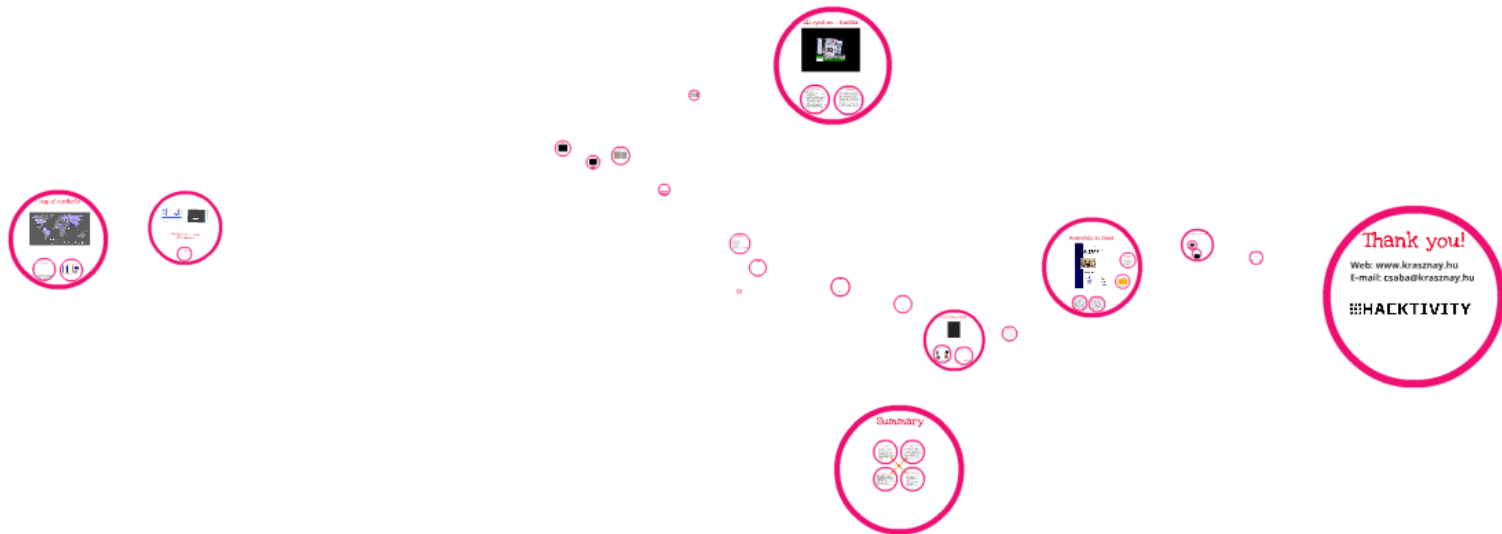


# Cyber soldiers in the world

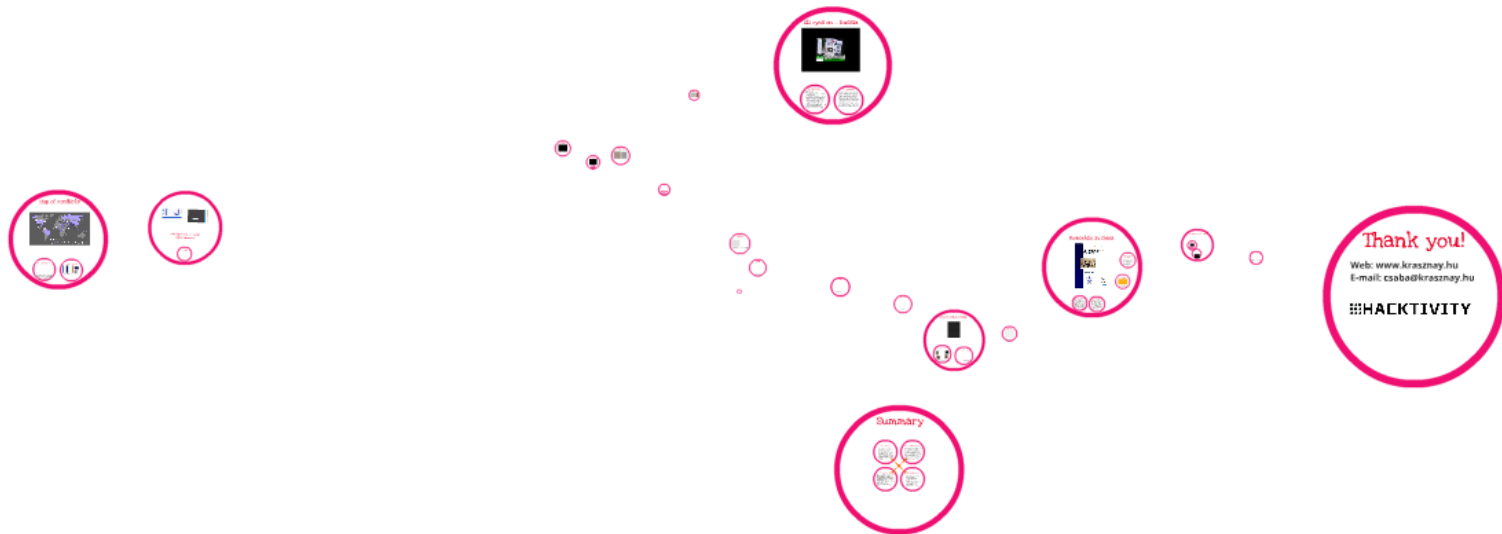
## How to become a military hacker?



Csaba Krasznay, PhD

# Cyber soldiers in the world

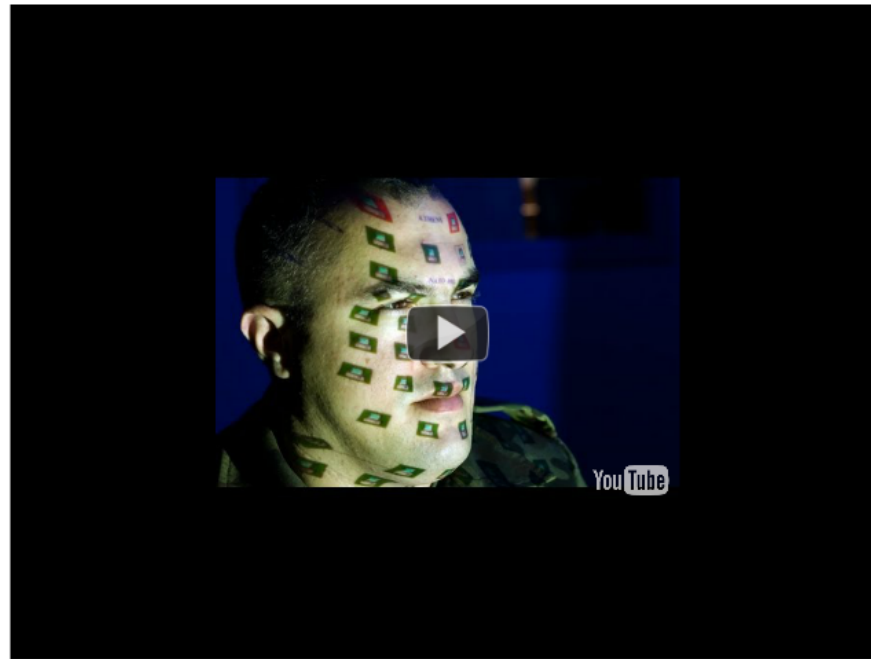
## How to become a military hacker?



Csaba Kraszmay, PhD



# Message from the experts



## The Hacker Ethic

### Mistrust authority—promote decentralization

The best way to promote the free exchange of information is to have an open system that presents no boundaries between a hacker and a piece of information or an item of equipment that he needs in his quest for knowledge, improvement, and time on-line. Hackers believe that bureaucracies, whether corporate, government, or university, are flawed systems.



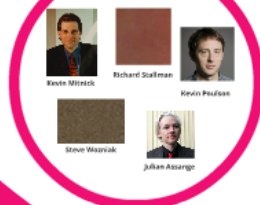


# The Hacker Ethic

**Mistrust authority—promote decentralization**

**The best way to promote the free exchange of information is to have an open system that presents no boundaries between a hacker and a piece of information or an item of equipment that he needs in his quest for knowledge, improvement, and time on-line. Hackers believe that bureaucracies, whether corporate, government, or university, are flawed systems.**

Some heroes of the hacker history



... and the present



# Some heroes of the hacker history



**Kevin Mitnick**



**Richard Stallman**



**Kevin Poulson**



**Steve Wozniak**



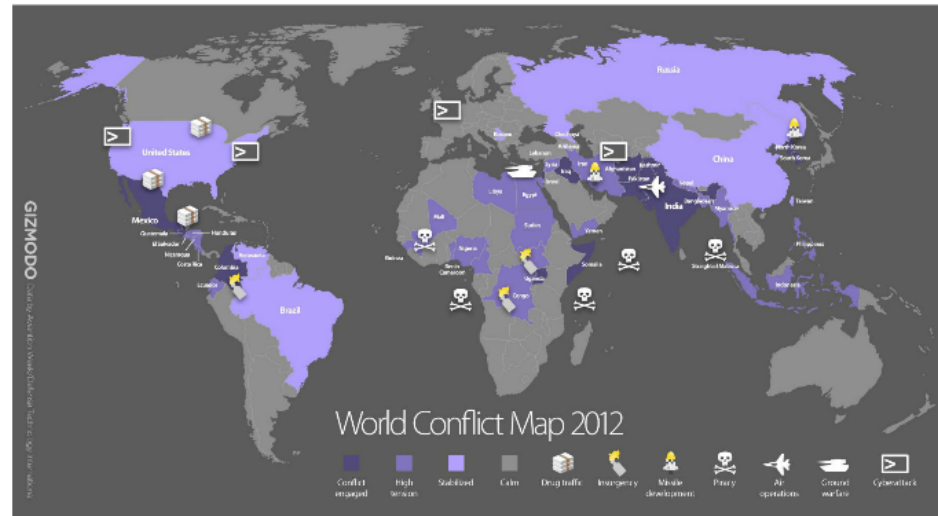
**Julian Assange**

... and the present





# Map of conflicts



## Need for hackers

### Government backs up hackers



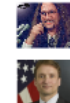
The NSA is hiring about 1,500 people in the fiscal year which ends in September 30 and another 1,500 next year, most of them cyber warriors. (...) It also engages in cyber-spying and other offensive operations, something it rarely, if ever, discusses publicly.

Source: <http://www.millicyber.com>

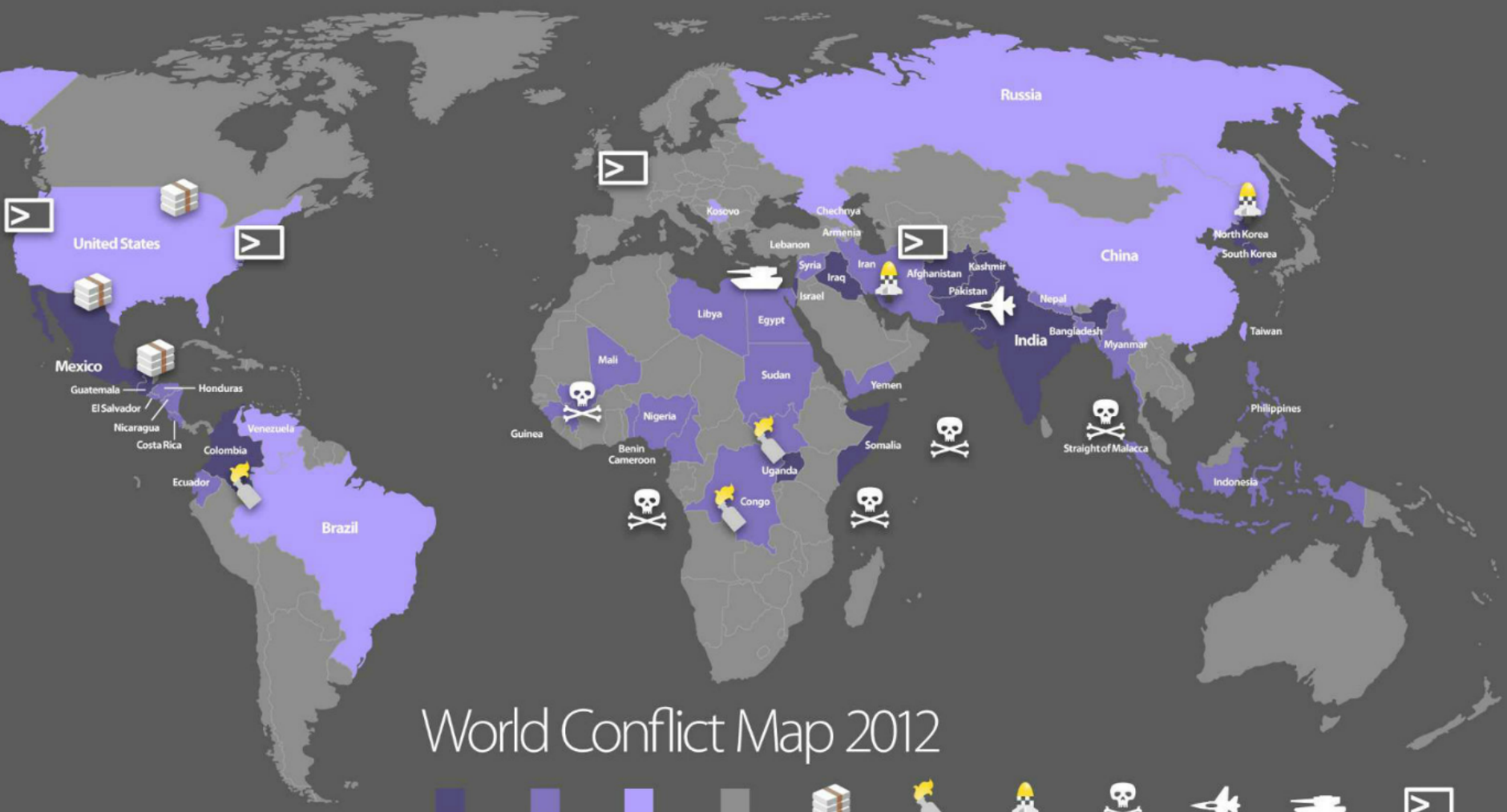
## ... and the solution

### Obama's cyber program for a hacker in a suit

The new cyber program will focus on...  
The new cyber program will focus on...  
The new cyber program will focus on...



Source: <http://www.millicyber.com>




# World Conflict Map 2012

- Conflict engaged
- High tension
- Stabilized
- Calm
- Drug traffic
- Insurgency
- Missile development
- Piracy
- Air operations
- Ground warfare
- Cyberattack

# Need for hackers

## Government hankers for hackers

Ajánlom  225 ember kedveli. Legyél te az első az ismerőseid közül



By Tabassum Zakaria  
WASHINGTON | Tue Aug 2, 2011 10:57am EDT

(Reuters) - The National Security Agency has a challenge for hackers who think they're hot stuff: prove it by working on the "hardest problems on Earth."

**The NSA is hiring about 1,500 people in the fiscal year which ends September 30 and another 1,500 next year, most of them cyber experts. (...) It also engages in cyber-spying and other offensive operations, something it rarely, if ever, discusses publicly.**

Source: <http://www.reuters.com/article/2011/08/02/idUSN1E7701KK20110802>



# Government hankers for hackers

👍 Ajánlom

👤 225 ember kedveli. Legyél te az első az ismerőseid közül!




By Tabassum Zakaria

WASHINGTON | Tue Aug 2, 2011 10:57am EDT

(Reuters) - The National Security Agency has a challenge for hackers who think they're hot stuff: prove it by working on the "hardest problems on Earth."

# Pentagon cyber program to fund hacker innovation

 Ajánlom


 25 ember kedveli. Legyél te az első az ismerőseid közül

By Tabassum Zakaria

LAS VEGAS | Thu Aug 4, 2011 6:20pm EDT

(Reuters) - A hacker-turned-defense official, decrying the government's slowness to change, rolled out a new program on Thursday that would enable the Pentagon to more quickly fund hackers to tackle its tough cybersecurity challenges.

Peiter Zatkó, a hacker known as Mudge who is now at the Defense Advanced Research Projects Agency, said he joined the Pentagon's research arm to try and build bridges between the government's

 Prezi security needs and hackers working on innovative projects

# ... and the solution

## Pentagon cyber program to fund hacker innovation

Ajánlom 25 ember kedveli. Legyél te az első az ismerőseid közül

By Tabassum Zakaria  
LAS VEGAS | Thu Aug 4, 2011 6:20pm EDT

(Reuters) - A hacker-turned-defense official, decrying the government's slowness to change, rolled out a new program on Thursday that would enable the Pentagon to more quickly fund hackers to tackle its tough cybersecurity challenges.

Peiter Zatkó, a hacker known as Mudge who is now at the Defense Advanced Research Projects Agency, said he joined the Pentagon's research arm to try and build bridges between the government's cybersecurity needs and hackers working on innovative projects.



Source: <http://www.reuters.com/article/2011/08/04/us-usa-security-cyber-idUSTRE7737BH20110804>

Booz | Allen | Hamilton

SEARCH RESULTS

SEARCH RESULTS FOR: **SECURITY**

SEARCH RESULTS

Job Title	Location	Job ID
Senior Security Analyst	Washington, DC	123456
Security Operations Center Analyst	Reston, VA	123457
Information Security Specialist	Herndon, VA	123458
Network Security Engineer	Reston, VA	123459
Security Compliance Analyst	Reston, VA	123460
Security Incident Response Analyst	Reston, VA	123461
Security Architecture Analyst	Reston, VA	123462
Security Policy Analyst	Reston, VA	123463
Security Awareness Trainer	Reston, VA	123464
Security Risk Assessment Analyst	Reston, VA	123465
Security Vulnerability Assessment Analyst	Reston, VA	123466
Security Incident Response Analyst	Reston, VA	123467
Security Incident Response Analyst	Reston, VA	123468
Security Incident Response Analyst	Reston, VA	123469
Security Incident Response Analyst	Reston, VA	123470
Security Incident Response Analyst	Reston, VA	123471
Security Incident Response Analyst	Reston, VA	123472
Security Incident Response Analyst	Reston, VA	123473
Security Incident Response Analyst	Reston, VA	123474
Security Incident Response Analyst	Reston, VA	123475
Security Incident Response Analyst	Reston, VA	123476
Security Incident Response Analyst	Reston, VA	123477
Security Incident Response Analyst	Reston, VA	123478
Security Incident Response Analyst	Reston, VA	123479
Security Incident Response Analyst	Reston, VA	123480
Security Incident Response Analyst	Reston, VA	123481
Security Incident Response Analyst	Reston, VA	123482
Security Incident Response Analyst	Reston, VA	123483
Security Incident Response Analyst	Reston, VA	123484
Security Incident Response Analyst	Reston, VA	123485
Security Incident Response Analyst	Reston, VA	123486
Security Incident Response Analyst	Reston, VA	123487
Security Incident Response Analyst	Reston, VA	123488
Security Incident Response Analyst	Reston, VA	123489
Security Incident Response Analyst	Reston, VA	123490
Security Incident Response Analyst	Reston, VA	123491
Security Incident Response Analyst	Reston, VA	123492
Security Incident Response Analyst	Reston, VA	123493
Security Incident Response Analyst	Reston, VA	123494
Security Incident Response Analyst	Reston, VA	123495
Security Incident Response Analyst	Reston, VA	123496
Security Incident Response Analyst	Reston, VA	123497
Security Incident Response Analyst	Reston, VA	123498
Security Incident Response Analyst	Reston, VA	123499
Security Incident Response Analyst	Reston, VA	123500

U.S. ARMY CYBER COMMAND

# ARMY CYBER

Home | About Us | News | Events | Search | Job | Contact Us | Privacy

## Cyber Warriors Needed

Are you a skilled, motivated individual with a passion for technology and a desire to serve the nation? The U.S. Army Cyber Command is seeking highly qualified individuals to join our team. We are currently looking for individuals with the following skills and experience:

- Strong background in computer science, engineering, or related field.
- Experience in network security, cryptography, or information systems.
- Excellent communication and teamwork skills.
- Ability to work in a fast-paced, high-pressure environment.

For more information, visit our website at [www.army.mil/cyber](http://www.army.mil/cyber).

Jobs for hack ... I mean  
Cyberwarriors



[Home](#) > [US Cybercom Jobs at Booz Allen](#)

Search results for "US CYBERCOM jobs"

Search by Keyword



Save Search as RSS Feed

Email jobs to me ▾ when they match this search.

Results 1 – 25 of 1168 [«](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [»](#)

Title	Location	Date
<input type="text" value="Filter: title"/>	<input type="text" value="Filter: city"/>	<input type="text" value="Filter: date"/>
<input type="button" value="Go"/> <a href="#">Reset</a>		
<a href="#">Linguistics Analyst Job</a>	Arlington, VA, US	Aug 1, 2013
<a href="#">University Students - Intelligence Analyst Job</a>	McLean, VA, US	Aug 16, 2013
<a href="#">Tactical Applications Engineer Job</a>	Aberdeen, MD, US	Aug 1, 2013
<a href="#">Export Compliance Specialist, Senior Job</a>	McLean, VA, US	Aug 27, 2013
<a href="#">Business Continuity Planner Job</a>	St. Louis, MO, US	Aug 13, 2013
<a href="#">Software Reverse Engineer Job</a>	Herndon, VA, US	Aug 21, 2013
<a href="#">Physical Security Specialist Job</a>	New Orleans, LA, US	Aug 16, 2013
<a href="#">Weapons Systems Training Analyst Job</a>	Norfolk, VA, US	Aug 16, 2013
<a href="#">Weapons Systems Training School Tactics Instructor Job</a>	Norfolk VA US	Aug 16, 2013

- CAREERS HOME
- EXPLORE BOOZ ALLEN
- LIFE AT BOOZ ALLEN
- MEET OUR PEOPLE
- GET STARTED
- FIND YOUR JOB
- TOP JOBS

Join our Talent Community

- Watch for Future Jobs
- Get Invited to Future Events

Already a member? [Sign in here](#)





U.S. ARMY CYBER COMMAND

ARMY CYBER

[Home](#)

[Organization](#) ▾

[News](#) ▾

[History](#)

[Support](#) ▾

[Jobs](#) ▾

[Vendor Info](#)

[SiteMap](#)

## Cyber Warriors Needed

We want to recruit, develop and retain the 21st century cyber warrior. Passionate-Creative – and determined to find solutions to the challenges we face in the 21st century.

Army Civilian Service provides worldwide opportunities.

Army Civilians – more than 330,000 men and women working in every profession imaginable - are not active duty military, but serve as an integral part of the Army team to support the defense of our nation. We are a global family that encourages excellence, professional development and balance.

Army Civilian Service positions generally fall within broad career groups that directly support the overall mission of the United States Army. A career program - like Mathematical Sciences - has a very specialized mission that is supported by professionals with a highly specific skill set. Other careers - like Accounting and Budget - have a much broader mission and hire professionals with a wide range of skills.

If you are determined to find solutions to the challenges we face in the 21st Century, match your skills/education to our careers and apply now.



**G1** - The U.S. Army Cyber Command Staff function is responsible for personnel matters within our command.

# Job description

## Reverse Engineer/Ethical Hacker Job

Apply now »

Date: Sep 16, 2013  
Location: Dayton, OH, US

Reverse Engineer/Ethical Hacker-01142452

### Description

#### Key Role:

Support the government client by performing analysis and reverse engineering of hardware, firmware, embedded systems, RF signals, network devices, and protocols. Perform security testing and vulnerability analysis of data communications and telecommunication networks. Leverage a good understanding of network data flow and protocol stacks. Work with a diverse team of experts, performing penetration testing to find exploitable vulnerabilities in hardware, firmware, software, and communication protocols.

#### Qualifications

**Basic Qualifications:**-2 years of experience with software and hardware reverse engineering-2 years of experience with network traffic collection and analysis tools-2 years of experience with performing protocol analysis-2 years of experience with CNO, CIA, CNE, and CND-2 years of experience with scripting languages, including Perl and Python-Experience with Linux-TS/SCI clearance -BA or BS degree in EE or Computer Engineering

**Additional Qualifications:**-Experience as an ethical hacker

#### Clearance:

Applicants selected will be subject to a security investigation and may need to meet eligibility requirements for access to classified information. TS/SCI clearance is required.

Integrating the full range of consulting capabilities, Booz Allen is the one firm that helps clients solve their toughest problems, working by their side to help them achieve their missions. Booz Allen is committed to delivering results that endure.

We are proud of our diverse environment. EOE, M/F/D/V.

Job: Information Technology  
Primary Location: United States-Ohio-Dayton  
Travel: Yes, 5 % of the Time

**Nearest Major Market:** Dayton  
**Nearest Secondary Market:** Cincinnati  
**Job Segments:** Telecom, Telecommunications, Consulting, Engineer, Firmware, Technology, Engineering

# Reverse Engineer/Ethical Hacker Job

Apply now »

**Date:** Sep 16, 2013

**Location:** Dayton, OH, US

Reverse Engineer/Ethical Hacker-01142452

## Description

### Key Role:

Support the government client by performing analysis and reverse engineering of hardware, firmware, embedded systems, RF signals, network devices, and protocols. Perform security testing and vulnerability analysis of data communications and telecommunication networks. Leverage a good understanding of network data flow and protocol stacks. Work with a diverse team of experts, performing penetration testing to find exploitable vulnerabilities in hardware, firmware, software, and communication protocols.

### Qualifications

**Basic Qualifications:**-2 years of experience with software and hardware reverse engineering-2 years of experience with network traffic collection and analysis tools-2 years of experience with performing protocol analysis-2 years of experience with CNO, CNA, CNE, and CND-2 years of experience with scripting languages, including Perl and Python-Experience with Linux-TS/SCI clearance  
-BA or BS degree in EE or Computer Engineering

**Additional Qualifications:**-Experience as an ethical hacker

### Clearance:

Applicants selected will be subject to a security investigation and may need to meet eligibility requirements for access to classified information; TS/SCI clearance is required.

Integrating the full range of consulting capabilities, Booz Allen is the one firm that helps clients solve their toughest problems, working by their side to help them achieve their missions. Booz Allen is committed to delivering results that endure.

We are proud of our diverse environment, EOE, M/F/D/V.

**Job:** Information Technology

**Primary Location:** United States-Ohio-Dayton

**Travel:** Yes, 5 % of the Time

**Nearest Major Market:** Dayton

**Nearest Secondary Market:** Cincinnati

**Job Segments:** Telecom, Telecommunications, Consulting, Engineer, Firmware, Technology, Engineering



# Meanwhile in China

## Occupying the Information High Ground:

### Chinese Capabilities for Computer Network Operations and Cyber Espionage



Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp



Bryan Krekel  
Patton Adams  
George Bakos

March 7, 2012

**NORTHROP GRUMMAN**

### And what about the subculture?

"Hackers are pervasive, their regimes traceable. There are hacker magazines, hacker clubs and hacker video series. A 2005 Shanghai Academy of Social Sciences survey reports hackers and their allies, with nearly 80 percent of cyber-styled students saying they "adore" China's hackers. One Weblog they want to be on: "This culture lives on a viral, Internet-driven marketplace." Source: IS&IT www.papers.com/tech/its/its/2005/04/hackers/0504060008

### Small remark



### University capabilities

**Academy of Military Sciences, Beijing**  
- The Academy of Military Sciences (AMS) is a leading research and development organization in China, focusing on military technology and information systems. AMS has conducted a wide range of research in computer network operations, information management, and intelligence analysis.  
- AMS has developed a variety of military information systems, including command and control systems, intelligence gathering systems, and communication systems.  
- AMS has also conducted research in computer network operations, including the development of military information systems and the use of computer network operations in military operations.  
- AMS has a long history of research and development in military information systems and has been instrumental in the development of many of the military information systems used by the Chinese military today.

### University capabilities

**National University of Defense Technology, Changsha**  
- National University of Defense Technology (NUDT) is a leading research and development organization in China, focusing on military research and development. The organization's research is primarily in the areas of computer network operations, information management, and intelligence analysis.  
- NUDT has developed a variety of military information systems, including command and control systems, intelligence gathering systems, and communication systems.  
- NUDT has also conducted research in computer network operations, including the development of military information systems and the use of computer network operations in military operations.  
- NUDT has a long history of research and development in military information systems and has been instrumental in the development of many of the military information systems used by the Chinese military today.

# Occupying the Information High Ground:

## *Chinese Capabilities for Computer Network Operations and Cyber Espionage*



Prepared for the U.S.-China Economic and Security Review Commission  
by Northrop Grumman Corp



Bryan Krekel  
Patton Adams  
George Bakos

March 7, 2012

**NORTHROP GRUMMAN**



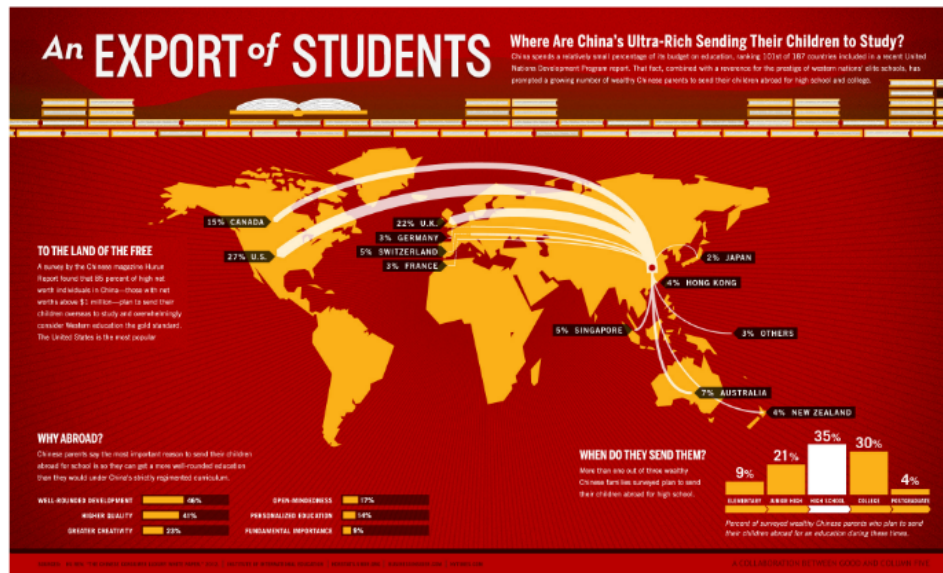
# University capabilities

- **Academy of Military Sciences, Beijing:**
  - PRC military's main body for military science research and strategy and doctrine development. Recent AMS research studies relevant to information warfare focus on the operational use of computer network exploitation, U.S. network-centric warfare models, and foreign military information management structures.
- **National Defense University, Beijing:**
  - Trains the nation's military command leaders. Recent NDU research studies relevant to information warfare focus on foreign military informatization and information warfare approaches.
- **Wuhan Communications Command Academy, Wuhan:**
  - Trains Third Department mid-level communications command and automated management personnel in information warfare and military communications systems and develops operational doctrine for information operations. Recent scholarship at CCA relevant to information warfare includes studies of Internet routing scalability, wireless Internet use in military environments, data mining techniques, distributed denial of service attacks, and U.S. network-centric warfare planning.

# University capabilities

- **National University of Defense Technology, Changsha:**
  - A technology-oriented university heavily involved in military research and development. The development center for China's Tianhe-1A supercomputer, lists among its key research areas electronic and information warfare target recognition in addition to biometrics, nanotechnology, quantum computing, and non-linear mathematics. NUDT faculty include professor Fang Binxing, often called the "Father of the Great Firewall."
- **Information Engineering University, Zhengzhou**
  - The military university with the most comprehensive involvement in information warfare and computer network operations training, planning, and possibly also execution. Published PLAIEU-sponsored research includes studies on worm propagation, network attack evaluation, kernel-mode rootkits, data hiding, malware behavior detection, and "emergency public opinion control."

# Small remark



Source: <http://geniusrecruiter.com/2012/07/06/why-chinese-students-are-going-abroad/>



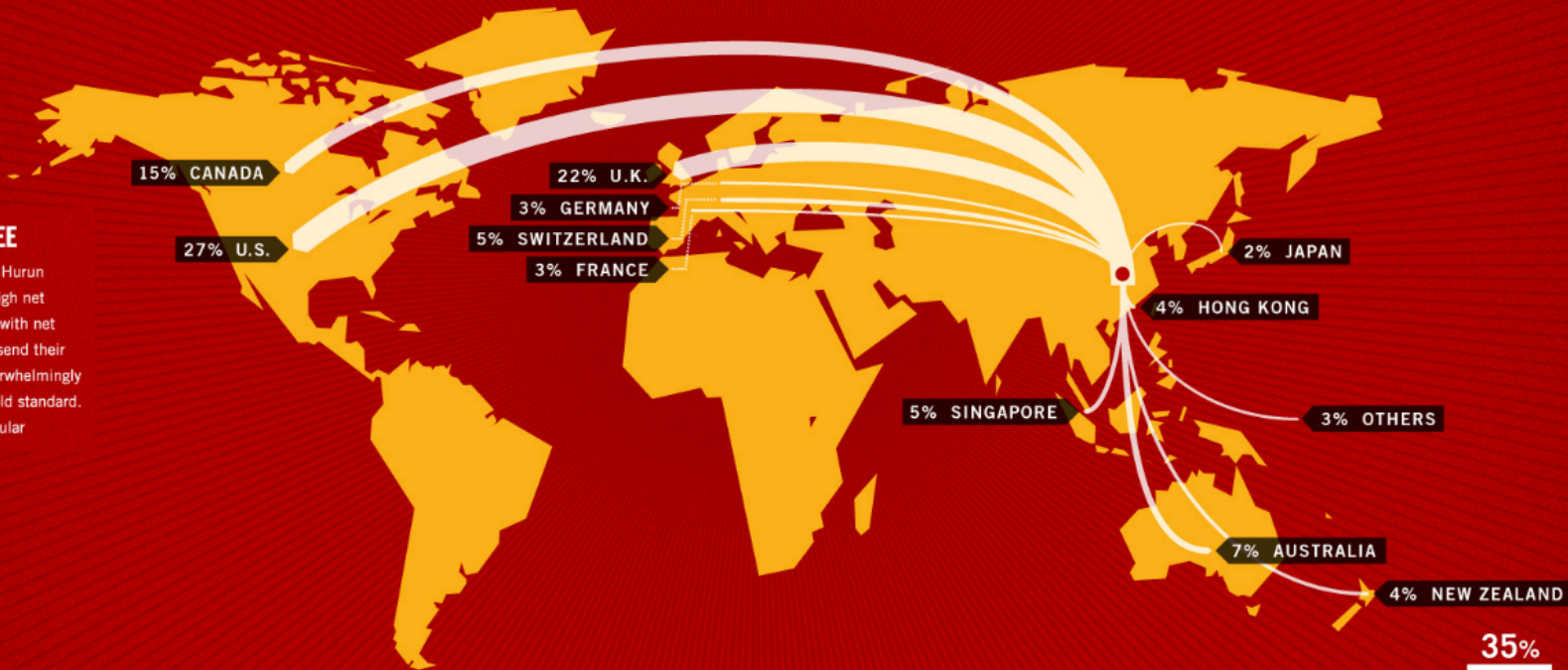
# An EXPORT of STUDENTS

## Where Are China's Ultra-Rich Sending Their Children to Study?

China spends a relatively small percentage of its budget on education, ranking 101st of 187 countries included in a recent United Nations Development Program report. That fact, combined with a reverence for the prestige of western nations' elite schools, has prompted a growing number of wealthy Chinese parents to send their children abroad for high school and college.

### TO THE LAND OF THE FREE

A survey by the Chinese magazine Hurun Report found that 85 percent of high net worth individuals in China—those with net worths above \$1 million—plan to send their children overseas to study and overwhelmingly consider Western education the gold standard. The United States is the most popular



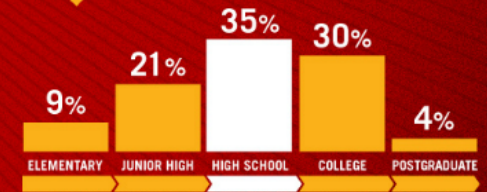
### WHY ABROAD?

Chinese parents say the most important reason to send their children abroad for school is so they can get a more well-rounded education than they would under China's strictly regimented curriculum.



### WHEN DO THEY SEND THEM?

More than one out of three wealthy Chinese families surveyed plan to send their children abroad for high school.



Percent of surveyed wealthy Chinese parents who plan to send their children abroad for an education during these times.

# And what about the subculture?

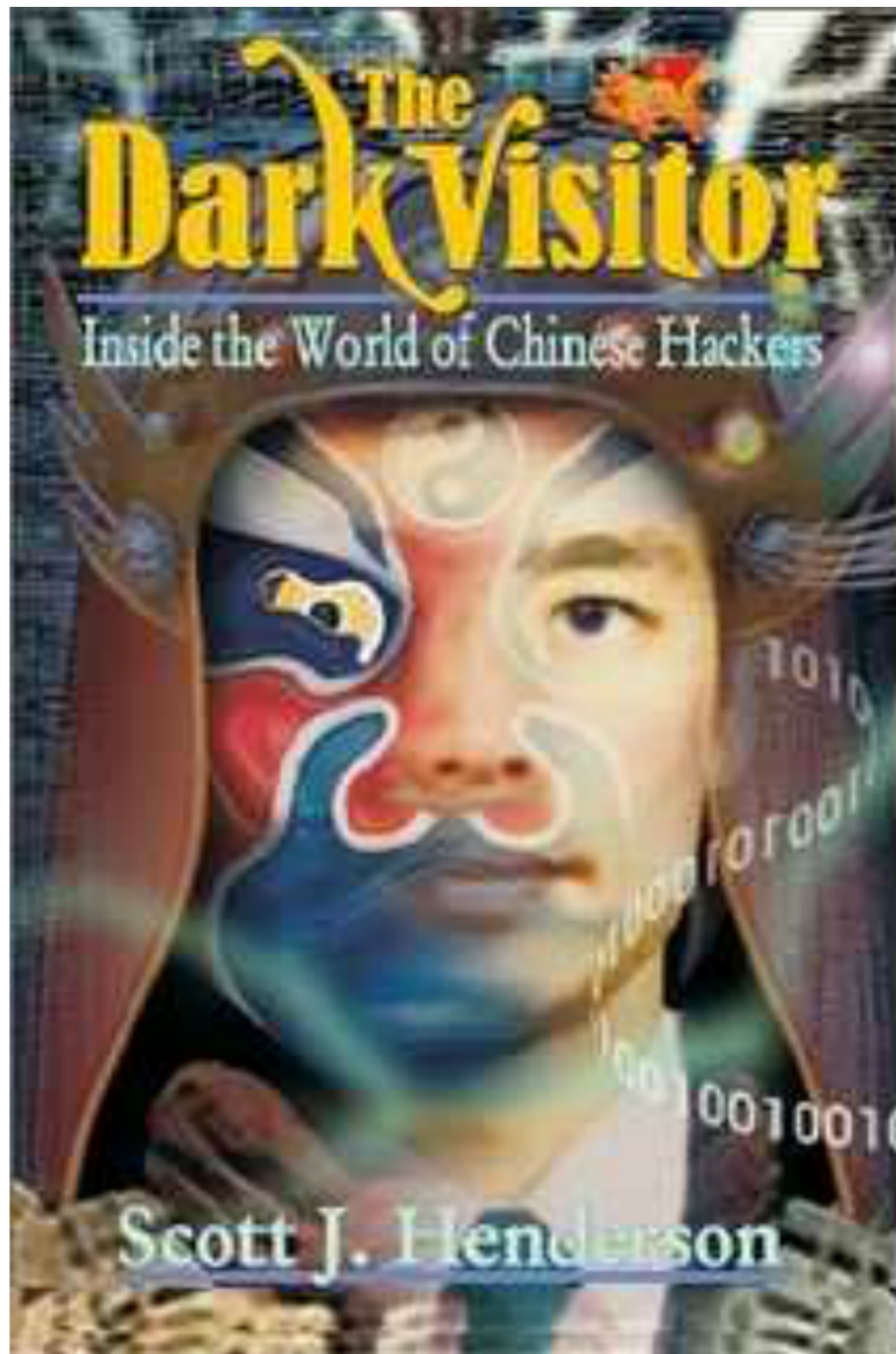
"Hackers are pervasive, their imprint inescapable. There are hacker magazines, hacker clubs and hacker online serials. A 2005 Shanghai Academy of Social Sciences survey equates hackers and rock stars, with nearly 43 percent of elementary-school students saying they "adore" China's hackers. One third say they want to be one. This culture thrives on a viral, Internet-driven nationalism." Source: <http://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome>





# The Dark Visitor

Inside the World of Chinese Hackers



Scott J. Henderson



# The two Koreas - the best students

## North Korea



## South Korea



# South Korea

## US, South Korea join forces to prevent cyberattacks by North Korea

By [Jennifer Chang](#), IDC News Service/Seoul Apr 3, 2013 1:25 PM

Recent massive cyberattacks that paralyzed computer networks at several South Korean banks and broadcasters, strongly suspected to have been launched by North Korean hackers, have prompted Washington and Seoul to come up with tough new countermeasures to stop Pyongyang from waging information warfare in the future.

"The U.S. and South Korean militaries will cooperate to develop diverse deterrence scenarios against hacking attacks and increase anti cyberwarfare forces to over 1,000 to better deal with emerging threats from countries like North Korea," said Kwon Khyoon, a spokesman at South Korea's Ministry of National Defense.

Details of this new counterstrategy cannot be revealed now for security reasons, Kwon said. But the plan is to flesh out the tactics by July, and test and refine them in cooperation with the U.S. military.

Source: [The Wall Street Journal](#)

## Seoul Puts a Price on Cyberdefense

By [Kurt Eichen](#), [The Wall Street Journal](#)

Looking for help with its cyberdefense, South Korea is trying to attract foreign investors and firms.

The defense ministry and the National Intelligence Service are jointly sponsoring a cyber-security competition, meant to help to screen and train talented cybersecurity experts nationwide to gain self-sufficiency. The ministry is making the money and doing the work, though it has received \$400 million from the U.S. to help with the program. The ministry has qualified for the first round, and the second round is set for June 26 and 27.

The ministry is also looking for private firms to help with its cyberdefense. The ministry has a budget of \$1 billion for the program. Cybersecurity is a major focus of South Korea's defense and intelligence strategy. The ministry is also looking for private firms to help with its cyberdefense. The ministry has a budget of \$1 billion for the program. Cybersecurity is a major focus of South Korea's defense and intelligence strategy. The ministry is also looking for private firms to help with its cyberdefense. The ministry has a budget of \$1 billion for the program. Cybersecurity is a major focus of South Korea's defense and intelligence strategy.





# US, South Korea join forces to prevent cyberattacks by North Korea

By [Jennifer Chang](#), IDG News Service\Seoul

Apr 3, 2013 1:25 PM



Recent massive cyberattacks that paralyzed computer networks at several South Korean banks and broadcasters, strongly suspected to have been launched by North Korean hackers, have prompted Washington and Seoul to come up with tough new countermeasures to stop Pyongyang from waging information warfare in the future.

“The U.S. and South Korean militaries will cooperate to develop diverse deterrence scenarios against hacking attacks and increase anti-cyberwarfare forces to over 1,000 to better deal with emerging threats from countries like North Korea,” said Kwon Kihyeon, a spokesman at South Korea’s Ministry of National Defense.

Details of this new counterstrategy cannot be revealed now for security reasons, Kwon said. But the plan is to finish drafting the tactics by July, and test and review them during the next joint U.S.-South Korea military drills, which begin in late August, before they’re

# Seoul Puts a Price on Cyberdefense

Article

Comments (1)



Email



Print



By Kwanwoo Jun

Looking for help with its cyberdefenses, South Korea is trying a straightforward approach: cash prizes.

The defense ministry and the National Intelligence Service are jointly sponsoring a computer-security competition, meant to help “to locate and train talented cybersecurity experts nationwide to cope with increasing cybersecurity threats,” as the ministry put it in a statement Monday. It announced that 98 of the 1,100 competitors who entered the contest earlier this month had qualified for the final round, set for Korea Military Academy Sept. 28 and 29.



Reuters

South Korea seeks the equivalent to defend its cyberspace.

The winners—six individuals and six teams—will share total prize money of 80 million won (\$74,000).

Cyberattacks crippled a number of South Korean government and news-media websites in June, three months after hostile hackers caused the crash of thousands of computers South Korean TV stations and banks. South Korea's government blamed both attacks—and similar ones in 2009, 2011 and 2012—on

North Korea, which Seoul says has thousands of hackers operating on its behalf. Pyongyang denies engaging in any cyberattacks.

A month after the June attacks, the Seoul government said it would boost its cyberdefense expertise by training 5,000 new cybersecurity experts by 2017.



# North Korea

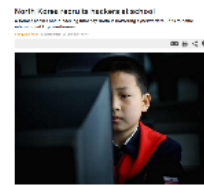


## (Imaginary?) Cyber forces

- Unit 110 - Also known as the "Technology Reconnaissance Team" was most likely responsible for the July 2009 DDoS attacks against the US and South Korea.
- Unit 35 - Also known as the "Central Party's Investigations Department" is the smallest group but is responsible for both internal defense and offensive capabilities.
- Unit 204 - Also known as the "Enemy Secret Department Cyber Psychological Warfare Unit" has about 100 hackers.
- Unit 121 - Also known as the "Korean People's Army (KPA) Joint Chiefs Cyber Warfare Unit" has over 600 hackers and would be responsible for disabling South Korea's C3 functions (Command, Control and Communications) in case of armed conflict.

Source: <http://cyberarms.wordpress.com/2012/02/22/north-koreas-cyber-war-forces/>

## Links to schools - and abroad



Source: <http://www.aljazeera.com/ind/english/features/2011/06/201162081543173439.html>

## (Imaginary?) Cyber forces

- Unit 110 – Also known as the “Technology Reconnaissance Team” was most likely responsible for the July 2009 DDoS attacks against the US and South Korea.
- Unit 35 – Also known as the “Central Party’s Investigations Department” is the smallest group but is responsible for both internal defense and offensive capabilities.
- Unit 204 – Also known as the “Enemy Secret Department Cyber Psychological Warfare Unit” has about 100 hackers.
- Unit 121 – Also known as the “Korean People’s Army (KPA) Joint Chiefs Cyber Warfare Unit” has over 600 hackers and would be responsible for disabling South Korea’s C3 functions (Command, Control and Communications) in case of armed conflict.

Source: <http://cyberarms.wordpress.com/2012/02/22/north-koreas-cyber-war-forces/>

# Links to Schools - and abroad

## North Korea recruits hackers at school

A former hacker and a hacking tutor say North is bolstering cyberwarfare units to battle international IT powerhouses.

Sangwon Yoon Last Modified: 29 Jun 2011 19:15



A child becomes computer literate at primary school while North Korea's most prodigious young students are identified and trained in advanced cyberwarfare techniques [GALLO/GETTY]

Source: <http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html>



# Secret weapon of India



## Top hackers of India



## Indian Cyber Army





norman

May 2013

# OPERATION HANGOVER

## Unveiling an Indian Cyberattack Infrastructure

Snorre Fagerland, Morten Kråkvik, and Jonathan Camp  
Norman Shark AS

Ned Moran  
Shadowserver Foundation



Part of a PDF decay from one of the malicious installers (md5 06e80767048f3edefc2dea301924346c).

# Top hackers of India



**Ankit Fadia**



**Sunny Vaghela**



**Pranav Mistry**



**Koushik Dutta**



**Vivek Ramchandran**

Source: [www.widgetgenerators.com/2013/06/top-10-hackers-of-india.html](http://www.widgetgenerators.com/2013/06/top-10-hackers-of-india.html)

# Indian Cyber Army



## NEWS

### U.K., India Sign Cybersecurity Pact



Gary Flood

[See more from Gary](#)

Connect directly with Gary: [Bio](#) | [Contact](#)

Government and law enforcement agencies will collaborate to protect U.K. data held by Indian outsourcing and cloud vendors.

Start The Discussion

15	19	5	8
Like	Tweet	+1	Share

submit

Gary Flood | February 25, 2013 12:55 PM

U.K. Prime Minister David Cameron last week signed a cybersecurity deal with India's Prime Minister Manmohan Singh to reassure Brits about protection of data held by outsourcing or cloud companies in India.

British newspaper [The Telegraph said](#) the pact will: create a joint task force to exchange and share information about identifying and countering threats; help police from the two nations share expertise in cyberforensics and other areas of detection and enforcement; and enable regular cooperation meetings among leaders in cybersecurity research from academic circles and industry.

#### MORE SECURITY INSIGHTS

##### Webcasts

- [Top Business Process](#)

What's particularly interesting is that the agreement-- framed as designed to improve "the protection of personal data and sensitive commercial and government information" -- may herald much greater use of offshoring and outsourcing of U.K. state information and communications technology (ICT) work to India.

Source: <http://www.informationweek.com/security/management/uk-india-sign-cybersecurity-pact/240149357>

# ISrael

## IDF Hackers Test Readiness In Israel for Cyberattacks



A magnifying glass is held in front of a computer screen in this picture illustration taken in Berlin, May 21, 2013. (photo by REUTERS/Pawel Kopczynski)

PRINT FONT SIZE Tweet +1 Recommend 59

By: Harel Eilam Translated from Calcalist (Israel).

[ליגת ההקשרים בעברית](#)

"An army hacker does not sit all by himself with a pizza and a Coke," says Lt. Col. M. and Capt. A., two senior officers serving in the Israeli Defense Forces (IDF) cybersecurity lineup. "We must work together, and we have to practice brainstorming and to allocate tasks. Ultimately, we are running against the clock. These are the qualities we are looking for in our soldiers – teamwork and the ability to think outside the box."

### ABOUT THIS ARTICLE

#### Summary :

IDF cybersecurity soldiers play hackers and defenders to simulate any possible attack against Israel's defense cyberspace.

**Publisher:** Calcalist (Israel)

**Original Title:**

Hackers in Uniform: When the IDF Breaks Into the IDF Computers

**Author:** Harel Eilam

Lt. Col. M., 39, is in charge of the [cyber] defense lineup – or the "blue team," as it is called in IDF jargon. The defense lineup, which is responsible for the maintenance of all monitoring and security systems designed to handle cyber threats, forms a part of the LOTEM unit, which operates under the command of the IDF Information and Communications Technology (ICT) Branch. Capt. A. heads the "red team" in the cybersecurity lineup, whose task is to simulate attacks and make up attempts to



# IDF Hackers Test Readiness In Israel for Cyberattacks



A magnifying glass is held in front of a computer screen in this picture illustration taken in Berlin, May 21, 2013. (photo by REUTERS/Pawel Kopczynski)

PRINT FONT SIZE



Tweet



Recommend

59

By: Harel Eilam Translated from Calcalist (Israel).

[לגרסה המקורית בעברית](#)

“An army hacker does not sit all by himself with a pizza and a Coke,” says Lt. Col. M. and Capt. A., two senior officers serving in the Israeli Defense Forces (IDF) cybersecurity lineup. “We must work together, and we have to practice brainstorming and to allocate tasks. Ultimately, we are running against the clock. These are the qualities we are looking for in our soldiers – teamwork and the ability to think outside the box.”

## ABOUT THIS ARTICLE

### Summary :

IDF cybersecurity soldiers play hackers and defenders to simulate any possible attack against Israel's defense cyberspace.

Publisher: Calcalist (Israel)

### Original Title:

Hackers in Uniform: When the IDF Breaks Into the IDF Computers

Author: Harel Eilam

Lt. Col. M., 39, is in charge of the [cyber] defense lineup – or the “blue team,” as it is called in IDF jargon. The defense lineup, which is responsible for the maintenance of all monitoring and security systems designed to handle cyber threats, forms a part of the LOTEM unit, which operates under the command of the IDF Information and Communications Technology (ICT) Branch. Capt. A. heads the “red team” in the cybersecurity lineup, whose task is to simulate attacks and work up attempts to

# Turkey

TurkHackTeam celebrates Turkey's Victory Day by hacking 350 websites

Posted date: August 31, 2013 In: Hacking News

AdChoices > > Hack Attack > Hacking > IT Security > Hackers



The online Turkish hackavists from Turk Hack Team have hacked and defaced 250 random websites from all over the world in a collective attack to celebrate Turkey's 91st Victory day.

Source: <http://hackread.com/turkhackteam-celebrates-turkeys-victory-day-by-hacking-350-websites/>

## Anti-hackers to fight local int'l e-threats

ISTANBUL - Hürriyet Daily News

**150 engineers have been assigned to Turkey's newly founded Cyber Security Institution to fight 'internal and external cyber attacks.'** Turkey is preparing for major cyber attacks coming from other countries, an official says

Tweetle

Print

Share

More



Erdem Güneş  
erdem.gunes@hds.com.tr



A team of 150 cyber security experts has begun working to protect official Turkish websites and information infrastructure, and an agreement is to be signed between Turkey's Transportation and Communication Ministry and the Scientific and Technological Research Council of Turkey (TÜBİTAK) in the forthcoming weeks, officials from these institutions said.

A Anonymous supporter holds a flag bearing the headless man logo, during a demonstration, in Paris. Turkey to establish a team of 150 experts to protect official websites and information infrastructure. AFP photo

"The agreement is expected to be signed in a few weeks," Turan Özyanık from the press office of the ministry told the Daily News yesterday. Özyanık said TÜBİTAK will provide the

Source: <http://www.hurriyetdailynews.com/anti-hackers-to-fight-local-intl-e-threats.aspx?PageID=238&NID=28403&NewsCatID=338>

## TurkHackTeam celebrates Turkey's Victory Day by hacking 350 websites

Posted date: August 31, 2013 In: Hacking News

AdChoices ▶

▶ [Hack Attack](#)


▶ [Hacking](#)

▶ [It Security](#)

▶ [Hackers](#)



The online Turkish hackavists from **Turk Hack Team** have hacked and defaced 250 random websites from all

 Prezimer the world in a collective attack to celebrate **Turkey's** 91st Victory day.



# Anti-hackers to fight local int'l e-threats

ISTANBUL - Hürriyet Daily News

**150 engineers have been assigned to Turkey's newly founded Cyber Security Institution to fight 'internal and external cyber attacks.' Turkey is preparing for major cyber attacks coming from other countries, an official says**

Tweetle

Pinit

f Share



Erdem Güneş  
erdem.gunes@hdn.com.tr



A team of 150 cyber security experts has begun working to protect official Turkish websites and information infrastructure, and an agreement is to be signed between Turkey's Transportation and Communication Ministry and the Scientific and Technological Research Council of Turkey (TÜBİTAK) in the forthcoming weeks, officials from these institutions said.

A Anonymous supporter holds a flag bearing the headless man logo, during a demonstration, in Paris. Turkey to establish a team of 150 experts to protect official websites and information infrastructure. AFP photo

"The agreement is expected to be signed in a few weeks," Turan Özyanık from the press office of

the ministry told the Daily News yesterday. Özyanık said TÜBİTAK will provide the

# Syria

## FAQs About Hacks: Everything You Need to Know About the Syrian Electronic Army

What is the Syrian Electronic Army? What are they after? Should you be scared? Read on for the answers.

By Brad Chaos  
Wed, August 28, 2013



PC World —



In the past 24 hours, the New York Times went down and Twitter images went wonky, while the Huffington Post dodged a digital bullet. All the chaos comes courtesy of the Syrian Electronic Army, a hacker group in love with Syrian president Bashar al-Assad—and this isn't the first time the cyber boogymen have lashed out at Western targets.

[ [Quiz: Name That Hacker](#) ]

But what's all the hub-bub about? Should you be worried about the Syrian Electronic Army? Is there a chance you and I could get caught in the crossfire, the way Lulzsec leaked so many passwords a few summers back? Read on to learn everything you need to know about the Syrian Electronic Army.

### What is the Syrian Electronic Army?

Nobody knows for sure, but all indications suggest that is a group of pro-al-Assad hackers, rather than an official government group.

The Syrian Electronic Army has been responsible for numerous high-profile hack attacks, including the hijacking of the Twitter accounts across the media spectrum--from venerable outlets like NPR, CBS, and the Associated Press all the way to BBC Weather, The Onion, and E! Online. Yesterday, the group claimed responsibility for the DNS-based troubles fouling the New York Times, Twitter, and the Huffington Post UK.

<http://www.cio.com/article/738876/>

[FAQs About Hacks: Everything You Need to Know About the Syrian Electronic Army](#)



# FAQs About Hacks: Everything You Need to Know About the Syrian Electronic Army

What is the Syrian Electronic Army? What are they after? Should you be scared? Read on for the answers.

By Brad Chacos  
Wed, August 28, 2013



[PC World](#) —



In the past 24 hours, the New York Times went down and Twitter images went wonky, while the Huffington Post dodged a digital bullet. All the chaos comes courtesy of the Syrian Electronic Army, a hacker group in love with Syrian president Bashar al-Assad--and this isn't the first time the cyber boogymen have lashed out at Western targets.

[ [Quiz: Name That Hacker](#) ]

But what's all the hub-bub about? Should you be worried about the Syrian Electronic Army? Is there a chance you and I could get caught in the crossfire, the way Lulzsec leaked so many passwords a few summers back? Read on to learn everything you need to know about the Syrian Electronic Army.

## What is the Syrian Electronic Army?

Nobody knows for sure, but all indications suggest that is a group of pro-al-Assad hackers, rather than an official government group.

The Syrian Electronic Army has been responsible for numerous high-profile hack attacks, including the hijacking of the Twitter accounts across the media spectrum--from venerable outlets like NPR, CBS, and the Associated Press all the way to BBC Weather, The Onion, and E! Online. Yesterday, the group claimed responsibility for the DNS-based troubles fouling the New York Times, Twitter, and the Huffington Post UK.

# Iran

## Iran denies cyber warfare chief was victim of 'assassination' but is investigating 'horrific incident'

- Mojtaba Ahmadi, an official of the elite Islamic Revolutionary Guards, was found with a bullet in his heart
- Ahmadi was found near Karaj, northwest of Tehran, after leaving his home
- Iran's Revolutionary Guards deny media reports of an assassination

By CAROLINE BYRNE

PUBLISHED: 12:23 GMT, 3 October 2013 | UPDATED: 14:45 GMT, 3 October 2013

 Share  Tweet  +1  Share | 14 shares

 21 [View comments](#)

Iran's Revolutionary Guards said they were investigating the death of an officer in a 'horrific incident' but denied media reports it was an assassination.

Mojtaba Ahmadi, an official of the elite Islamic Revolutionary Guard Corps (IRGC), was found shot dead near Karaj, a town northwest of the capital Tehran, the Iranian website Alborz reported earlier this week.

He had left his house on Monday morning and was found a few hours later with a bullet in his heart, the website said.

Source: <http://www.dailymail.co.uk/news/article-2442435/Iranian-cyber-warfare-commander-shot-dead-suspected-assassination.html>

# Iran denies cyber warfare chief was victim of 'assassination' but is investigating 'horrific incident'

- Mojtaba Ahmadi, an official of the elite Islamic Revolutionary Guards, was found with a bullet in his heart
- Ahmadi was found near Karaj, northwest of Tehran, after leaving his home
- Iran's Revolutionary Guards deny media reports of an assassination

By CAROLINE BYRNE

PUBLISHED: 12:23 GMT, 3 October 2013 | UPDATED: 14:45 GMT, 3 October 2013



14 shares

21 View comments

Iran's Revolutionary Guards said they were investigating the death of an officer in a 'horrific incident' but denied media reports it was an assassination.

Mojtaba Ahmadi, an official of the elite Islamic Revolutionary Guard Corps (IRGC), was found shot dead near Karaj, a town northwest of the capital Tehran, the Iranian website Alborz reported earlier this week.

He had left his house on Monday morning and was found a few hours later with a bullet in his

# Pakistan

## About Us

### About Pakistan Cyber Army™



Pakistan Cyber Army is not a hacking or cracking group or anything illegal to be, Pakistan Cyber Army is a symbol of all the Pakistani Security Expert's who wanted to safeguard Pakistan Cyber Space from hacking attack's. As the Information Technology boosted in 21st Century and everyone is attached online with business or pleasure or anything representation while all this like police or army, who protects nation of their desire country. We also feel the need of Pakistan Cyber Army, which is led by patriotic Pakistani student's while other's use to play and have fun in life, we were online securing our Cyber Space from enemies and random attack's.

We mastered it and now we are here to announce that we are no longer blackhat's, there was a time when we used to be but only for our country safeguard and our nation pride. Here at Pakistan Cyber Army you will find the Top Security Specialists of Pakistan serving the nation with their expertise and ideas.

**Source: <http://www.cyberarmy.com.pk/p/about-us.html>**



# About Us

## About Pakistan Cyber Army™



Pakistan Cyber Army is not a hacking or cracking group or anything illegal to be, Pakistan Cyber Army is a symbol of all the Pakistani Security Expert's who wanted to safeguard Pakistan Cyber Space from hacking attack's. As the Information Technology boosted in 21st Century and everyone is attached online with business or pleasure or anything representation while all this like police or army, who protects nation of their desire country. We also feel the need of Pakistan Cyber Army, which is led by Patriotic Pakistani student's while others use to play and have fun in life, we were online securing our Cyber Space from enemies and random attack's.

We mastered it and now we are here to announce that we are no longer blackhat's, there was a time when we used to be but only for our country safeguard and our nation pride. Here at Pakistan Cyber Army you will find the Top Security Specialists of Pakistan serving the nation with their expertise

and idea's.



# Bangladesh



By Lorraine Murphy on July 31, 2013 [Email](#) [Follow](#)

62

Shares

38

Like

24

Tweet

↑  
↓

in

Share

When does a hacker crew beef become a **cyberwar**? The answer is, arguably, "yesterday," as a team of Bangladesh hackers attacked vulnerable websites across Indonesia, taking revenge on Indonesian crews in an international game of chicken.

Members of Bangladeshi team Grey Hat (in this case a crew name as well as a set of professional ethics) successfully defaced or took down several websites, claiming that Indonesian cyber-crews had been attacking their crew website and insulting their country.

The Daily Dot spoke with a source involved, who stressed that the participants are all, as far as he is aware, civilians doing this on their own time and for their own reasons.

Defacements are significantly harder to pull off than simple DDoS attacks, showing a greater level of digital sophistication. According to [statements on Facebook](#), the goal of the Bangladeshi crew's attacks was to demonstrate their superior level of skills relative to the Indonesians. In simple terms, to school them.

Source: <http://www.dailydot.com/news/hacker-war-indonesia-bangladesh/>



# Bangladeshi and Indonesian hackers play international game of chicken

By [Lorraine Murphy](#) on July 31, 2013 [Email](#) [Follow](#)

When does a hacker crew beef become a [cyberwar](#)? The answer is, arguably, "yesterday," as a team of Bangladesh hackers attacked vulnerable websites across Indonesia, taking revenge on Indonesian crews in an international game of chicken.

Members of Bangladeshi team Grey Hat (in this case a crew name as well as a set of professional ethics) successfully defaced or took down several websites, claiming that Indonesian cyber-crews had been attacking their crew website and insulting their country.

The Daily Dot spoke with a source involved, who stressed that the participants are all, as far as he is aware, civilians doing this on their own time and for their own reasons.

Defacements are significantly harder to pull off than simple DDoS attacks, showing a greater level of digital sophistication. According to [statements on Facebook](#), the goal of the Bangladeshi crew's attacks was to demonstrate their superior level of skills relative to the Indonesians. In simple terms, to school them.

62

Shares ↗

38

Like

24

Tweet



in

Share

# Japan

## SECURITY

### Japan needs 80,000 EXTRA info-security bods to stay safe

**Chronic shortage of 'outstanding manpower' in the Far East**

By Phil Muncaster, 9th October 2013

10

With a top of the range HP Spectre laptop

Japan has an 80,000 shortfall in infosec professionals, and needs to provide extra training for more than half of those currently in the industry, if it's to protect key IT systems from attack, according to the government.

#### RELATED STORIES

Security firm  
links HIRED GUN  
hackers to  
Aurore 880  
megahacks

A government panel of information security experts met back in June to draw up a long term plan to address Japan's chronic shortage of trained infosec pros, according to *Kyodo* news agency.

Citadel botnet  
reunites to storm  
Japanese PCs

The panel apparently concluded that aside from the 80,000 new recruits, some 100,000 of the 265,000 currently in the industry need additional training to bring them up to speed on the latest threats.

UK doesn't have  
the SKILLS to  
save itself from  
cyber threats

The strategy calls for a review of the current qualification system for info-security professionals as well as an update to university and other courses in the field.

Cyber Security  
Challenge winner  
announced

The aim is apparently not only to boost numbers but to find "manpower with outstanding abilities" – which is easier said than done, especially when budgets are tight and graduates continue to favour other careers.

10

One way Japan is trying to overcome the shortage is through hacking competitions and training camps, according to *Kyodo*.

The Information-Technology Promotion Agency, overseen by the Ministry of Economy, Trade and Industry, is responsible for these and has also apparently been given budget to hire a dozen info-security grads every year.

It's unclear how the government plans to encourage the tens of thousands more needed into the industry.

Source: [http://www.theregister.co.uk/2013/10/09/japan\\_infosecurity\\_skills\\_shortage/](http://www.theregister.co.uk/2013/10/09/japan_infosecurity_skills_shortage/)

### Japan-U.S. security talks likely to highlight Tokyo's cyber-defense woes

Y ✓ X

f t t e

REUTERS Ruairidh Villar October 2, 2013 11:27 AM

By Ruairidh Villar

TOKYO (Reuters) - Top U.S. security officials meet their Japanese counterparts on Thursday as concerns are growing that the hosts cannot protect themselves from malicious internet hackers.

Cyber security is on the agenda when the military and diplomatic chiefs of the two countries hold their first joint meeting in Japan. But even Japanese officials acknowledge they cannot keep up with the proliferating threat of attacks on computer networks from private or state-sponsored hackers.

"Cyber attacks are getting more and more sophisticated, and sometimes we cannot defend against them using the systems we currently have in place," said Kazunori Kimura, the Defense Ministry's director of cyber-defense planning.



Japan's Defence Minister Itsunori Onodera attends a news conference at the Japan National Press Club ...

Source: <http://news.yahoo.com/japan-u-security-talks-likely-highlight-tokyos-cyber-152729325--sector.html>

# Japan needs 80,000 EXTRA info-security bods to stay safe

## Chronic shortage of 'outstanding manpower' in the Far East

By Phil Muncaster, 9th October 2013

10

Win a top of the range HP Spectre laptop

### RELATED STORIES

Securo-boffins link HIRED GUN hackers to Aurora, Bit9 megahacks

Citadel botnet resurges to storm Japanese PCs

UK doesn't have the SKILLS to save itself from cyber threats

Cyber Security Challenge winner announced



Japan has an 80,000 shortfall in infosec professionals, and needs to provide extra training for more than half of those currently in the industry, if it's to protect key IT systems from attack, according to the government.

A government panel of information security experts met back in June to draw up a long term plan to address Japan's chronic shortage of trained infosec pros, according to [Kyodo](#) news agency.

The panel apparently concluded that aside from the 80,000 new recruits, some 160,000 of the 265,000 currently in the industry need additional training to bring them up to speed on the latest threats.

The strategy calls for a review of the current qualification system for info-security professionals as well as an update to university and other courses in the field.

The aim is apparently not only to boost numbers but to find "manpower with outstanding abilities" – which is easier said than done, especially when budgets are tight and graduates continue to favour other careers.

One way Japan is trying to overcome the shortage is through hacking competitions and training camps, according to [Kyodo](#).

The Information-Technology Promotion Agency, overseen by the Ministry of Economy, Trade and Industry, is responsible for these and has also apparently been given budget to hire a dozen info-security grads every year.

It's unclear how the government plans to encourage the tens of thousands more needed into the industry.

## Japan defens



By Ruairidh

TOKYO (R  
Japanese c  
that the hos  
internet hac


Cyber secu  
diplomatic c  
meeting in  
they cannot  
computer n

"Cyber attac  
sometimes  
we currently  
Ministry's di



# Japan-U.S. security talks likely to highlight Tokyo's cyber-defense woes



 **REUTERS** Ruairidh Villar October 2, 2013 11:27 AM

By Ruairidh Villar

TOKYO (Reuters) - Top U.S. security officials meet their Japanese counterparts on Thursday as concerns are growing that the hosts cannot protect themselves from malicious internet hackers.

Cyber security is on the agenda when the military and diplomatic chiefs of the two countries hold their first joint meeting in Japan. But even Japanese officials acknowledge they cannot keep up with the proliferating threat of attacks on computer networks from private or state-sponsored hackers.

"Cyber attacks are getting more and more sophisticated, and sometimes we cannot defend against them using the systems we currently have in place," said Kazunori Kimura, the Defense Ministry's director of cyber-defense planning.



Japan's Defence Minister Itsunori Onodera attends a news conference at the Japan National Press Club ...



# All eyes on ... Russia



## What we know...

- Officially: nothing
- But there are numerous signs:
  - Currently known cyberwars effected Russia (Estonia, Georgia)
  - Russian gangs are key players in organized cybercrime (it's used to be a connection between authorities and criminals)
  - North Korean sources mentions Frunze Academy as the top institute in cyber warfare
  - As Wiki writes, these activities are coordinated by the signal intelligence of FSB and Ministry of Internal Affairs
  - Russian hackers have very strong skills

## My guesses

- Russian officials will deny their capabilities, because this belongs to their secret service
- Maybe there is a strong, unofficial connection between secret service and hacker groups
- Maybe the military uses this connection
- There might be a strong knowledge of cyber warfare leadership, which is an export item for other countries
- They might have skills for devastating cyber attacks (e.g. Russinovich: Zero Day)
- But I'm sure, that they don't have the interest to unfold their capabilities - not now!



## what we know...

- **Officially: nothing**
- **But there are numerous signs:**
  - **Currently known cyberwars effected Russia (Estonia, Georgia)**
  - **Russian gangs are key players in organized cybercrime (it's used to be a connection between authorities and criminals)**
  - **North Korean sources mentions Frunze Academy as the top institute in cyber warfare**
  - **As Wiki writes, these activities are coordinated by the signal intelligence of FSB and Ministry of Internal Affairs**
  - **Russian hackers have very strong skills**

# My guesses

- **Russian officials will deny their capabilities, because this belongs to their secret service**
- **Maybe there is a strong, unofficial connection between secret service and hacker groups**
- **Maybe the military uses this connection**
- **There might be a strong knowledge of cyber warfare leadership, which is an export item for other countries**
- **They might have skills for devastating cyber attacks (e.g. Russinovich: Zero Day)**
- **But I'm sure, that they don't have the interest to unfold their capabilities - not now!**



# UK - US, BFF





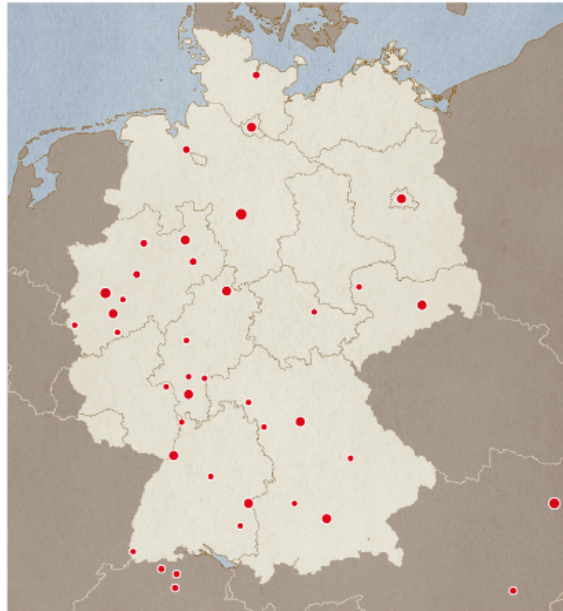
BFBS



FOR HARDWORKING PEOPLE

YouTube

# Germany - the controversial country



Federal Ministry  
of the Interior

## Cyber Security Strategy for Germany



# Estonia - the only victim

 **KAITSELIIT** et en

[to the homepage](#) | [Sitemap](#)

Text size: a a a  
Print

[Estonian Defence League](#) | [District](#) | [Women's Home Defence](#) | [Young Eagles](#) | [Home Daughters](#) | [EDL School](#) | [Cyber Unit](#) | [Contact](#)

## Estonian Defence League's Cyber Unit

[EDL » Cyber Unit](#)

The Estonian Defence League's Cyber Unit (EDL CU) is a voluntary organisation aimed at protecting Estonian cyberspace.

The Cyber Unit's mission is to protect Estonia's high-tech way of life, including protection of information infrastructure and supporting broader objectives of national defence

The Cyber Unit includes specialists in key cyber security positions in national critical infrastructure, patriotic individuals with IT skills, including youth who are ready to contribute to cyber security, and specialists in other fields that concern cyber security (lawyers, economists etc).

EDL CU objectives:

- development of cooperation among qualified volunteer IT specialists
- raising the level of cyber security for critical information infrastructure through the dissemination of knowledge and training
- creation of a network which facilitates public private partnership and enhances preparedness in operating during a crisis situation
- education and training in information security
- participation in international cyber security training events

[History of the EDL CU](#)

[The main tasks of the EDL CU](#)

[Frequently Asked Questions](#)

 **press information**

[EDL Museum](#)





# KAITSELIIT

et | en

[To the homepage](#) | [Sitemap](#)



Text size: a a a

Print

[Estonian Defence League](#)

[District](#)

[Women's Home Defence](#)

[Young Eagles](#)

[Home Daughters](#)

[EDL School](#)

[Cyber Unit](#)

[Contact](#)

## Estonian Defence League's Cyber Unit

[EDL](#) » [Cyber Unit](#)

The Estonian Defence League's Cyber Unit (EDL CU) is a voluntary organisation aimed at protecting Estonian cyberspace.

The Cyber Unit's mission is to protect Estonia's high-tech way of life, including protection of information infrastructure and supporting broader objectives of national defence

The Cyber Unit includes specialists in key cyber security positions in national critical infrastructure, patriotic individuals with IT skills, including youth who are ready to contribute to cyber security, and specialists in other fields that concern cyber security (lawyers, economists etc).

EDL CU objectives:

- development of cooperation among qualified volunteer IT specialists
- raising the level of cyber security for critical information infrastructure through the dissemination of knowledge and training
- creation of a network which facilitates public private partnership and enhances preparedness in operating during a crisis situation
- education and training in information security
- participation in international cyber security training events

[History of the EDL CU](#)

[The main tasks of the EDL CU](#)

[Frequently Asked Questions](#)



### press information

[EDL Museum](#)

# Hungary - and Hacktivity

## Miniszteri utasítás a honvédségi kibervédelemről

Forrás: MTI | 2013. október 08. kedd 16:41 |



**Mától hatályos a Magyar Honvédség (MH) kibervédelmi szakmai koncepciójának kiadásáról szóló miniszteri utasítás, amely a honvédség kiberművelési tevékenységének alapelveit, feladatait határozza meg.**

A Honvédelmi Minisztérium (HM) a Magyar Honvédség kommunikációs és információs rendszereinek védelméért, valamint az ehhez szükséges kibervédelmi képességek kialakításáért és fejlesztéséért felelős.

A tárca az MTI megkeresésére azt közölte: a koncepció célja, hogy a nemzeti és nemzetközi törekvésekkel összhangban szabályozza a Magyar Honvédség katonai szervezeteinek vezetéséhez és irányításához szükséges katonai híradó és informatikai rendszer (MH Kormányzati Célú Elkülönült Hírközlő Hálózat) védelmi képességeinek megerősítését.

... and the long journey



Peszleg Tibor

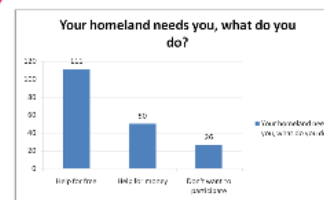


Muha Lajos



Kovács László

You told me: Digital Mohács



## Miniszteri utasítás a honvédségi kibervédelemről

Forrás: MTI | 2013. október 08. kedd 16:41 |



**Mától hatályos a Magyar Honvédség (MH) kibervédelmi szakmai koncepciójának kiadásáról szóló miniszteri utasítás, amely a honvédség kibernműveleti tevékenységének alapelveit, feladatait határozza meg.**

A Honvédelmi Minisztérium (HM) a Magyar Honvédség kommunikációs és információs rendszereinek védelméért, valamint az ehhez szükséges kibervédelmi képességek kialakításáért és fejlesztéséért felelős.

A tárca az MTI megkeresésére azt közölte: a koncepció célja, hogy a nemzeti és nemzetközi törekvésekkel összhangban szabályozza a Magyar Honvédség katonai szervezeteinek vezetéséhez és irányításához szükséges katonai híradó és informatikai rendszer (MH Kormányzati Célú Elkülönült Hírközlő Hálózat) védelmi képességeinek megerősítését.

# ... and the long journey



Peszleg Tibor



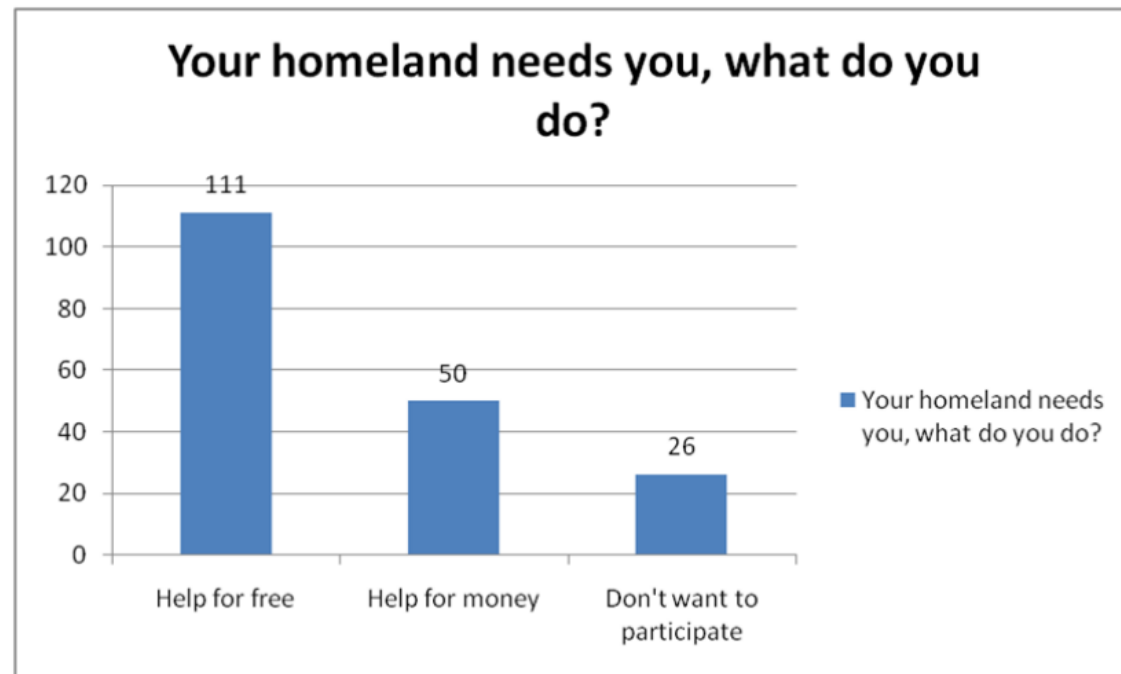
Muha Lajos



Kovács László



## You told me: Digital Mohács



# Summary

## The USA way

- You have good SIGINT capabilities
- You are a western democracy or allied partner
- You have strong IT industry
- IT security knowledge come from civil universities
- You talk much about cyber defense
- You try to recruit from the civil experts
- You have both offensive and defensive capabilities
- Example: USA, UK, South Korea, India, Israel, Japan

## Russian-Chinese way

- You have good SIGINT capabilities
- You have communist heritage in your military
- You're engineers are quite good in IT
- You have military schools for cyber security and you get many knowledge from western universities through patriot students
- It seems that everyone tries to blame you with hacking, but you state innocence
- You have a plenty of well educated cyber soldiers
- You have mainly offensive capabilities
- Examples: Russia, China, North Korea

## The patriot way

- You're army is ready for a traditional conflict
- You are a developing (Asian) country
- You're economy is not IT/network centric
- IT security knowledge come from abroad and hacker communities
- You don't talk about cyber defense, but talk about your problems with neighbor countries
- You have patriot hackers
- You have offensive capabilities
- Example: Syria, Iran, Pakistan, Bangladesh, Turkey

## The European way

- You have SIGINT capabilities that need for NATO and self defense
- You are EU and NATO member
- IT is strong part of your economy
- IT security knowledge come from civil universities
- You feel, that everyone is against you in the cyberspace
- You try to recruit from the civil experts (as officers or as reservists)
- You have defensive capabilities
- Example: Germany, Estonia, Hungary

## The USA way

- You have good SIGINT capabilities
- You are a western democracy or allied partner
- You have strong IT industry
- IT security knowledge come from civil universities
- You talk much about cyber defense
- You try to recruit from the civil experts
- You have both offensive and defensive capabilities
- Example: USA, UK, South Korea, India, Israel, Japan



## Russian-Chinese way

- You have good SIGINT capabilities
- You have communist heritage in your military
- You're engineers are quite good in IT
- You have military schools for cyber security and you get many knowledge from western universities through patriot students
- It seems that everyone tries to blame you with hacking, but you state innocence
- You have a plenty of well educated cyber soldiers
- You have mainly offensive capabilities
- Examples: Russia, China, North Korea



## The patriot way

- You're army is ready for a traditional conflict
- You are a developing (Asian) country
- You're economy is not IT/network centric
- IT security knowledge come from abroad and hacker communities
- You don't talk about cyber defense, but talk about your problems with neighbor countries
- You have patriot hackers
- You have offensive capabilities
- Example: Syria, Iran, Pakistan, Bangladesh, Turkey



## The European way

- You have SIGINT capabilities that need for NATO and self defense
- You are EU and NATO member
- IT is strong part of your economy
- IT security knowledge come from civil universities
- You feel, that everyone is against you in the cyberspace
- You try to recruit from the civil experts (as officers or as reservists)
- You have defensive capabilities
- Example: Germany, Estonia, Hungary

Thank you!

Web: [www.krasznay.hu](http://www.krasznay.hu)

E-mail: [csaba@krasznay.hu](mailto:csaba@krasznay.hu)

 **HACKTIVITY**