The European Centre for Information Policy and Security (ECIPS)

Presents

Speaker Mr. Ricardo Baretzky

Cyber Terrorism & Counter Intelligence behind it.

FIVE MOST COMMON SOURCES OF CYBER THREATS

- National Governments (Cyber Conflict)
- Industrial Spies and Organized Crime Groups
- Hacktivists
- Hackers
- Terrorists

The Cyber Terrorists

- Terrorists (groups seeking to expand their capability in this area)
- Terrorist sympathizers/ supporter (<u>the most likely group to launch a cyber attack</u>)
- "The Thrill" seekers (a minor threat because they are driven by a desire to show off their skills rather than a desire to destroy)

It All began In 2002

The use of the Internet to spread their messages began in 2002 when Imam Samudra claimed responsibility for the Bali bombings via istimata.com

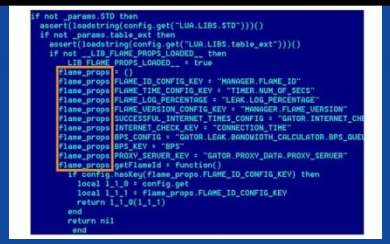
Today's Governments are confronted with two types of Terrorist

A) Those who focus on Nation States <u>Conflict Time ?</u>

B) Cyber Terrorists & Insurgents

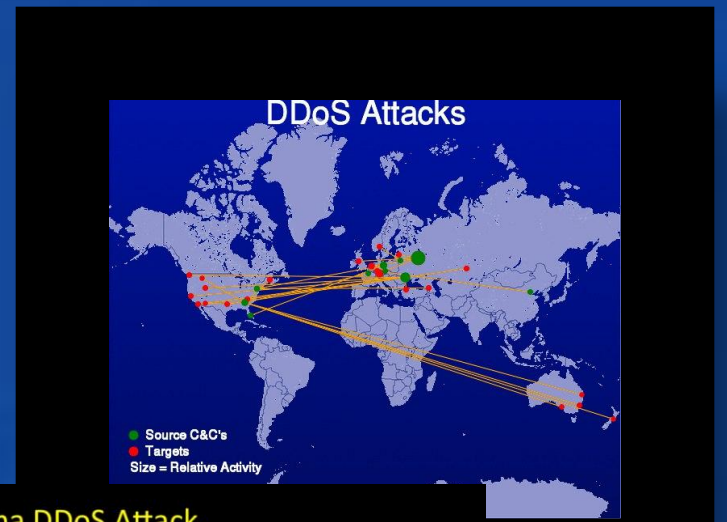
<u>New emerging threat</u>:(Cyber crime future state over past three years)

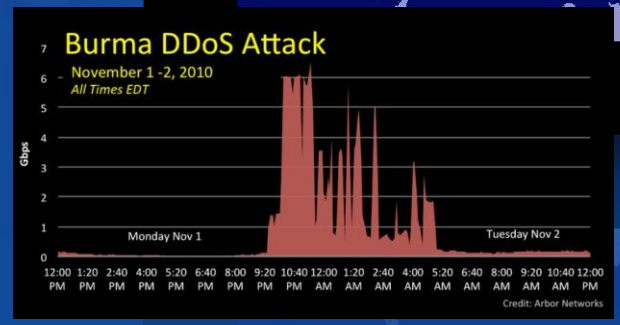
Asymmetric use of the cyber domain including kinetic



TYPES OF CYBER ATTACKS KNOWN TILL NOW

Distributed Denial of Service (DDoS) attack commonly used in attacking banking and government sites.





WE ARE PASS THE DDoS STAGE !

ECIPS Identified four levels of Cyber Terror Capability

1. Simple-Unstructured
2. Advanced-Structured
3. Complex-Coordinated
4. Complex-DoD level

1) Simple-Unstructured:

- The capability to conduct basic hacks against individual systems using tools created by someone else.
- The organization possesses little target analysis, command and control, or learning capability.

2) Advanced-Structured:

- The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools.
- The organization possesses an elementary target analysis, command and control, and learning capability.

3) COMPLEX-COORDINATED:

- The capability for a coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography).
- Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability.

4) Complex-DoD-Leval:

The capability for a coordinated Conflict attacks capable of causing mass-Economical and Government disruption and Shut down. Military standard capability target analysis, command and control.

Cyber Terrorism Targets

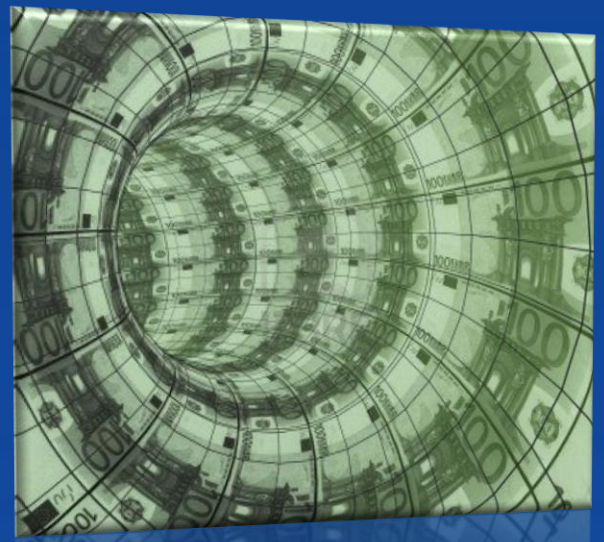
1. Banking
2. Governments
3. Tv Stations
4. Radios
5. Newspapers

and much more !

THE MONEY TREAT –SEUS /SPYEYE

1. Are responsible for around 80% of all attacks against financial Institutions
2. Over $1 billion in global losses since 2010

Organized Crime & Terrorist Group Using Malware.



OBJECTIVE: To Steal Money

1. Get the Money
2. Data theft
3. Bank transfers
4. Stolen passwords
5. Swiped Identities

The Shift: Cyber Terrorism To Cyber-Conflict Capability.

The conflict space has moved to information and cyber space.

The traditional war game IS LOST and the CYBER war has gone viral.

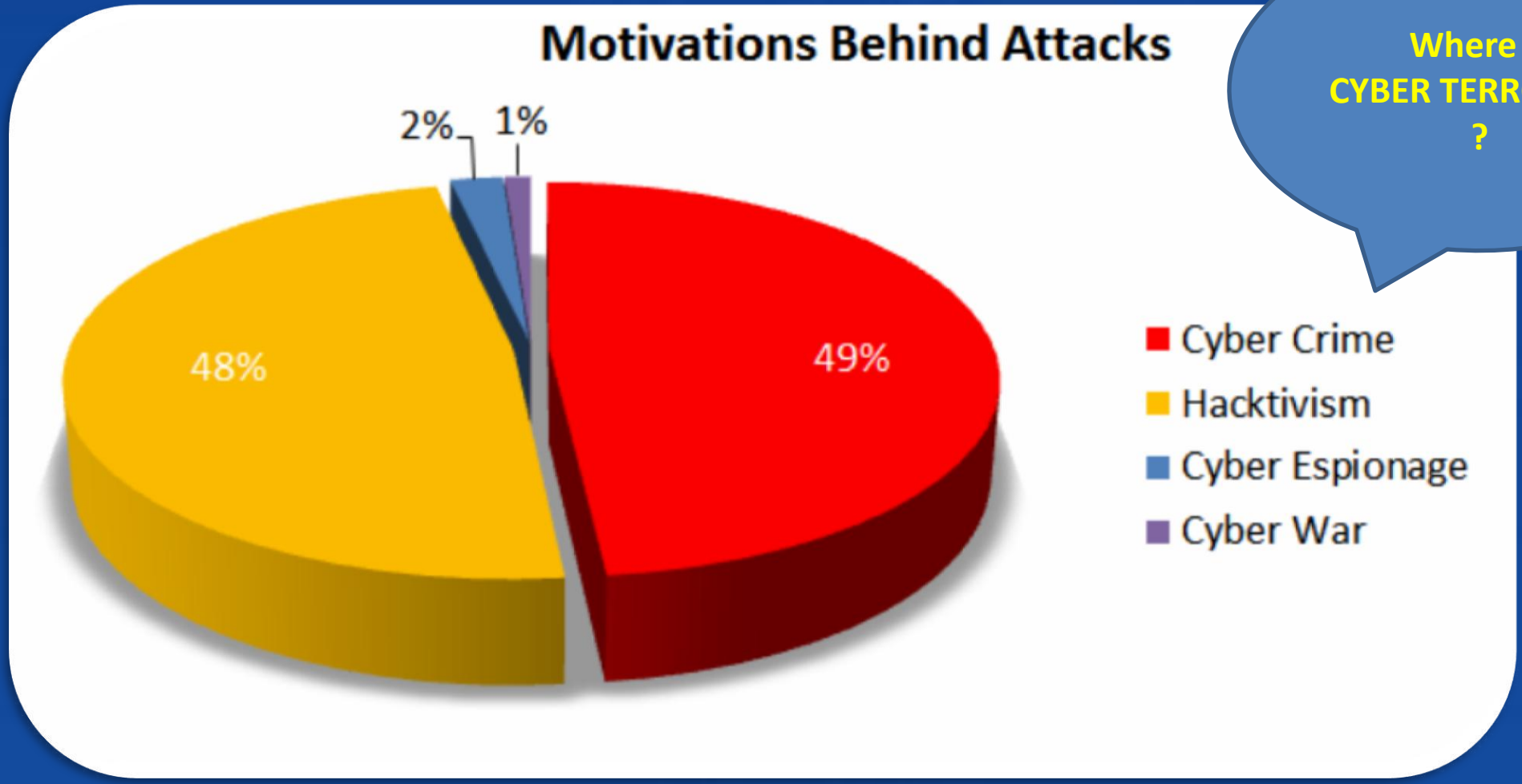
The question is how are we going to solve this ?

You The Audience Vote ?

“Cyber Jihad”

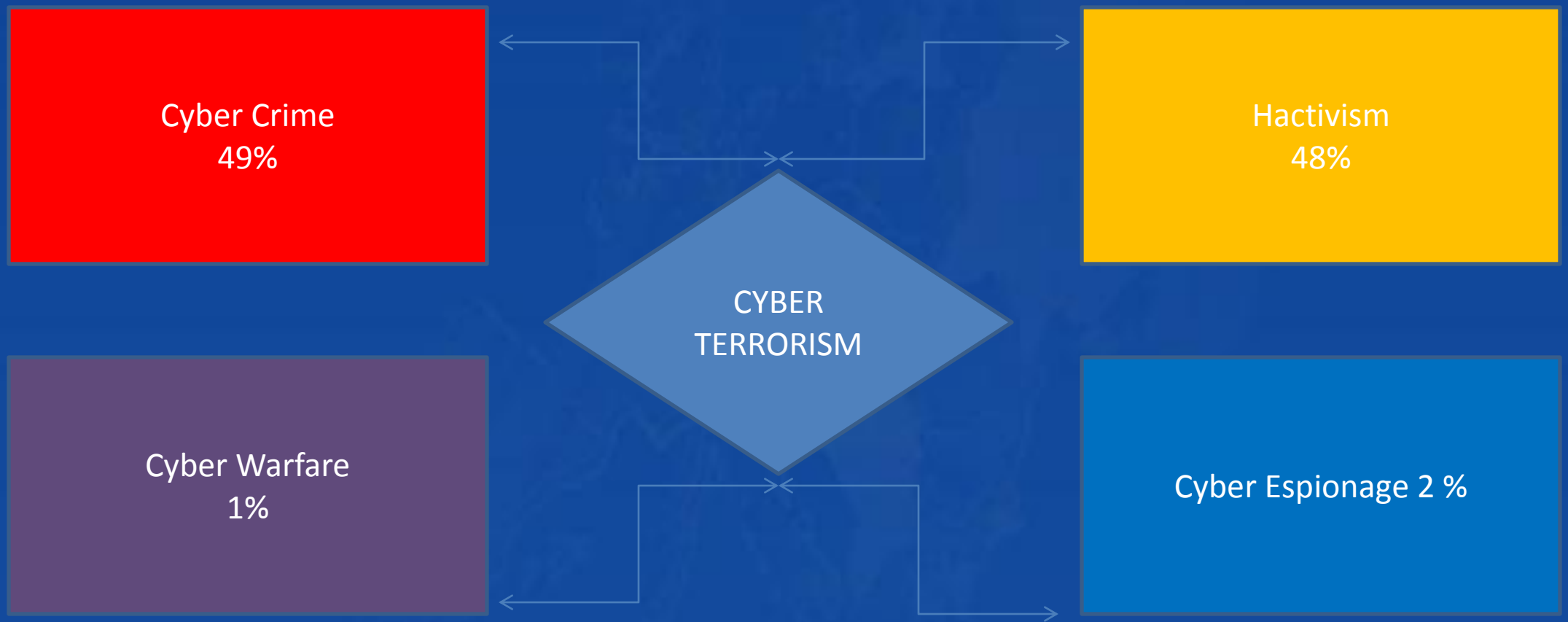
FACT OR ILLUSION

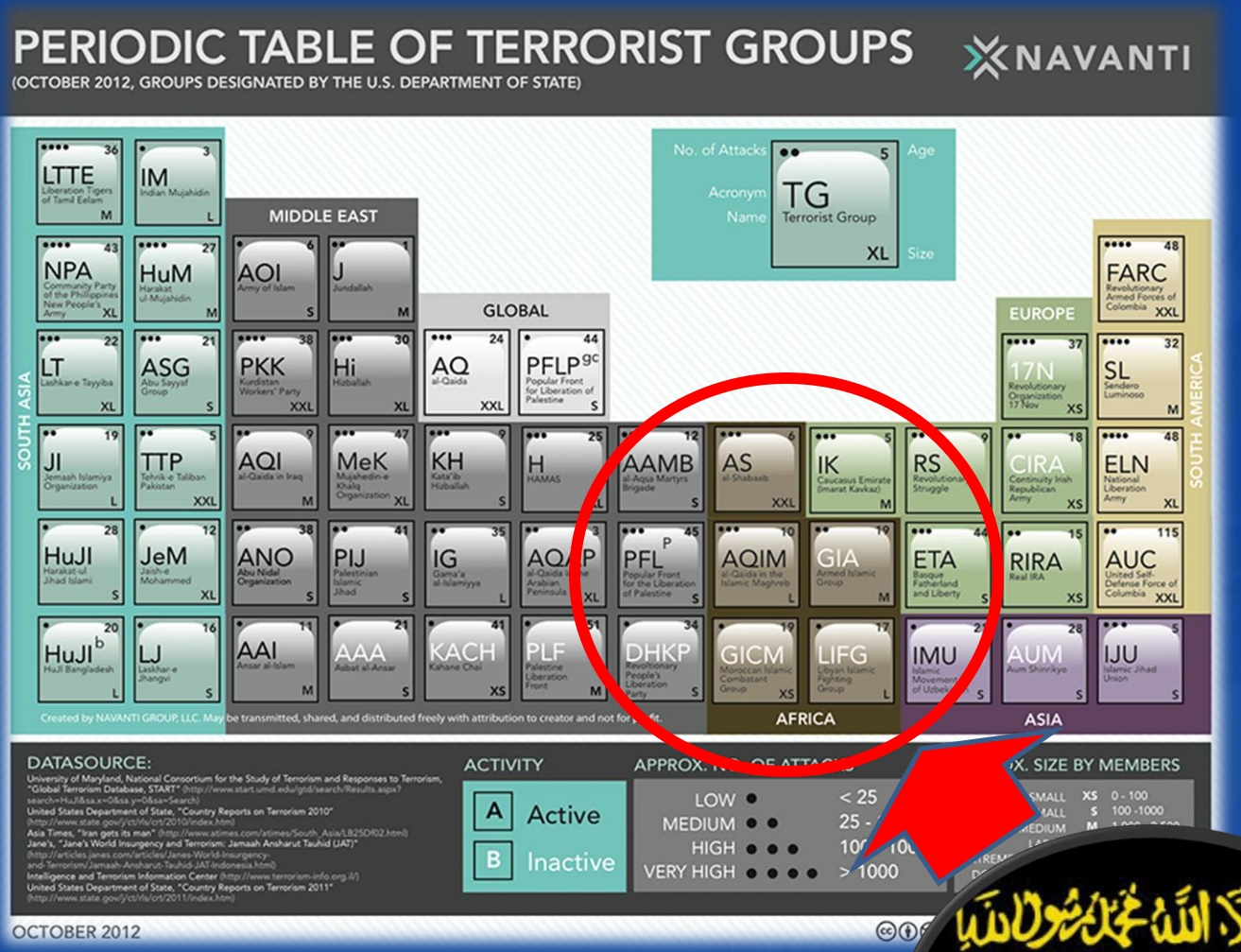
The Motivations Behind Cyber Attacks 2013?



Where is CYBER TERRORISM ?

The "Looming" Hidden Factor





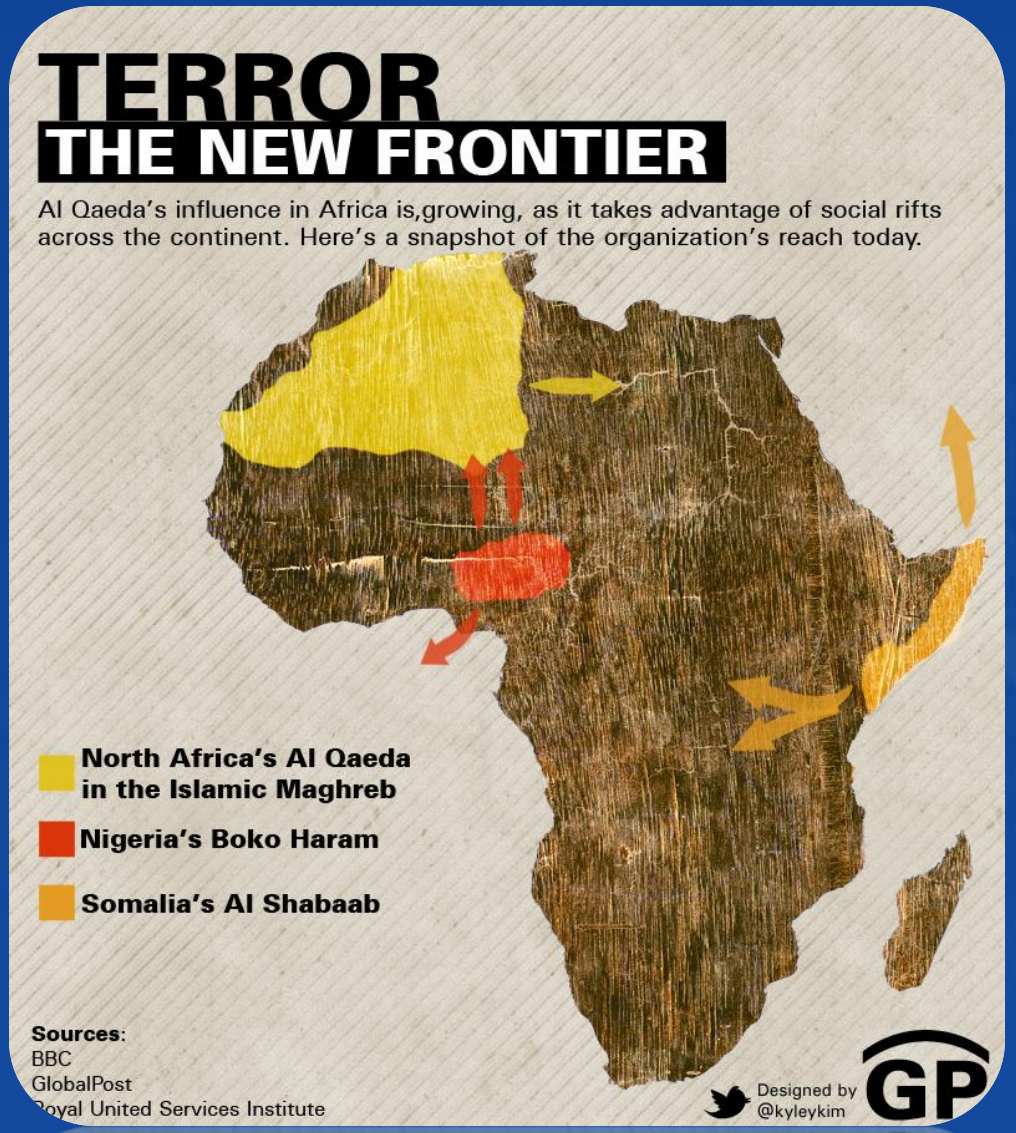
THE FAME !

2012 - Periodic Table of Terrorist Organizations

[infographic] using groups designated by the United States

Department of State.

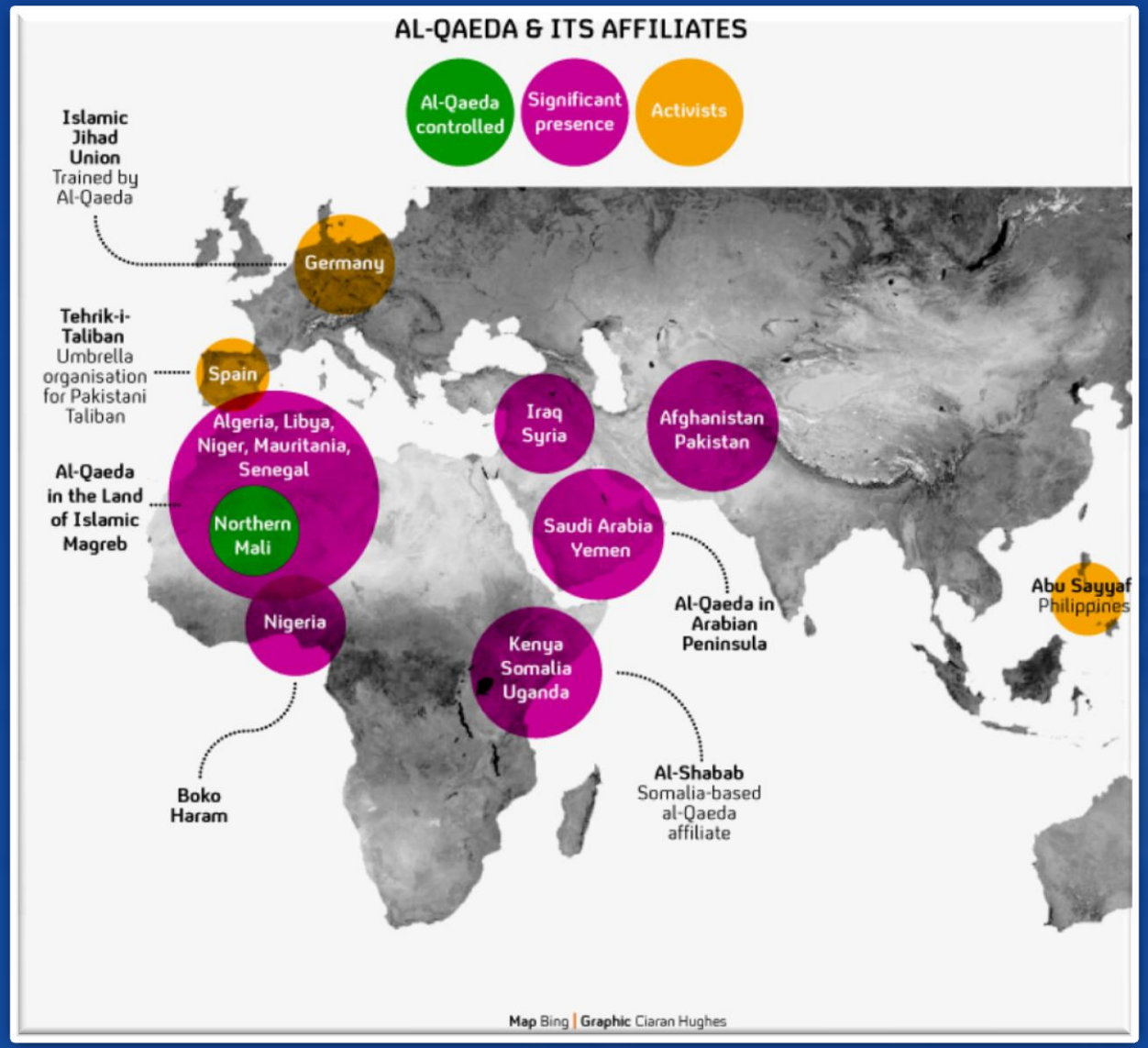
SOUTH ASIA & MIDDLE EAST



AFRICA

The Birth Place of Al-Qaida

Returning "Home"



PRESENT

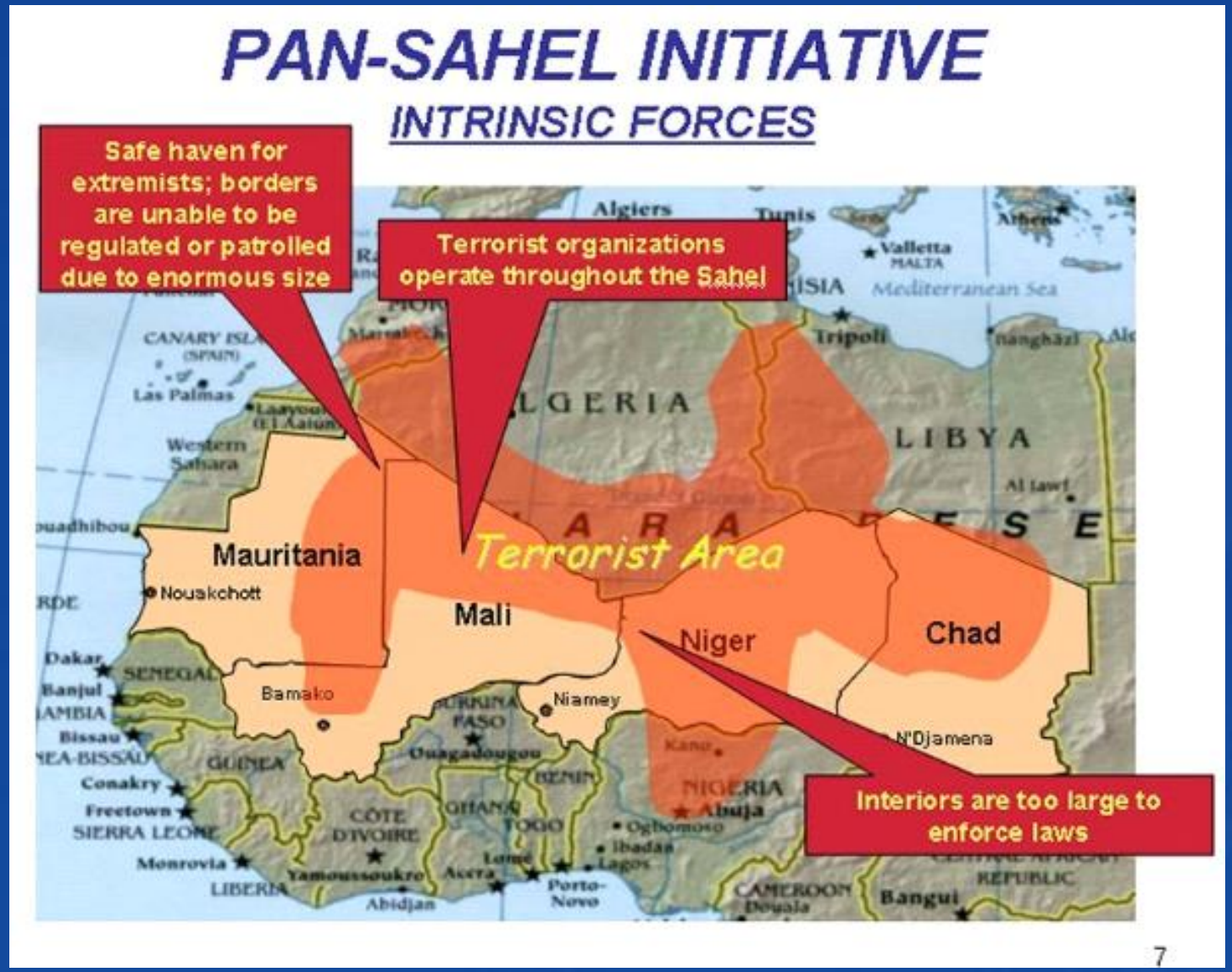
Al-Qaida & Its Affiliates

Do you still think a **'Cyber Jihad'** Is a HOAX ?

Fast Emerging Territories with Cyber and Internet Capability

Africa
Middle-East
South-America

June 4, 2013 USA Intel reports Iranian Terror Cells Infest South America.



WHAT IS THE PROBLEM WITH THIS PICTURE ?

THE CYBER INFRA-STRUCTURE

WHERE WILL CYBER THREAT COME FROM ?

Research indicates that CYBER TERRORIST organizations WILL be FOCUSING on FAST Reliable NEW Emerging Internet Territories to operate from where they have immunity to a large extend and where there is little focus on their activities

"HUH"

ECIPS RESEARCH AND PREDICTIONS INDICATES!

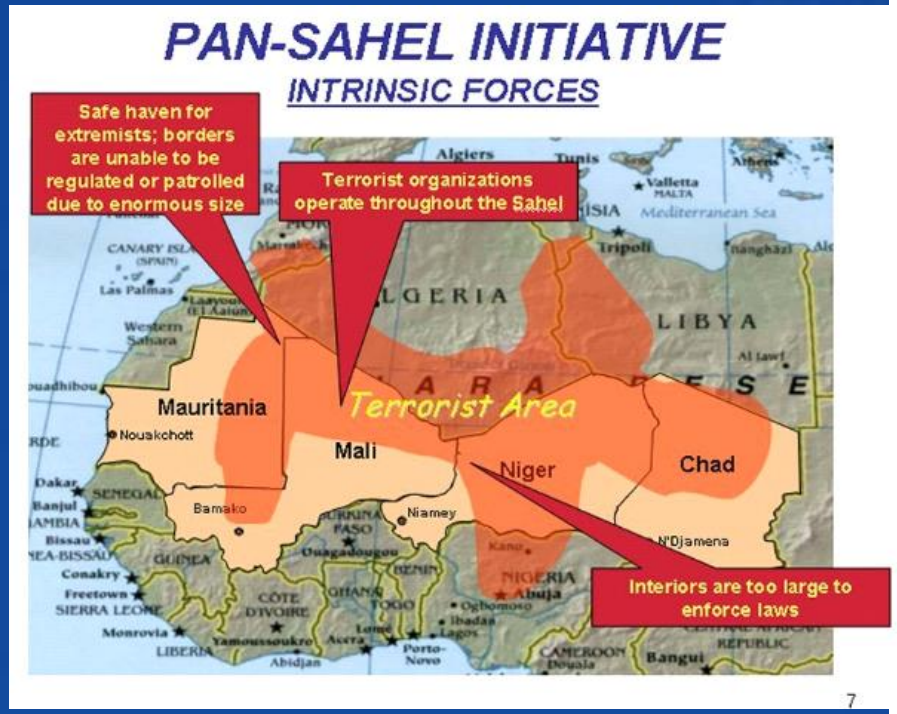
CYB- TER-CELL'S TRENDS TOWARDS ATTRACTIVE CYBER INFRASTRUTURES

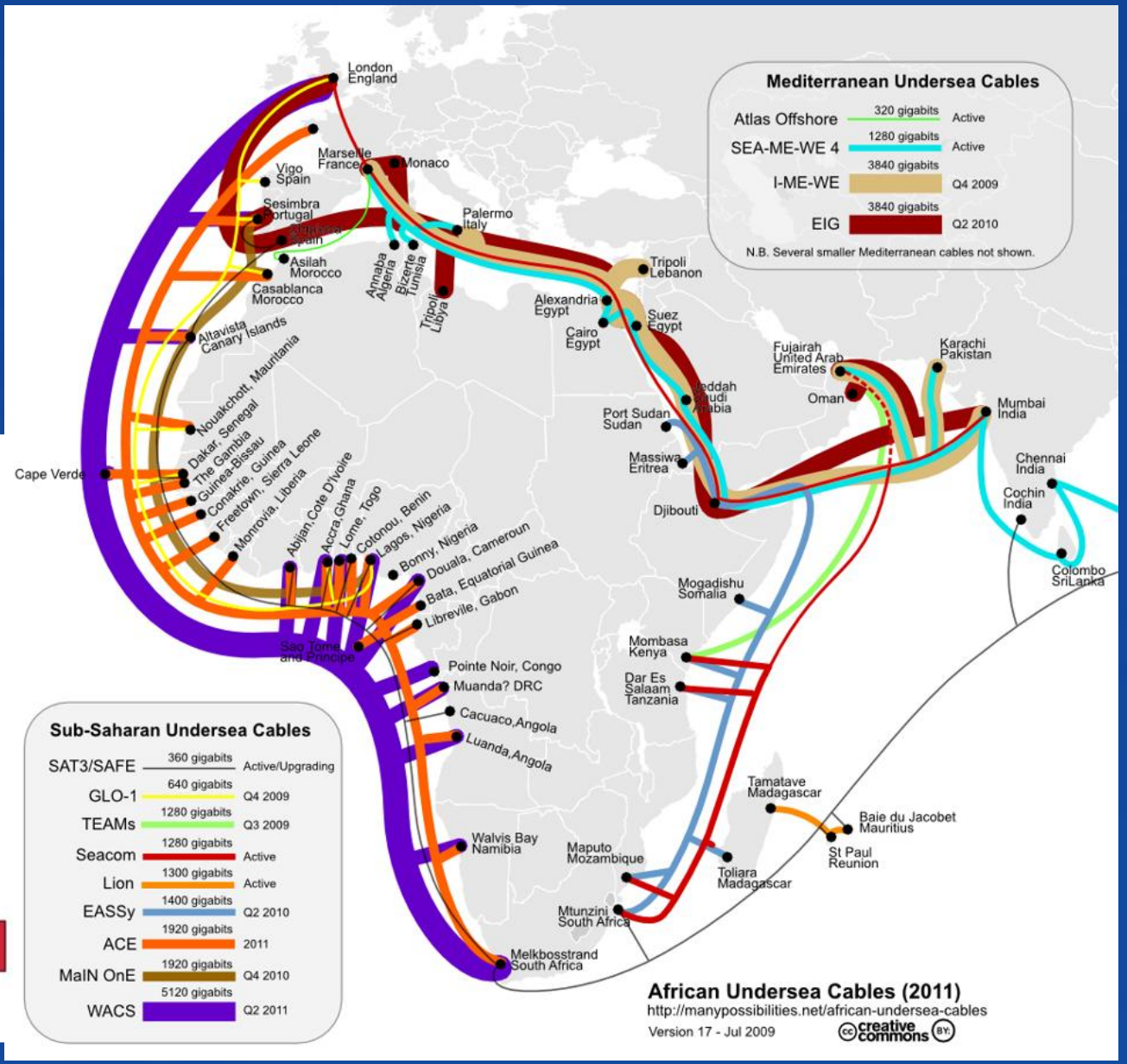
1. Excellent Anonymous Internet capability and access to rest of the world.
2. Access to Banking structure of the US, EU, Asia and Middle East.
3. Access to partial immunity from USA and EU
4. And most important access to financing structures that can't be detected such as the Diamond industry.

CYBER TERRORIST'S OPERATIONAL DESTINATION OPTIONS:

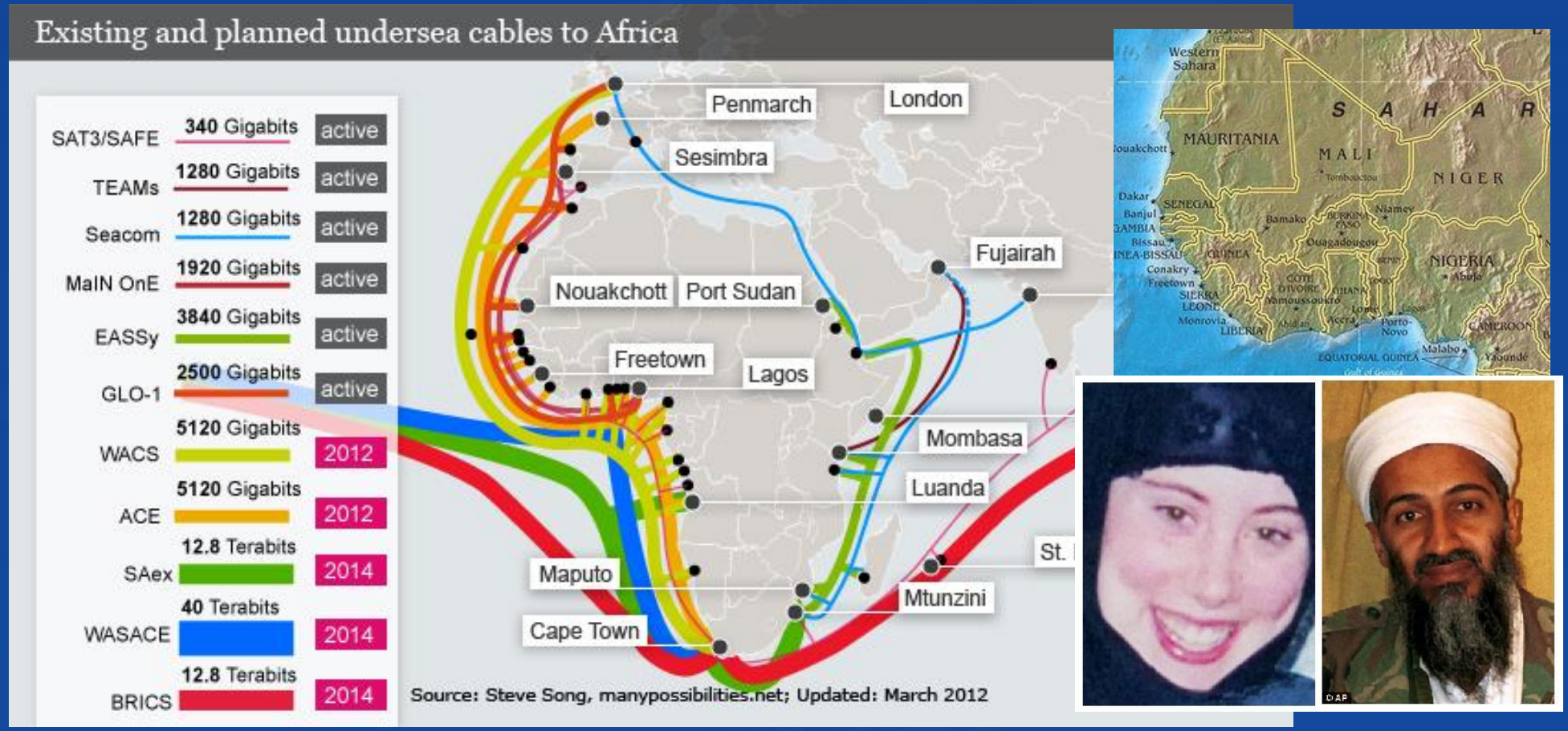
- AFRICA as destination NO 1
- South America as No 2
- South East Asia as No 3
- Russia as NO 4

AFRICAN UNDER-SEA CABLES INTERNET 2011





INTERNET GROWTH AFRICA 2014



*Files found on 'White Widow's'

THE CHANGE OF HIGH-SPEED INTERNET

1. Whole new world of Risks
2. Better anonymity
3. Less visibility

CHANGES EVERYTHING !

AFRICA - NOT EQUIPPED TO COMBAT THIS GROWING PROBLEM

A statement by an Official of the Military Department South Africa said :

"If our military department or any Nuclear facility were to be hacked today, we have no counter measure in place and God knows what will be the result"

The role of Social media

They usually use social media and/or free blog hosting such as Face book or BlogSpot to post information or ideas about jihad.

The Internet is one of the most effective ways for extremists to deliver their messages and find like-minded people.

SOCIAL MEDIA IN 2013

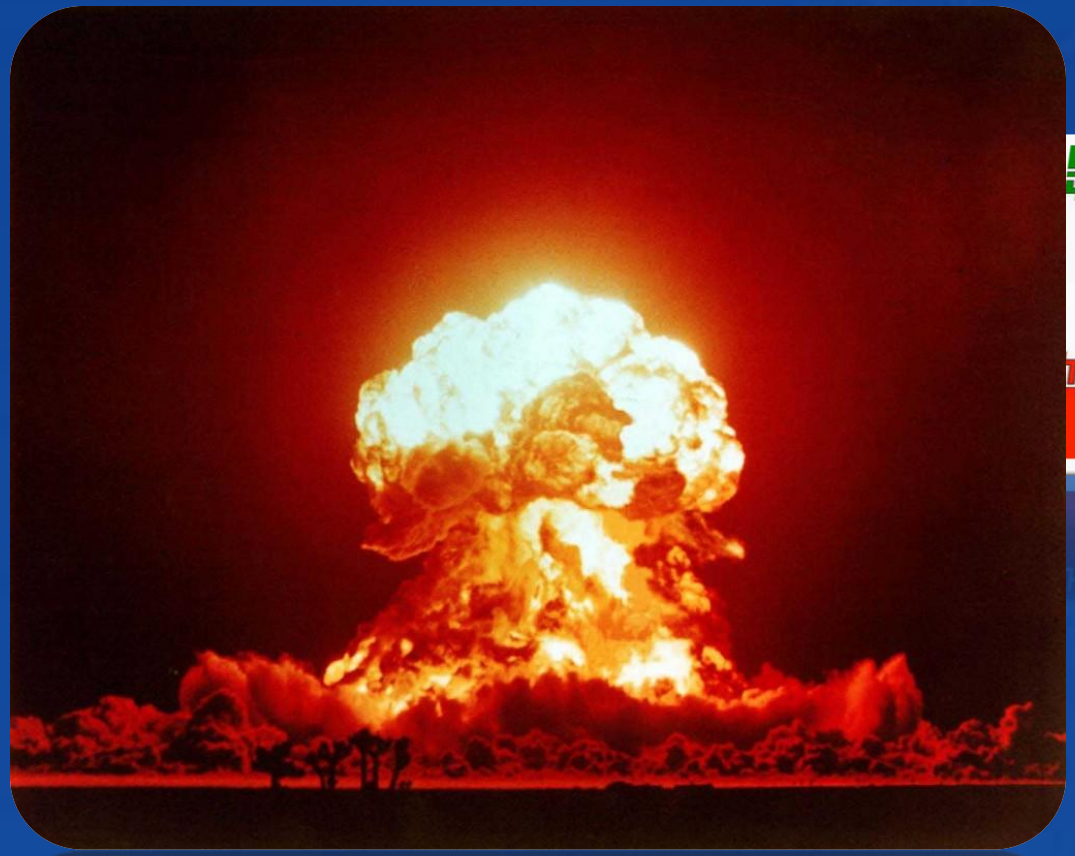
1.61 Billion Users on Social Media Channels in 2013

1/7 OF WORLD POPULATION

The Risk Of an Uncontrolled Social Media Internet Platform.

1. ALLOWS SOCIAL MESSAGING.
2. ALLOWS GROWING CELLS AND THREATS TO EMERGE.
3. ALLOWS GROUPING OF LIKE MINDED POEPLE.
4. INCLUDING GROUPING OF CYBER EXTREAMIST.

Cyber Terror Is the New Language of War!



Combined with Social Media

It's a recipe for disaster

Types of threat attacks that are used by Cyber Terrorist

- Stuxnet is a computer virus that was discovered in June 2010.
- Stuxnet almost ruined one-fifth of the Iranian nuclear centrifuge by spinning out of control while simultaneously replaying the recorded system values which shows the normal functioning centrifuge during the attack

Duqu

Duqu trojan built by 'old school' programmers,

- Duqu is a collection of computer Malware discovered on 1 September 2011, thought to be related to the Stuxnet worm.
- The Laboratory of Cryptography and System Security (CrySyS Lab) of the Budapest University of Technology and Economics in Hungary discovered the threat, analyzed the malware, and wrote a 60-page report.

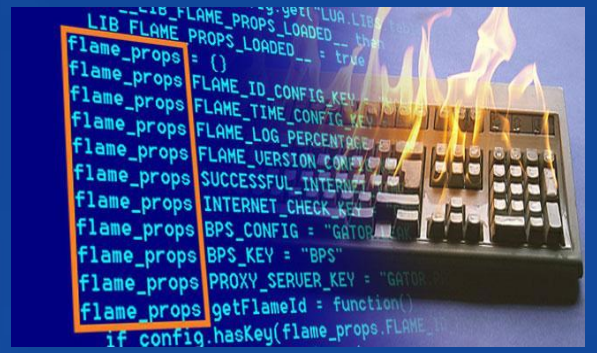
DUQU HAS THE CAPACITY !

Duqu trojan built by 'old school' programmers,

- Duqu has the capacity to steal digital certificates to help future viruses appear as secure software.
- Duqu's replication methods inside target networks remain unknown, however due to its modular structure, a special payload could theoretically be used in further cyber-physical attacks.

Malware Known as Flame is 20 Times the Size of Stuxnet

- Flame is huge: It's about 20 times larger than Stuxnet, the malware that infected Iranian nuclear centrifuges in 2010.
- Flame - is designed to carry out cyber espionage and steal valuable information, including stored files, contact data and audio conversations,

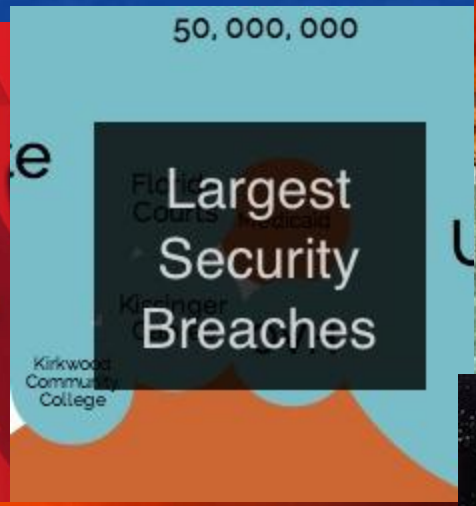


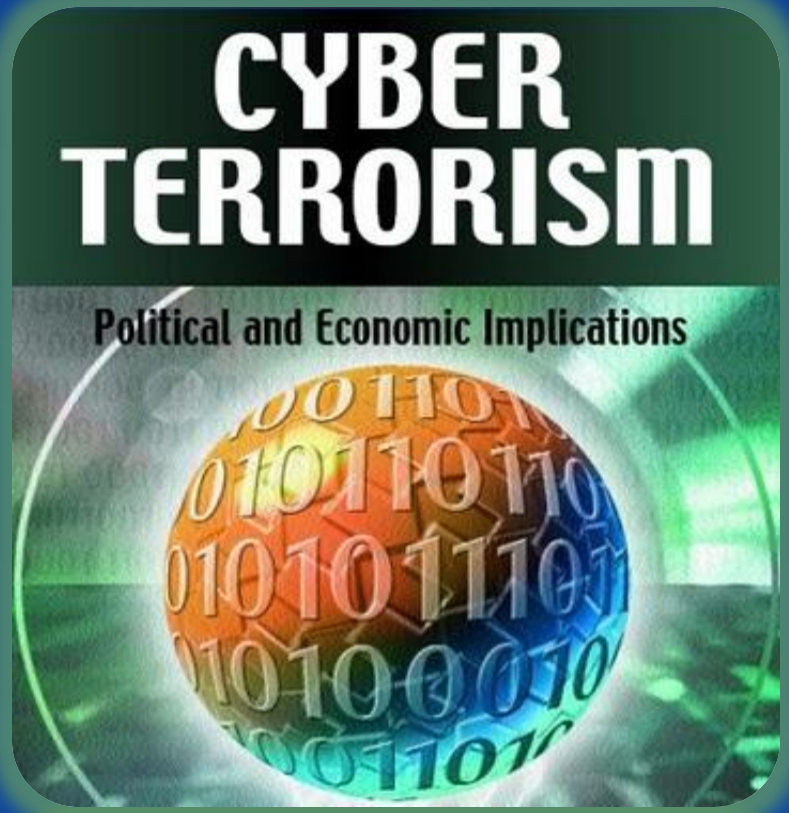
Flame malware was jointly developed by the U.S. and Israeli governments in preparation for a cybersabotage campaign

GAUSS WAS DESIGNED TO STEAL SENSITIVE INFORMATION.

- Gauss was designed to steal sensitive information and was discovered during the ITU investigation into Flame.
- It is believed that the malware has been operating since September **2011** and was uncovered in June **2012**.

IT'S NOT IF, BUT WHEN IT HAPPENS !





CYBER-TERRORISM

What is the Political and Economical Implications if ignoring this threat

!

A GLOBAL CYBER ACCESS PROVIDES TOOLS FOR TERRORIST !

Last Year computer hackers hacked the Twitter account of The Associated Press and sent a tweet stating that there had been two explosions at the White House and that President Barack Obama was injured. Within two minutes, the stock market dropped by 143 points. The Syrian Electronic Army later claimed credit for the attack.

The Risks!

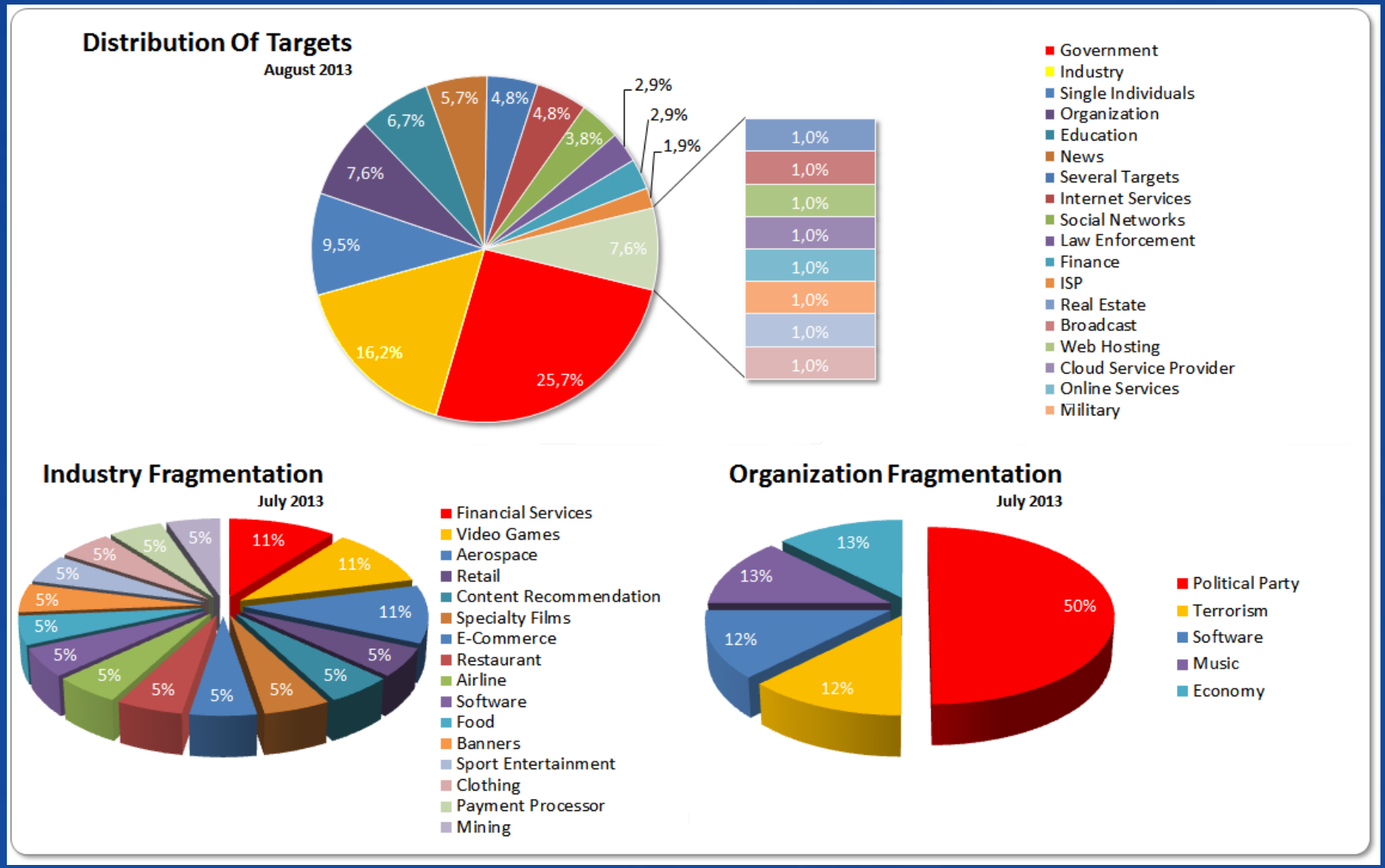
As the world begins to wage warfare in currency markets and programming code, the demand has never been greater for a new international legal framework to rightfully penalize covert provocateurs for manipulating economic structures and engaging in acts of sabotage!

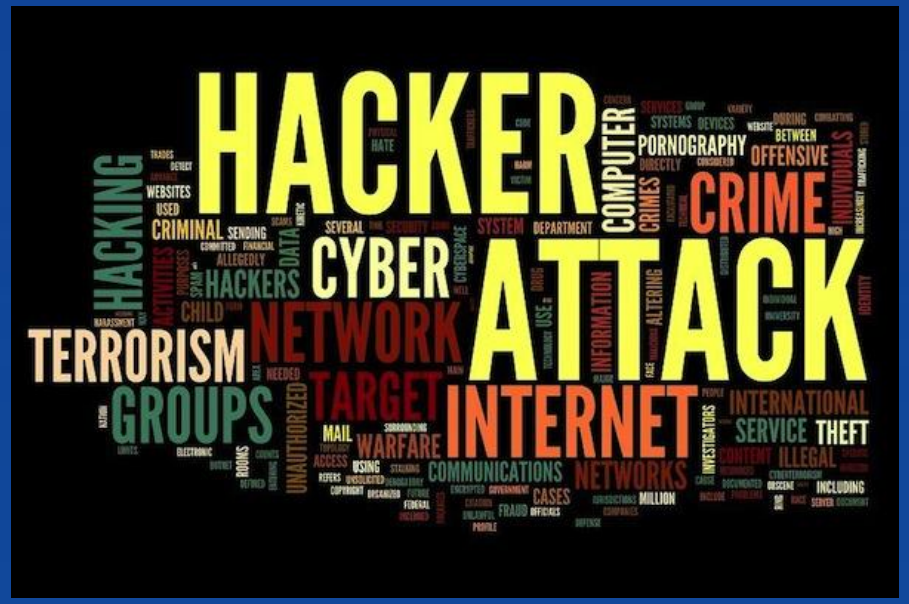
WHATS DOES THE STATISTICS SAY ?

What was the Figure for 2013

93 %

September 2013 Cyber Attacks





The Missing Link ?

What are we missing ?

Why ?

When did we miss it ?

Who is to blame ?

Nobody

Where did we miss it – Internet AGE

R-T-I ?

"Real Time information is Knowledge"

What is R-T-I ?

"HOW DOES THE WORD TRAVEL ? "

CYBERTERRORISM

"How Real is the threat"

What is the word on the street saying ?

What Has Changed in 2013?

Mar 11, 2013 - White House tells China to stop cyber attacks

Apr 23, 2013 Syrian Electronic Army (SEA) Hacked the Associated Press

Aug. 26 2013-Chinese Internet hit by biggest cyber attack in its history

Oct 27, 2013-Israeli tunnel hit by cyber attack

iHLS
Israel's Homeland Security Home

Lab report

Kaspersky Lab report reported-91% of organizations worldwide suffered at least one cyber attack in 2013

ICS Alert

The ICS-Cert, which monitors attacks on computer systems that run industrial processes issued an alert and said "The government was "highly concerned about hostility against critical infrastructure organizations,"

ECIPS ASSESSMENT OF 2014?

ECIPS concluded that 97% of organizations worldwide will suffer at least one cyber attack in 2014

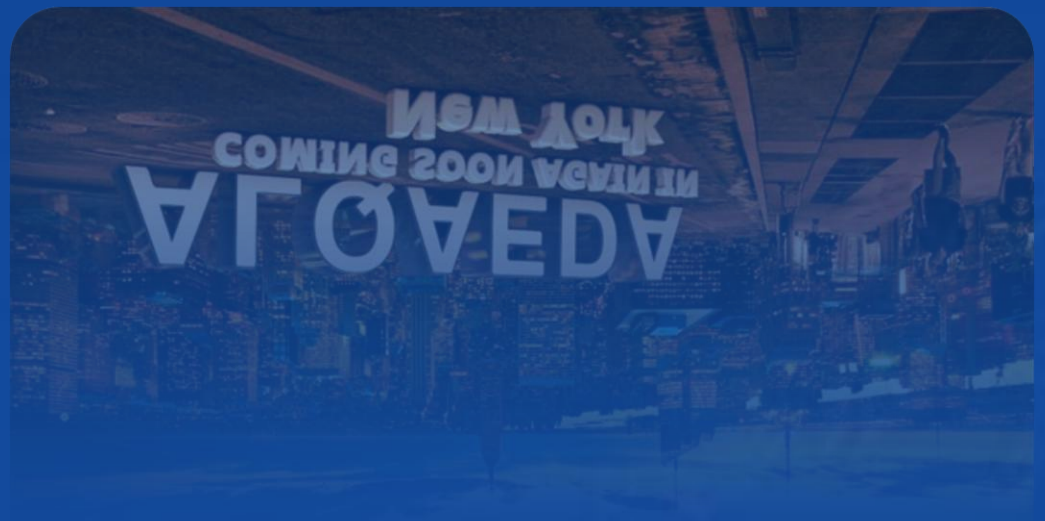
ALARM !

WHAT'S IS AL-QAIDA DOING?

Waiting!

Or Adapting

?



How will Al-Qaida Visit NY?

Are they not already in NY, Paris, London Bruxelles ?

Terrorist Knows !

- The spotlight falls on information gathering,
- The lack of information from the streets, at your fingertips, actionable in *real time*, with *real results*.
- If we had Real Time Information at our finger tips, then Benghazi would not have happened, the Arab Spring would not have the hold of the Middle East as it does today. Iraq, Syria, Turkey and Iran would be settled and stable, instead of rocking all our worlds.

THE WARNING SIGNS ARE WRITTEN ON THE WALLS OF OUR TIME !

The real danger is just around the corner if we are not able to create a strong defense against cyber attacks !

AGE OF THE "QUANTUM TERRORIST"

The age of the "Quantum Terrorist" Has arrived !

THANK YOU !

No Distribution

European Centre for Information Policy and Security (ECIPS) ©
Reg. No 08372076 UK

All legal rights in this regard are strictly reserved.

Distribution and dissemination of any part of this Presentation Slideshow without expressed written consent is a violation of the Treaty of San Francisco, 1945, enforceable in all member nations.

Extradition and prosecution of violators is "at will" and enforced rigorously.

All Information in this presentation contains confidential information and is intended only for the individual/s corporations named. If you are not the named addressee you should not disseminate, distribute or copy this slide show.
Access to this Presentation by anyone else is unauthorized .
If verification is required please email to legal@ecips.eu