

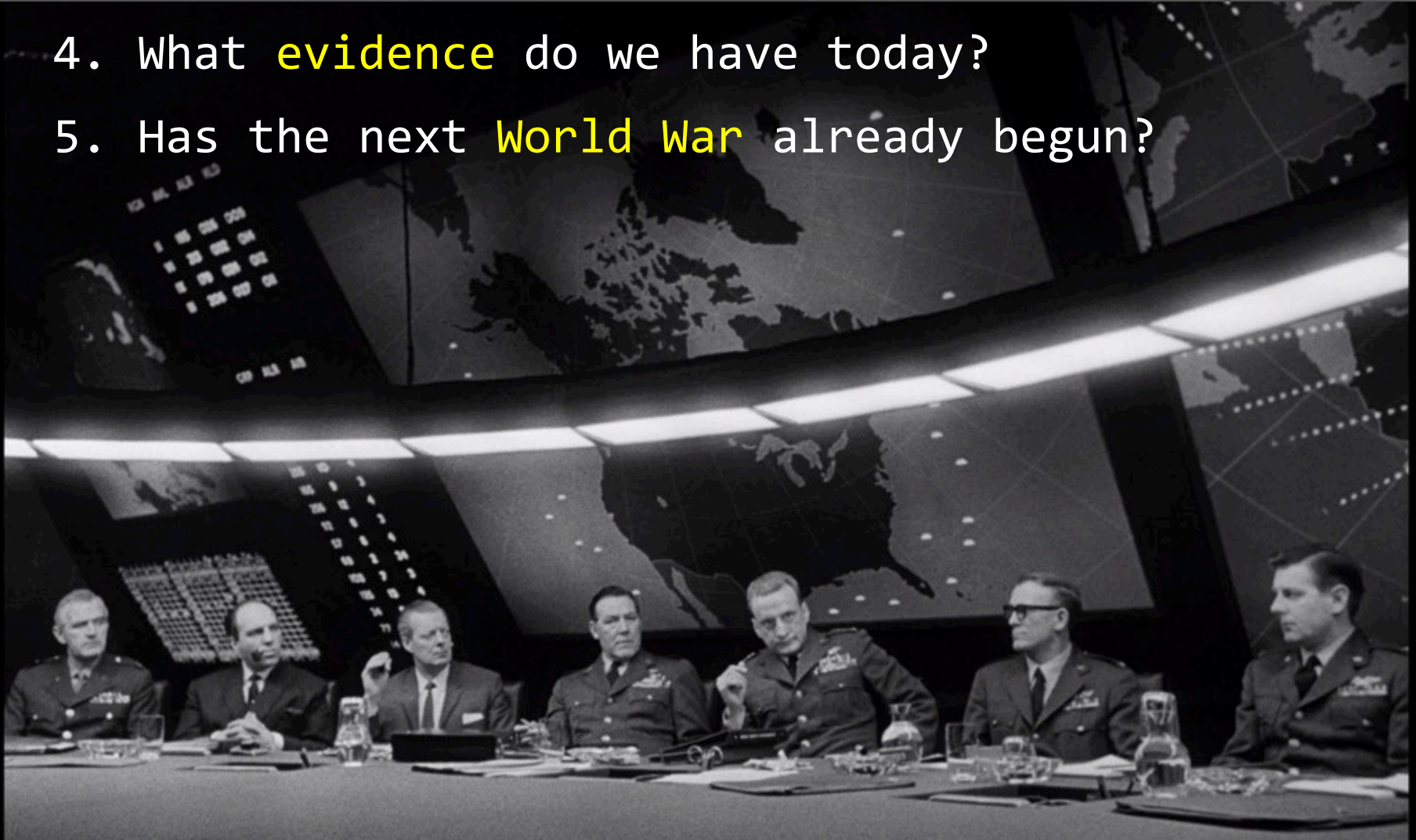


Cyberspace as Battlespace

Kenneth Geers

2501

1. Can computer hacking be an **act of war**?
2. What are the **limits to hacking** in peacetime?
3. Do **cyber war preparations** = cyber war?
4. What **evidence** do we have today?
5. Has the next **World War** already begun?



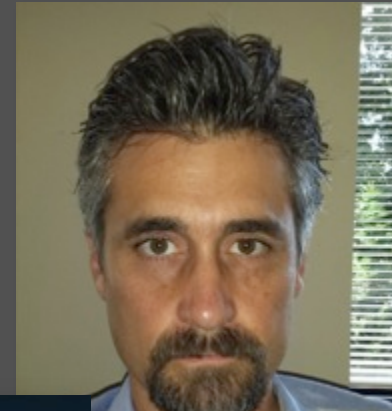
Kenneth Geers, PhD CISSP

- 2501

- U.S. Government: 20 years
 - NSA, NCIS, NATO
- NATO Cyber Centre Ambassador
- FireEye

- Author

- Strategic Cyber Security
- Editor: The Virtual Battlefield
- Technical Expert: Tallinn Manual
- 20+ articles/chapters
 - Cyber conflict



Books: www.ccdcoe.org
Blog: www.2501research.com
Twitter: [@KennethGeers](https://twitter.com/KennethGeers)

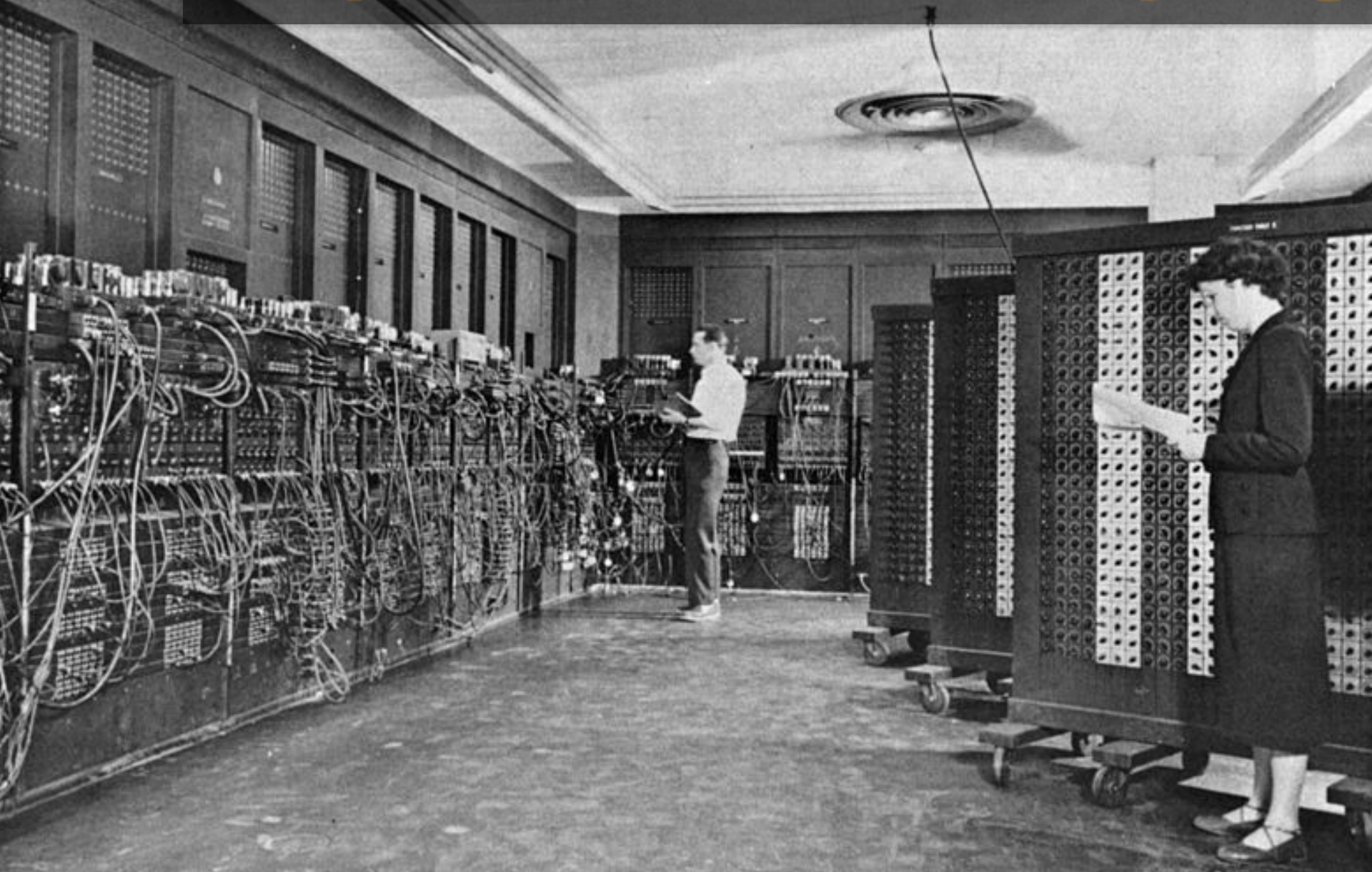
A traditional Chinese landscape painting in the style of a 'Shan Shui' (mountain-water) genre. The scene depicts a vast, hazy landscape with rolling hills, sparse trees, and a few small figures in the distance. The color palette is dominated by earthy tones of brown, ochre, and green. In the upper left corner, there is a vertical inscription of Chinese calligraphy and several red artist seals. A semi-transparent black rectangular box is overlaid on the left side of the image, containing the title text. A 3D-rendered, metallic, saucer-shaped UFO is positioned in the lower-left quadrant of the image, appearing to float in the sky.

Science fiction or Sun Tzu?

“Supreme excellence consists in breaking the enemy’s resistance **without fighting.**”

“The best thing of all is to take the enemy’s country **whole and intact.**”

The power of electronic computing



E = PRMLUL-1M -1R -1P -1



The KGB
The Computer
and Me



Want
her
email address?

It's only
\$10

Operation Orchard



U.S. GOVERNMENT



1. Denial of Service
2. Data Modification

Syria



To the Syrian people: The world stands with you against the brutal regime of Bashar Al-Assad. Know that time and history are on your side – tyrants use violence because they have nothing else, and the more violent they are, the more fragile they become. We salute your determination to be non-violent in the face of the regime's brutality, and admire your willingness to pursue justice, not mere revenge. All tyrants will fall, and thanks to your bravery Bashar Al-Assad is next.

To the Syrian military: You are responsible for protecting the Syrian people, and anyone who orders you to kill women, children, and the elderly deserves to be tried for treason. No outside enemy could do as much damage to Syria as Bashar Al-Assad has done. Defend your country – rise up against the regime! – Anonymous

إلى الشعب السوري : إن العالم يملك معكم ضد النظام الوحشي لبشار الأسد. أعتقد أن الوقت والقوانين ، أول جالتكم -- الطغاة يمتدحون التعلك لأن يوم لديهم أو شرا آخر . و كلما زاد عنفهم ، كلما أكثر مفاقة اصبحوا . ليس تصديقكم على أن تكفروا سلبياً بل مواجهة وحشية النظام . ونعجب استعدادكم لتحقيق العدالة و ليس الانتقام . سوف يفظ جميع الطغاة . وينقل جثثكم... بشار الأسد عز التنازل.

إلى الجيش السوري : أنت مسؤول عن حماية الشعب السوري. وكل من يأمره بقتل النساء والأطفال والمسنين يستحق أن يماتم بتهمة الخيانة. لا يمكن أن نعو نأرجح أن يخلق الضرر سوريا بغير ما قام به بشار الأسد. دافعوا عن بلدكم - اطلبوا ضد النظام - مجهول



July 2014

- **Truecaller**
 - 100B tel numbers
- **Tango**
 - Millions of accounts
- **Viber**
 - 200M users in 193 countries



LATEST SYRIAN ELECTRONIC ARMY NEWS



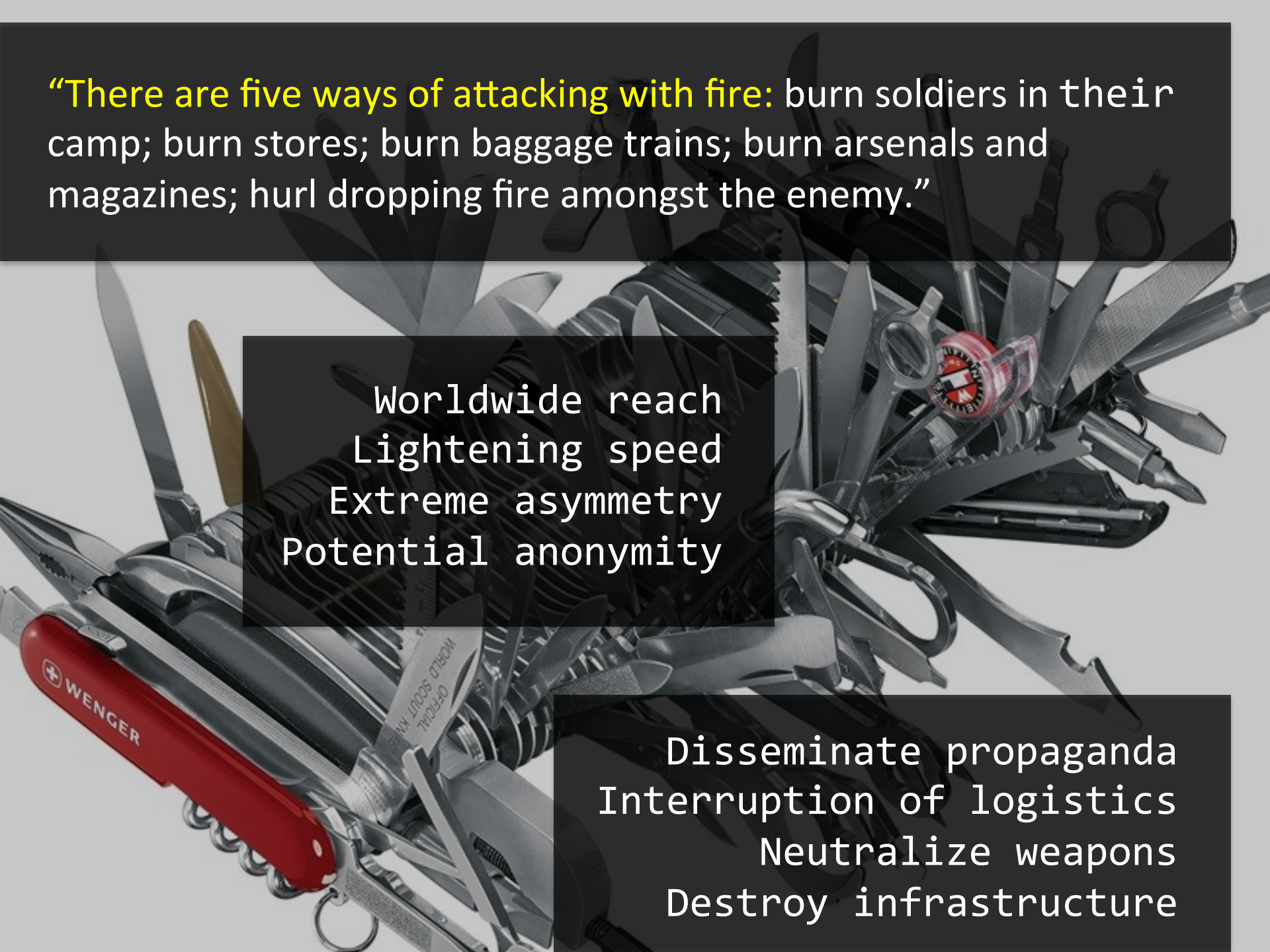
Grand cyber strategy

- Defend sovereignty
- Project power
- Net ubiquity/amplification
- Network vulnerabilities
- High return on investment
- Immature cyber defenses
- Plausible deniability
- Propaganda

Stuxnet



Wikileaks



“There are five ways of attacking with fire: burn soldiers in their camp; burn stores; burn baggage trains; burn arsenals and magazines; hurl dropping fire amongst the enemy.”

Worldwide reach
Lightening speed
Extreme asymmetry
Potential anonymity

Disseminate propaganda
Interruption of logistics
Neutralize weapons
Destroy infrastructure



F-35
Cockpit

Navy's Self-Guided, Unmanned Patrol Boats Make Debut

NORFOLK, Va. — Oct 5, 2014, 6:37 AM ET

By BROCK VERGAKIS Associated Press

 Like 7.8k

 share 1,429

 Tweet 783

 +1 23

  167 Comments 



This Tuesday Aug. 12, 2014 photo provided by the U.S. Navy shows an unmanned 11-meter rigid hulled inflatable boat (RHIB) from Naval Surface Warfare Center Carderock, as it operates autonomously during an Office of Naval Research demonstration of... [View Full Caption](#)

The Associated Press

Cyber Army



- Intelligence = intelligence
- HUMINT = social engineer
- Special forces = special forces
- Engineer = software developer
- Infantry = hacker
- Terrain = hardware
- Tents = software
- Weapons = information



Invisible battlefield

USA

Fischer

INTERNATIONALER GROSSMEIS

SOWJETUNION

Mich



Geneva Convention Legitimate targets:

- Military
- Infrastructure
- Communications
- Industry
- Research
- Energy



(Cyber) Arms Control

- Public knowledge
- Political will
- Military desire
- Diplomacy
- Prohibition
- Assistance
- Inspection



- **CYBERCOM: Analogies Project**

- Pearl Harbor

- Surprise Attack

- Predelegation

- Economic Warfare

- Air Power / Air Defense

- Offense-Defense Balance

- Innovation War



U.S. Cyber Command



Cybercom seal

On June 23, 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command to establish a sub-unified command, United States Cyber Command (USCYBERCOM). Full Operational Capability (FOC) was achieved Oct. 31, 2010. The command is located at Fort Meade, Md.

Formal Name

U.S. Cyber Command (USCYBERCOM)

Commander

[Admiral Michael S. Rogers](#)

Mission

USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

Focus

The Command has three main focus areas: Defending the DoDIN, providing support to combatant commanders for execution of their missions around the world, and strengthening our nation's ability to withstand and respond to cyber attack.



Joint Forces Command

Part of [Ministry of Defence](#)

What we do

We work toward making military operations successful by making sure joint capabilities, like medical services, training and education, intelligence, and cyber-operations, are efficiently managed and supported. We also ~~communicate actual experience in operational theatres so that it can be~~ reflected in top-level decision making.

News story

New cyber reserve unit created

From: [Ministry of Defence, Joint Forces Command](#) and [The Rt Hon Philip Hammond MP](#)

First published: 29 September 2013

Part of: [Leading international efforts to resolve concerns about Iran's nuclear programme](#), [Providing versatile, agile and battle-winning armed forces](#) and [a smaller, more professional Ministry of Defence](#), + others

Britain will build a dedicated capability to counter-attack in cyberspace and, if necessary, to strike in cyberspace.

Involved
Announcements



Enjeux

- Politique de Défense
- Doctrine
- Modernisation
- Restructurations
- Economie de Défense
- Recherche et développement
- Equipements
- Cyberdéfense**

La cyberdéfense

🏠 | T+ | T- | ★ Ajouter aux favoris | ✉ Envoyer à un ami | **PARTAGER** ...

Mise à jour : 30/04/2014 11:04 - Auteur : La rédaction

Priorité stratégique pour la souveraineté nationale, la cyberdéfense représente l'avenir de la Défense dans un milieu virtuel et sans frontière. Par le biais de nombreux acteurs, le ministère de la Défense participe activement à la protection et à la défense des systèmes d'information dans le cyberspace.

La cyberdéfense est un enjeu majeur

« Le ministère de la Défense est au rendez-vous du défi immense qui se pose à chacun d'entre nous. A travers ses capacités et son expertise, il assume plus que jamais le rôle qui doit être le sien. Les menaces cyber nous concernent tous. C'est collectivement que nous parviendrons à y répondre. » (Extrait de l'élocution du ministre de la Défense, Jean-Yves Le Drian, le 21 janvier 2014 à Lille, forum internationale de la cybersécurité).

Le Livre blanc pour la défense et la sécurité nationale de 2013 fait de la cyberdéfense une priorité nationale. « Avec le Livre blanc 2013, nous venons déposer la pierre d'angle de l'ambition nationale en matière de cyberdéfense », a annoncé le ministre de la Défense, Jean-Yves Le Drian, le 3 juin 2013, à Rennes.



Pour le ministère de la Défense, la cyberdéfense est un enjeu majeur. En effet, le ministère de la Défense développe et opère des systèmes d'information et de communication particulièrement complexes tant en France qu'à l'extérieur du territoire national, supports essentiels des opérations militaires. Il est responsable des systèmes les plus stratégiques, ceux liés à la dissuasion nucléaire mais également des systèmes d'armes sophistiqués : aéronefs de combat ou de transport, navires de surface ou sous-marins, véhicules de combat terrestres.

Aujourd'hui, toute opération militaire comporte un volet cyber plus ou moins développé. Au même titre que la terre, la mer, l'air et l'espace, le cyberspace est un milieu à part entière dont la

défense est une nécessité permanente. ~~Pénétration des réseaux à des fins d'espionnage,~~ prise de contrôle à distance, destruction d'infrastructures vitales, les types de menaces sont nombreux.

La cyberdéfense est prise en compte au plus haut niveau de décision au sein du ministère de la Défense. Le Pacte Défense Cyber, lancé par Jean-Yves Le Drian renforce significativement ~~les moyens dévolus à la cyberdéfense, dans la continuité de la Loi de programmation militaire~~ 2014-2019.

Le Pacte Défense Cyber, lancé le 7 février 2014, met en perspective l'ensemble des travaux menés par le ministère de la Défense. A travers 50 actions, il se fonde sur une démarche pragmatique et des projets concrets. Ainsi, le renforcement de la base industrielle de technologies de défense et de sécurité nationale est assuré. Les crédits consacrés aux études amont sont renforcés. La formation et la recherche académique sont également encouragées afin de préparer l'avenir à court, moyen et long terme.



News > News and Events

SHARE

- News** | Close
- News and Events
 - A Nation's Army
 - Innovation
 - Features
 - Personal Stories
 - Commanders Speak

- News Channels** | Close
- Personal Stories
 - A Nation's Army
 - Innovation
 - Features
 - Commanders Speak

IDF in cyber space: Intelligence gathering and clandestine operations

IDF defines its activity in cyber space as a platform to improve operational effectiveness and defense. IDF has been relentlessly operating in the field

Date: 03/06/2012, 1:54 PM Author: Rotem Pessu

IDF Operations Department recently defined the essence of IDF cyber warfare, putting together instructions that define the military's operational methods in cyber space and clarify its goals in facing potential enemies. IDF Website exclusively reveals these instructions for the first time.

According to the document, cyber space is to be handled similarly to other battlefields on ground, at sea, in the air and in space. The IDF has been engaged in cyber activity consistently and relentlessly, gathering intelligence and defending its own cyber space. Additionally if necessary the cyber space will be used to execute attacks and intelligence operations.

There are many, diverse, operational cyber warfare goals, including thwarting and disrupting enemy projects that attempt to limit operational freedom of both the IDF and the State of Israel, as well as incorporating cyber warfare activity in completing objectives at all fronts and in every kind of conflict. Moreover, it will be used to maintain Israel's quality and advantage over its enemies and prevent their growth and military capabilities, while limiting their operation in this field.

Additional goals defined by the document published by the Operations Department include creation of operational conditions that will assist in fulfilling IDF capabilities in combat as well as influence public opinion and raise awareness by advocating in the cyber space.

Overall cyber space will be used to improve the operational effectiveness of the IDF, both during war and peace time. This will be done through clandestine activity, while maintaining confidentiality and expertise.



More in this channel

- "A dramatic period for women's service in the IDF"
- Naval officers to undergo ground-combat testing
- IDF honors outstanding Bedouin soldiers
- Artillery, shots fired from Syria at IDF forces

Iran to launch first cyber command

According to *The New York Times*, the American covert projects include the creation of independent cellphone networks in foreign countries, as well as the "Internet in a suitcase" program.

The establishment of independent cellphone networks would enable political dissidents to communicate outside the reach of governments in countries like Iran and Syria, according to the report.

"Internet in a suitcase" could also be secretly smuggled across a border and contains all the necessary hardware and networking devices to promptly establish a wireless network over a large area that can connect to the global Internet.

"Internet in a suitcase" is apparently in a prototype stage and the US government has provided a grant of USD two million to get it up and running.

In one of the most ambitious efforts, US officials say, the State Department and Pentagon have also spent at least USD 50 million to establish an independent cellphone network in Afghanistan using towers on protected military bases inside the country.

More recently, Washington has supported the development of software that preserves the anonymity of users in places such as China, and offers training to citizens that want to pass information through the internet without getting caught.

MP/MMA/MB



Deputy Head of Iran's Armed Forces Joint Chiefs of Staff Brigadier General Masoud Jazayeri

A senior Iranian military commander has announced plans to establish its first cyber command for the country's Armed Forces in order to counter 'soft warfare' against the Islamic Republic.

Wed Jun 15, 2011 10:20AM

0

0

Share

Tweet

Deputy Head of Iran's Armed Forces Joint Chiefs of Staff Brigadier General Masoud Jazayeri told reporters on Tuesday that comprehensive studies on the cyber command have already been carried out and the results will soon be rendered to the Iranian Armed Forces, IRNA reported.

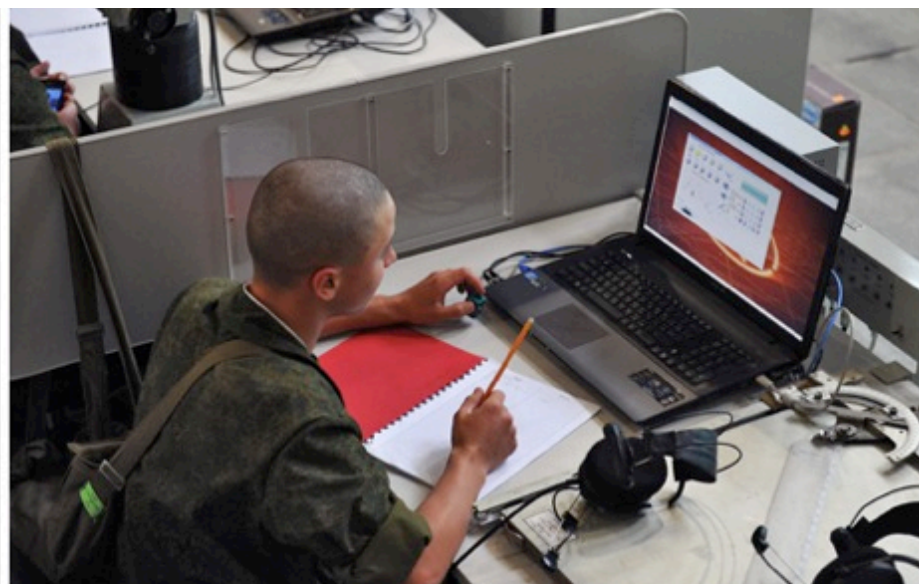
The Iranian commander also emphasized that Iran's military forces must be equipped with state-of-the-art technology when it comes to soft warfare.

The remarks come as the Obama administration is actively engaged in the process of establishing a "shadow" internet and mobile phone systems throughout the world.

Russia to get cyber troops

July 16, 2013 Anastasia Petrova, Vzglyad

A new service branch, responsible for information security, would be added to the Russian army as soon as this year.



The new service's key tasks would include monitoring and processing information coming from the outside, as well as countering cyber threats. Source: Kommersant

By the end of this year, Russia's armed forces will get a new service branch responsible for information security. Officers serving in the branch will be required to have a linguistic background. President Vladimir Putin believes that the "firepower" of information attacks could be higher than that of conventional weapons.

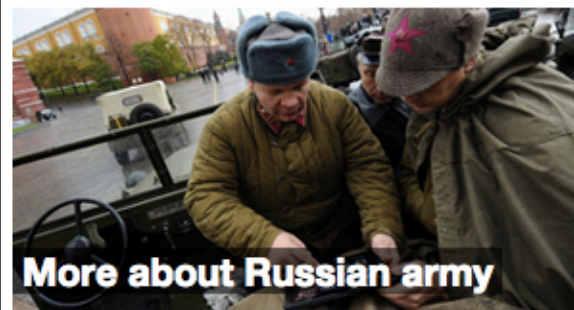
President Vladimir Putin stated on Friday, July 5, that it was necessary to counter cyber threats effectively. "We have to be prepared to counter threats in cyberspace effectively, to improve the level of protection of the relevant infrastructure—above all, information systems of strategic and mission-critical facilities," the head of state told a [Security Council meeting](#) dedicated to improving Russia's military organization through 2020.

Putin reminded his audience that "information attacks" were already being used to achieve [military and political goals](#). He also noted that their "firepower" could be higher than that of conventional weapons.

A source at the Ministry of Defense told RIA Novosti that a service branch responsible for the nation's information security would be added to the Russian army as soon as this year.

The source confirmed that the new service's key tasks would include monitoring and processing information coming from the outside, as well as countering cyber threats—"in other words, something along the lines of the United States Army Cyber Command."

Officers preparing to serve in this branch will require linguistic training; they will have to learn a foreign language, primarily English.



More about Russian army

This matter was first brought up for broad discussion last spring, according to [Deputy Prime Minister Dmitry Rogozin](#). [Minister of Defense Sergei Shoigu](#) asked several General Staff divisions last

February to complete the development of a cyber command.

Alexander Sharavin, director of the Institute for Political and Military Analysis and member of the Academy of Military Sciences, claims that the Ministry of Defense received proposals on creating such a command 10 years ago.

"We had a rather heated discussion about it back then, and, as far as I know, we should get this command very soon. Protecting our cyber networks is not only a task for our armed forces; it's a task for the entire state, for our security services. A cyber war is already on, so such commands are tasked not only with protecting but also with delivering counter strikes if needed," Sharavin told RIA Novosti. He added that Russia could outstrip its rivals in this area by listening to experts, because it was an urgent task "yesterday and the day before yesterday."

"A concept for using [cyber weapons](#) was developed six or seven years ago. Today, this sort of weapon is second in importance only to nuclear arms," [Anatoly Toyganok](#), director of the Center for Military Forecasting and lecturer at Moscow State University's Global Policy Department, told Vzglyad.



President Vladimir Putin believes that the "firepower" of information attacks could be higher than that of conventional weapons. Source: ITAR-TASS

"Cyber weapons are widely used in military conflicts, most recently during the U.S. intervention in Libya, where they controlled not only airspace [...], but also telecommunication networks. They were hacking into Libyan TV networks to broadcast programs for the local population," said Tsyganok.

According to the expert, Israel leads the way in this area, having implemented advanced digital technology in 2005. "The American protection ranks second, followed by Western Europe's," Tsyganok said.

During the same week, Shoigu asked his associates to locate the students of one St. Petersburg university, which had won a global computer programming championship for the fifth time. "I heard on the TV today that students at a St. Petersburg university won the global computer programming championship for the fifth time. We have to find them. We have to work with these guys somehow, because we need them badly," the minister said in early July, during a meeting with university rectors and the public on the subject of science units in the army.

"The minister of defense has asked me to meet these guys personally and tell them about military-related software development projects that we are actively carrying out," Deputy Minister Oleg Ostapenko told journalists on Friday. He added that solving these problems requires supreme skills and unconventional approaches to developing optimal algorithms for subsequent programming.

"These are the exact qualities that have always

been characteristic of the Russian programming school, which enjoys a stellar reputation among major software developers around the world. Perhaps these guys might be interested in some of our projects," Ostapenko was quoted by RIA Novosti as saying.

In this case, Ostapenko said, the Ministry of Defense would be ready to offer them the required conditions, including project finance (at least at the market level) to create an environment for effective work.

Related:

[Russian army developing cyberattack defenses](#)

[Russian Army to enlist computer wizards in innovation push](#)

[Russia warns against NATO document legitimizing cyberwars](#)



MINISTRY OF NATIONAL DEFENSE THE PEOPLE'S REPUBLIC OF CHINA

WWW.MOD.GOV.CN

[Home](#) [Ministry](#) [Defense News](#) [Press Briefings](#) [Opinion](#) [Int'l Military](#) [Photos](#) [Video](#) [Chinese\(GB\)](#)

You're at: [News Channels](#)>> [Defense News](#)

SEARCH:

ALL

GO

China: U.S. hacking report groundless

(Source: China Military Online) 2014-September-22 16:36

BEIJING, September 22 (MOD) -- Geng Yansheng, spokesman of the Chinese Ministry of National Defense (MND), said on September 20, 2014 that the report released by the U.S. accusing China of hacking is completely groundless and ill-founded.

Geng Yansheng pointed out that the U.S. Senate Committee on Armed Services released a so-called China hacking report, lodging irresponsible assaults and accusations against China. The U.S. report is completely groundless and ill-founded.

He stressed that neither the Chinese government nor its military has ever engaged in or supported any cyber attack or espionage activities. China consistently and firmly objects and cracks down on such crimes as cyber attacks according to law.

Geng Yansheng noted that China is one of the major victims of hacker attacks in the world facing severe threat of cyber attack. China has obtained sufficient evidence for cyber attacks against it from overseas.

Geng Yansheng emphasized that it has been more than one year after the "PRISM" event, the U.S. should reflect on its own actions of cyber espionage, wiretapping and monitoring on high-ranking foreign government officials, enterprises and individuals, and provide clear explanations to China and the international community. We urge the U.S. side to do something helpful for the cyber peace and security instead of something opposite.

Defense News

[PLA to perform military missions in Bohai Sea](#)

[China issues opinion on military information security](#)

[Troops rush to quake-hit Pu'er for rescue](#)

[Chinese naval ship berths in Salalah Port for replenishment](#)

[Chinese soldiers join Australian, U.S. troops in joint exercises in Australia](#)

[MORE](#)

Press Briefings

[Defense Ministry's regular press conference on Sep. 25, 2014](#)

[China says submarine docking in Sri Lanka was 'routine'](#)

[China, India have smooth communication on boundary issue](#)

[China, U.S. to hold defense talks](#)

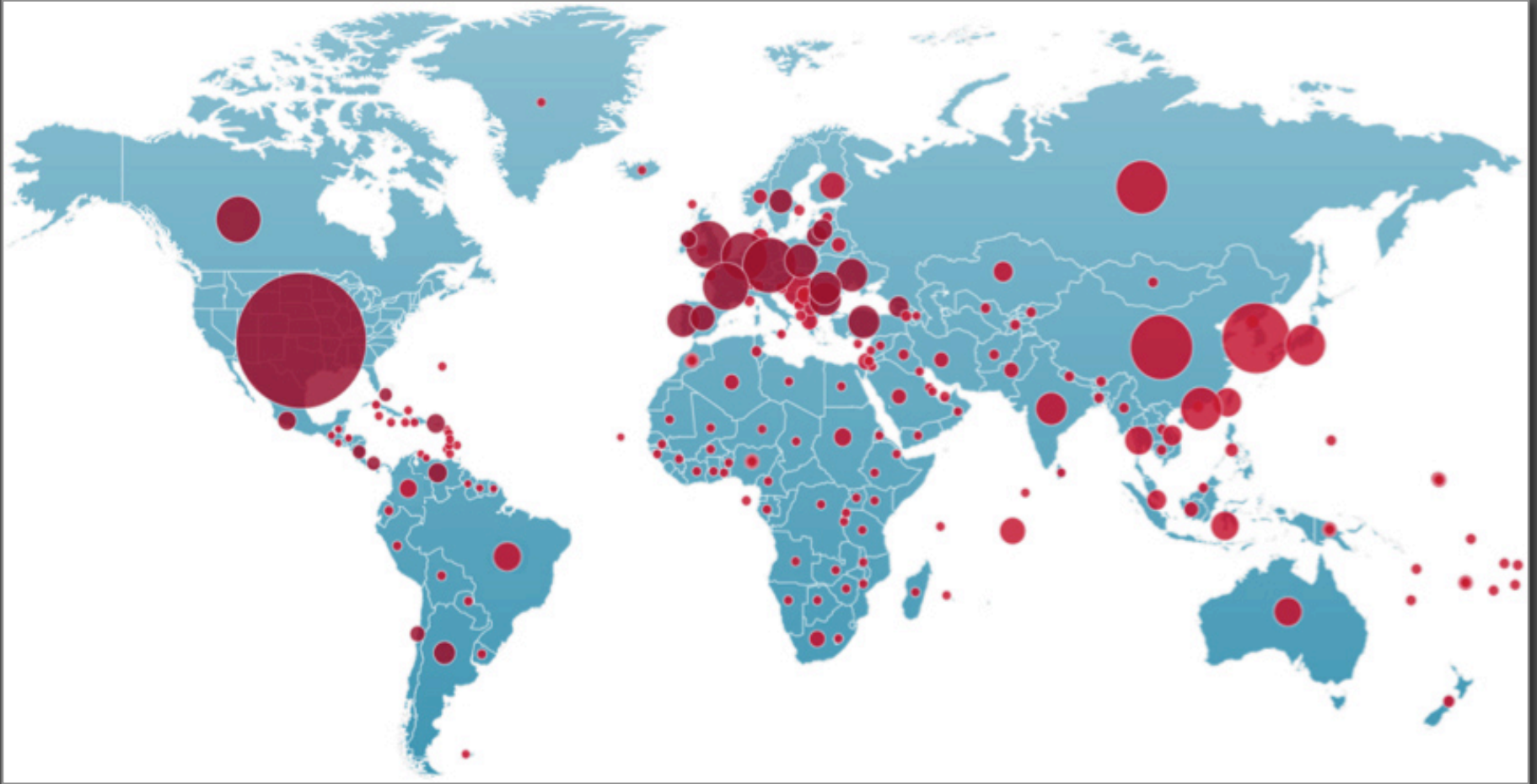
[China to send 700 peacekeepers to South Sudan for UN mission](#)

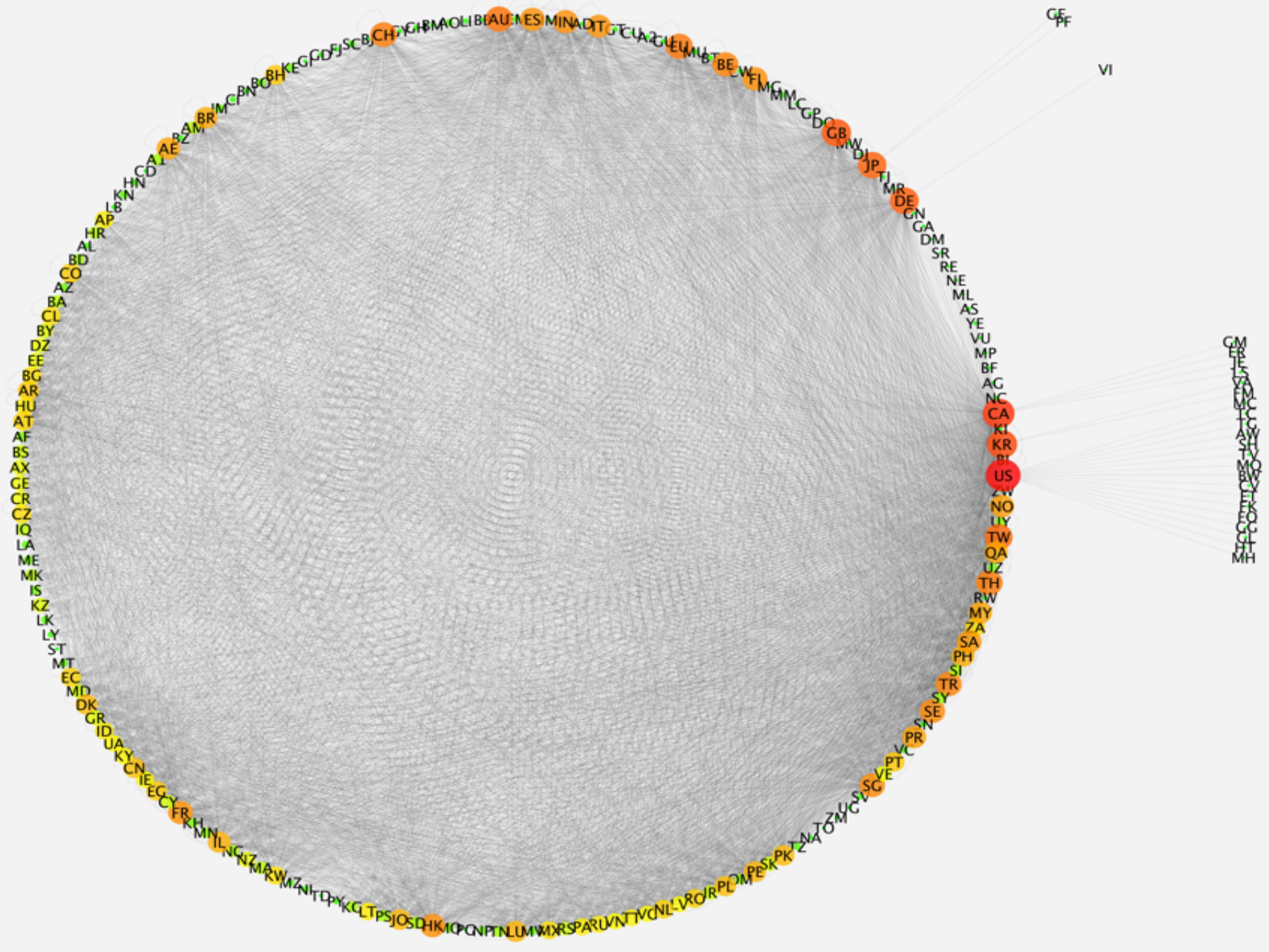
Nation States

- **Offense**
 - APT
- **Defense**
 - Net Sec
 - Law Enforcement
 - Counter-intelligence
- **Last line ...**
 - Military?



How much is **occupied ground**?





Ramifications

1. It is **hard to predict** the next war.
2. **Hostile activities** are taking place in **peacetime**.
3. **Human rights** may be needlessly harmed.
4. This dynamic may be a **recipe for chaos** on the Internet.





IRANIANS

we will never bomb your country

We ♥ You

**Cyber
Diplomacy**



Lackin:

ISRAELIS

We do not want a nuclear BOMB

We want peace and democracy

We Are Your Friends



Future

- There is **one Internet / one cyber battlefield**
 - Governments spy on students (and vice versa)
- Tactical investment
 - Technical education
- Strategic investment
 - Concept development
- Transparency / accountability in government
 - **Internet itself is the best mechanism**
- International problem = **international solution**
 - NATO / EU / UN best places to start

Cyberspace as Battlespace

Kenneth Geers

2501