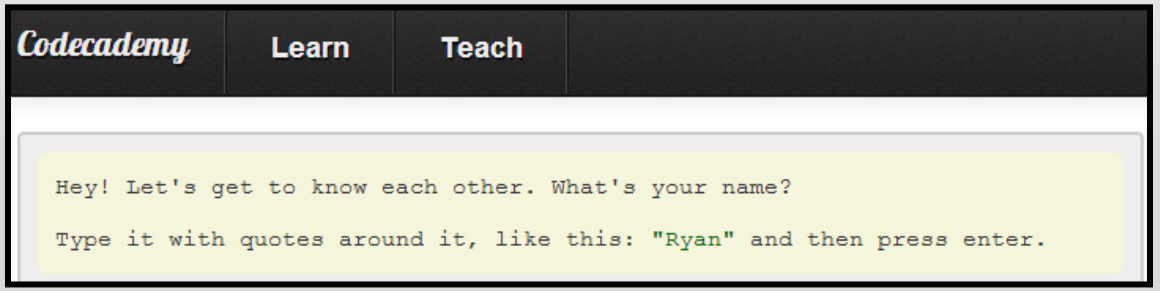
http://th3j35t3r.wordpress.com


212,440,054 lessons delivered
KHANACADEMY
Learn almost anything for free


HackThisSite IRC Forums Radio Store Like Us Follow Us
HACKTHISSITE.ORG


edX
EXPLORE FREE COURSES FROM LEADING UNIVERSITIES.
3.091x Introduction to Solid State Chemistry
MITx
CS50x Introduction to Computer Science I
CS50.NET
HarvardX
CS169.1x Software as a Service
SaaS
CS169.1x teaches the fundamentals for engineering long-lived software using Agile techniques to develop Software as a Service
BerkeleyX


PYTHON
CHALLENGE


Codecademy
Learn
Teach
Hey! Let's get to know each other. What's your name?
Type it with quotes around it, like this: "Ryan" and then press enter.

- hackINT (Hacking Intelligence)
- Started April 2012 (official 501(3)© Jan 2013)
  - "Cyber professional shortage" but why?
  - Inspired by Salman Khan, Johnny Long, and others
- ~200 DoD students trained in Germany
- Free online classes (Youtube + Website) coming in Summer/Fall 2013
  - Focuses on: Forensics, Intelligence, Hacking, Defense

Conclusion

- Apply lessons learned from airpower
  - Military plays a role learn from its past
- Need to prepare during the Interim Years
  - Not going to get easier
- Security AND Privacy
- Must work together
  - govt/civ/hackers/etc
  - Making the domain darker is not a victory
- Education is a major long term strategy

Questions?

There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success than to take the lead in the introduction of a new order of things.

— Machiavelli

My latest papers:
"The History of Stuxnet: Key Takeaways for Cyber Decision Makers"
Found at: www.afcea.org/committees/cyber/documents/TheHistoryofStuxnet.pdf

"The Interim Years of Cyberspace"
Found at: http://www.airpower.au.af.mil/digital/pdf/articles/Jan-Feb-2013/F-Lee.pdf