

Cyber [Crime|War]

Connecting the dots

Iftach Ian Amit

Managing Partner, Security & Innovation

Agenda

- ✦ Who am I?
- ✦ CyberWar [Attack | Defense]
- ✦ CyberCrime [Attack | Defense]
- ✦ Past events revisited...
 - ✦ Connecting the dots
- ✦ Future

Who Am I



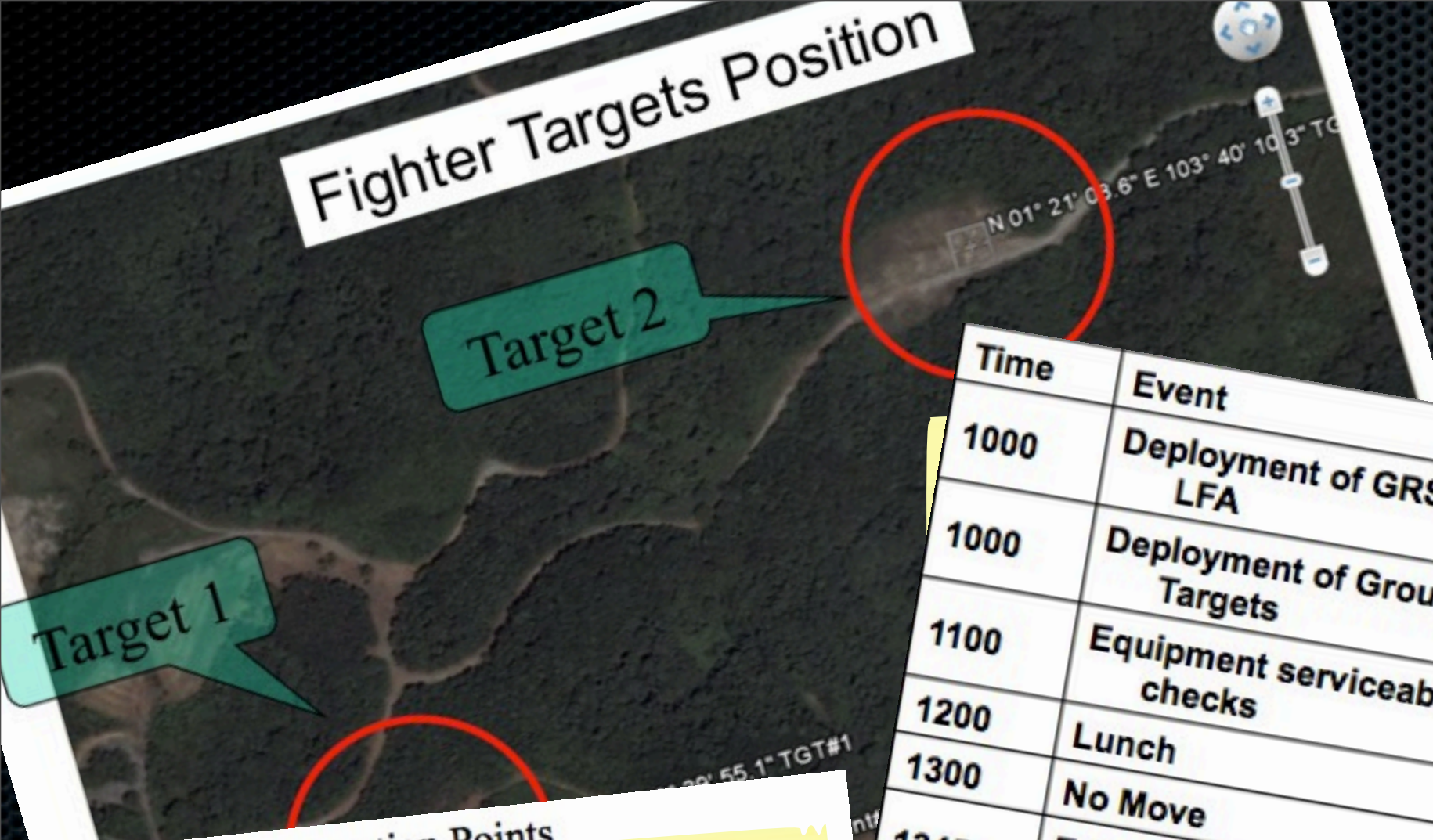
This is NOT going to be



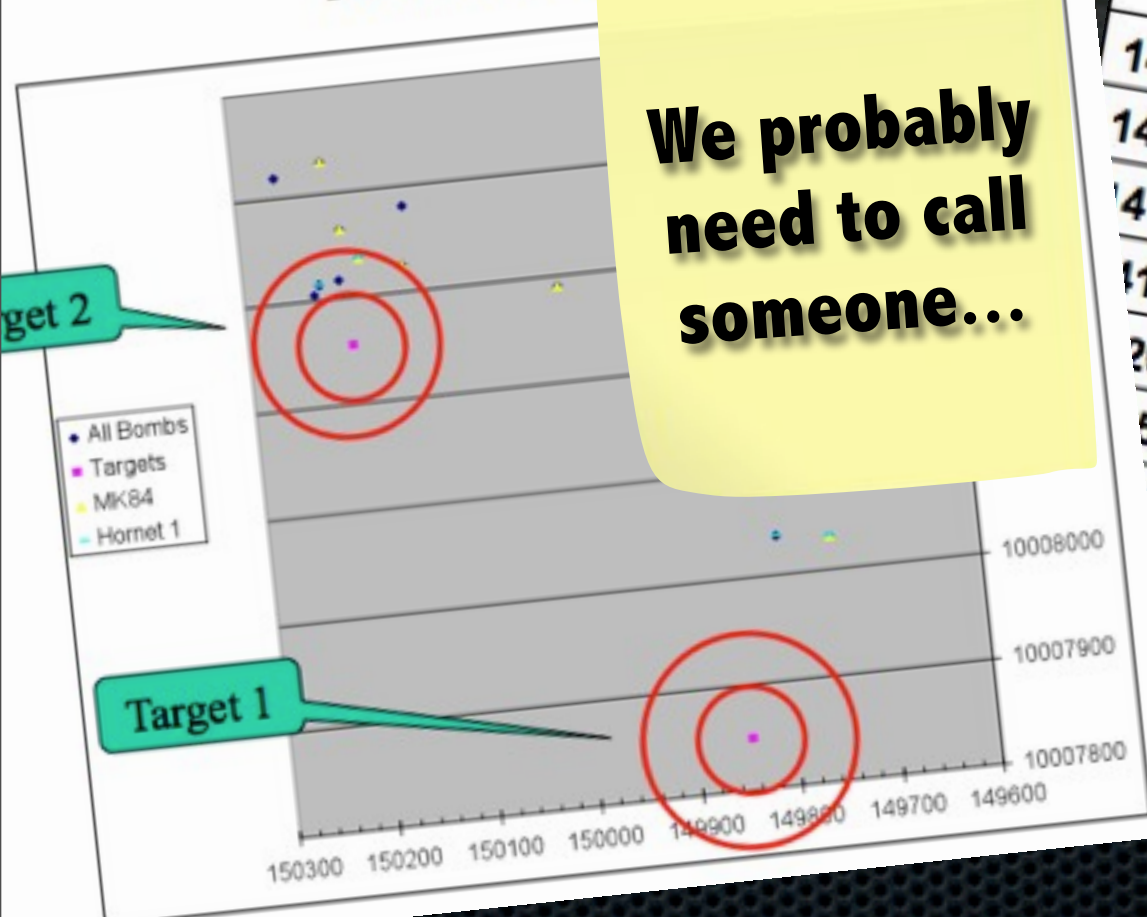
Picking up where we left off

At least as far as last year's research is concerned...

Fighter Targets Position



Detonation Points

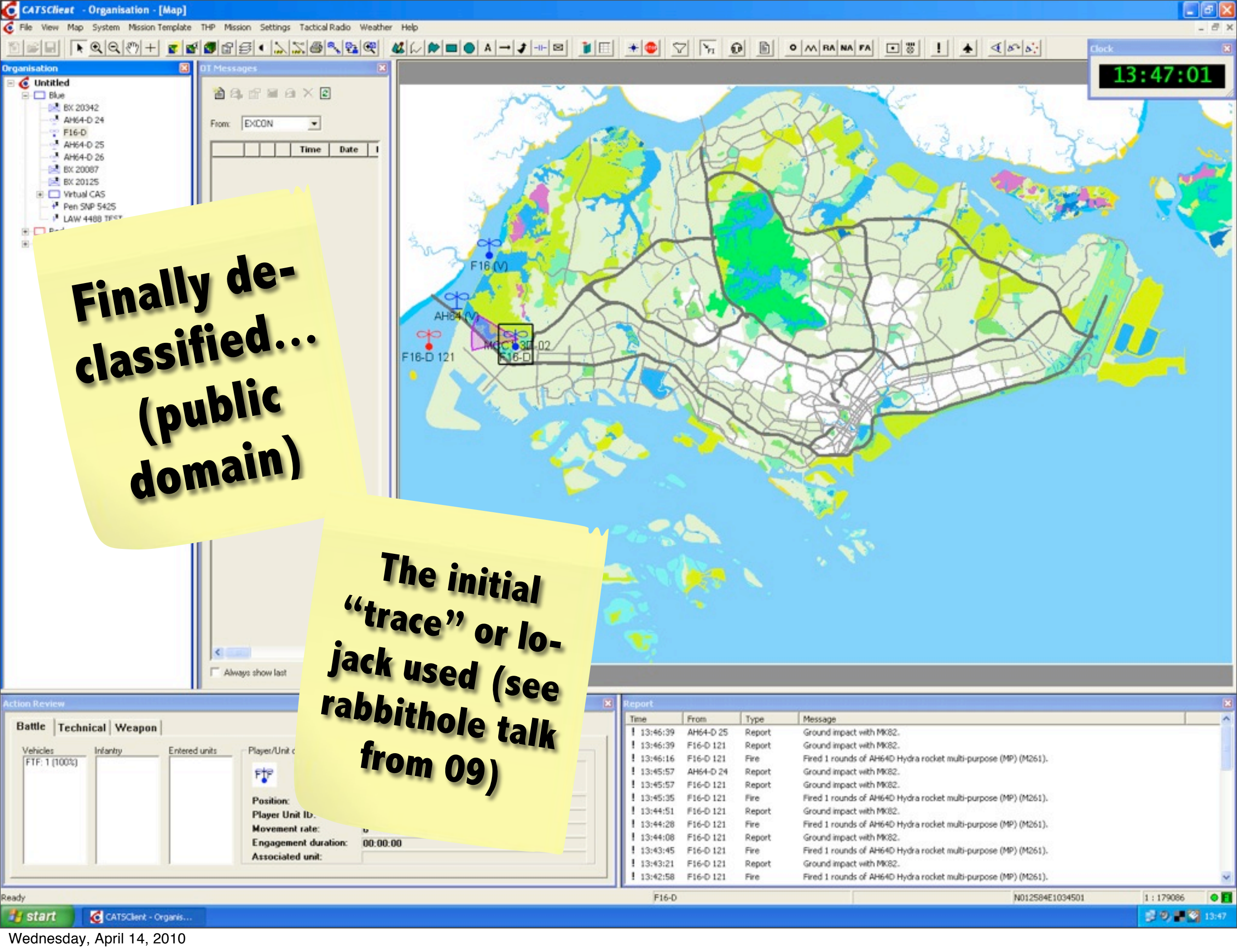


**We probably
need to call
someone...**

Time	Event
1000	Deployment of GRS #9 to LFA
1000	Deployment of Ground Targets
1100	Equipment serviceability checks
1200	Lunch
1300	No Move
1345	Establish comms between MCC and BCDS
1400	F-16 launch
1405	Trial #1
1410	Trial #2
1415	Trial #3a
1420	Trial #3b
1425	Trial #3c
	Recovery of GRS
	Debrief

Pac kag e	Events
1	F-16 bomb drops on ground targets (Mk82, Mk84)
2	F-16 bomb drops on ground targets (Mk82, Mk84)
	Virtual Close Air Support
3a	F-16 bomb drops on ground targets (Mk82, Mk84)
	Ground-to-ground engagements at ALIGN GRS
3b	F-16 bomb drops on ground targets (Mk82, Mk84)
	Ground-to-ground engagements at normal GRS
	F-16 bomb drops on ground targets (Mk82, Mk84)
	Ground-to-ground engagements at ALIGN GRS
	Ground-to-ground engagements at normal GRS

**I think this
is from my
powerpoint!**



**Finally de-
classified...
(public
domain)**

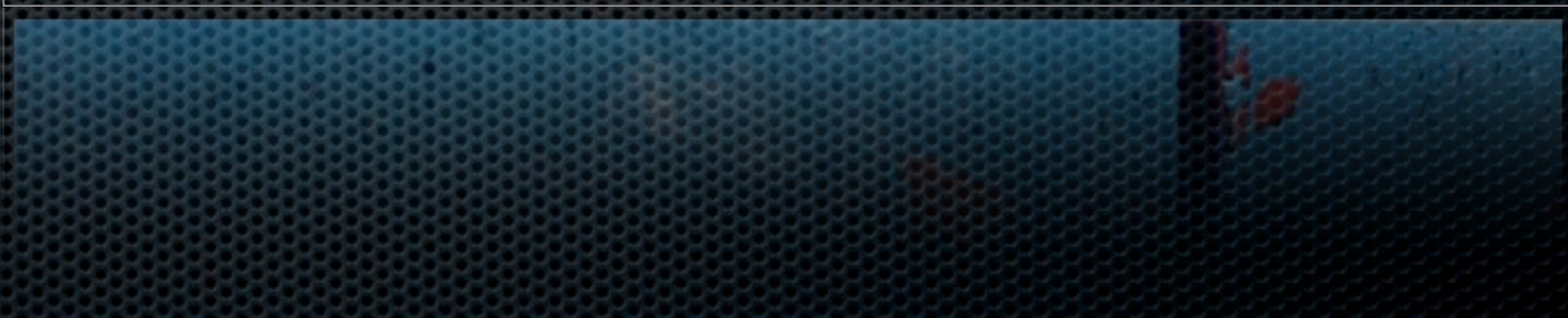
**The initial
"trace" or lo-
jack used (see
rabbithole talk
from 09)**

Time	From	Type	Message
13:46:39	AH64-D 25	Report	Ground impact with MK82.
13:46:39	F16-D 121	Report	Ground impact with MK82.
13:46:16	F16-D 121	Fire	Fired 1 rounds of AH64D Hydra rocket multi-purpose (MP) (M261).
13:45:57	AH64-D 24	Report	Ground impact with MK82.
13:45:57	F16-D 121	Report	Ground impact with MK82.
13:45:35	F16-D 121	Fire	Fired 1 rounds of AH64D Hydra rocket multi-purpose (MP) (M261).
13:44:51	F16-D 121	Report	Ground impact with MK82.
13:44:28	F16-D 121	Fire	Fired 1 rounds of AH64D Hydra rocket multi-purpose (MP) (M261).
13:44:08	F16-D 121	Report	Ground impact with MK82.
13:43:45	F16-D 121	Fire	Fired 1 rounds of AH64D Hydra rocket multi-purpose (MP) (M261).
13:43:21	F16-D 121	Report	Ground impact with MK82.
13:42:58	F16-D 121	Fire	Fired 1 rounds of AH64D Hydra rocket multi-purpose (MP) (M261).

Hungry yet?

This was just the appetizer...

Question 1: What is **this**?



Perceptions may be deceiving...



War



Crime

War

- ✦ Government / state
- ✦ Official backing
- ✦ Official resources
- ✦ Financing
- ✦ Expertise?
- ✦ Exploits/Vulns?

Crime

- ✦ Private
- ✦ semi-official backing
(think organized crime)
- ✦ Official resources
- ✦ Self financing?
- ✦ Established expertise
(in-house + outsourced)
- ✦ Market for exploits

CyberWar

“Cyberwarfare, (also known as cyberwar and Cyber Warfare), is the use of computers and the Internet in conducting warfare in cyberspace.”

Wikipedia

It **did not** happen yet
Estonia being an exception?

“There is no Cyberwar”





This is not the **only** way!

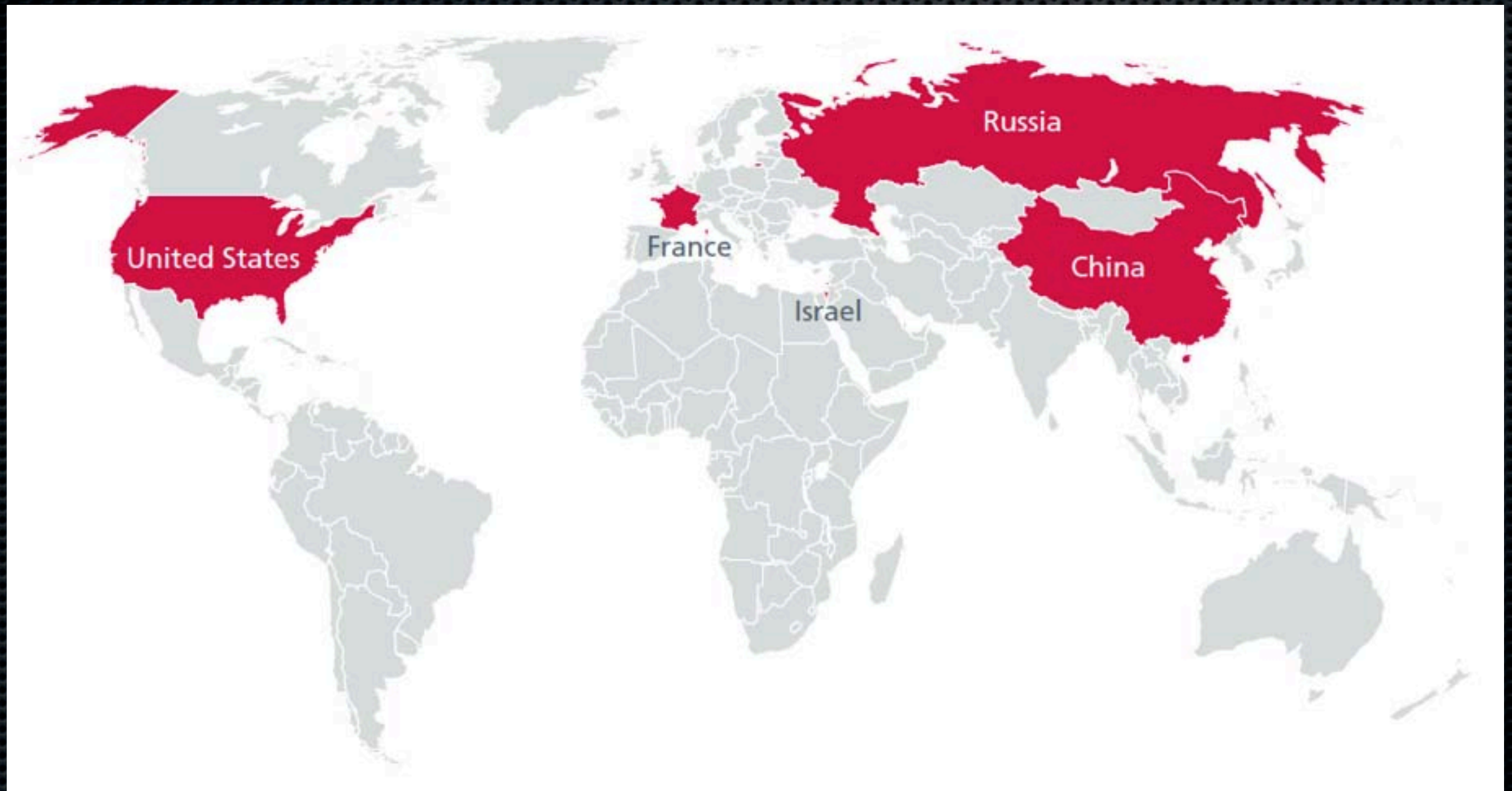


Neither is this...



But civilian are
always at stake!

Many faces of how CyberWar is perceived...

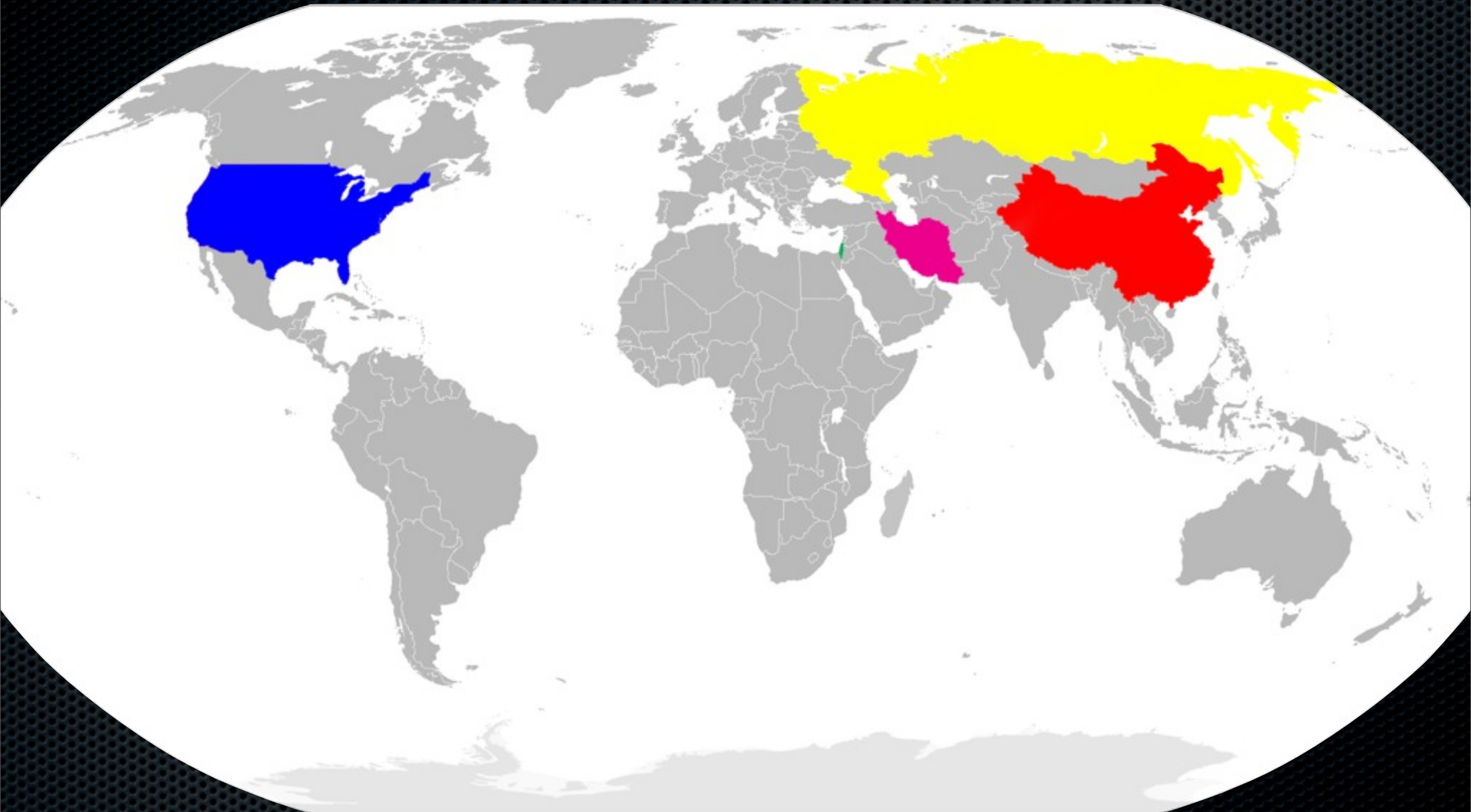


From McAfee's "Virtual Criminology Report 2009"

Image caption:

"countries developing advanced offensive cyber capabilities"

We'll focus on current players:



And no, here size does **NOT** matter...

USA

- Thoroughly documented activity around cyberwar preparedness as well as military/government agencies with readily available offensive capabilities
- Massive recruiting of professional in attack/defense for different departments:
 - USCC (United States Cyber Command - includes AirForce, Marines, Navy and Army service components)
 - NSA
 - Other TLA's...



Russia

- ✦ GRU (Main Intelligence Directorate of the Russian Armed Forces)
- ✦ SVR (Foreign Intelligence Service)
- ✦ **FSB** (Federal Security Services)
- ✦ Center for Research of Military Strength of Foreign Countries
- ✦ Several “National Youth Associations” (**Nashi**)



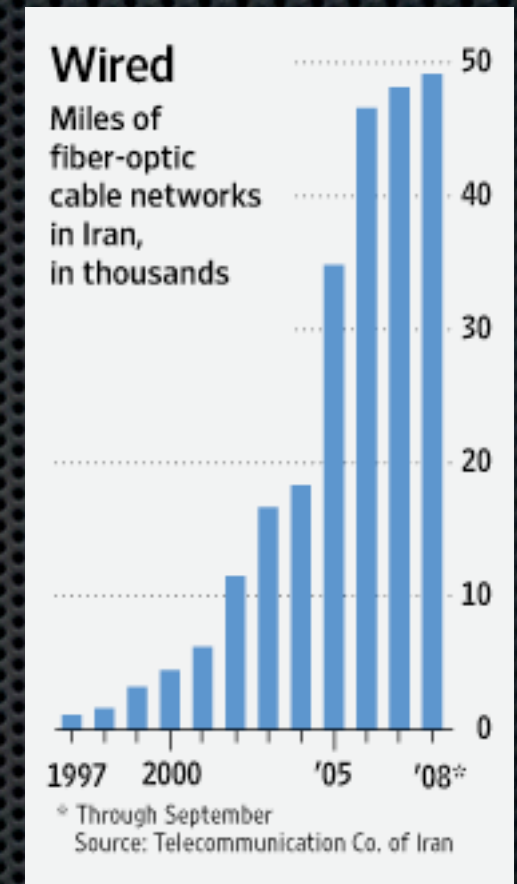
China



- ✦ PLA (People's Liberation Army)
 - ✦ Homework: read the Northrop Grumman report...
 - ✦ General Staff Department 4th Department - Electronic Countermeasures == Offense
 - ✦ GSD 3rd Department - Signals Intelligence == Defense
- ✦ Yes... Titan Rain...

Iran

- ✧ Telecommunications Infrastructure co.
- ✧ Government telecom monopoly
- ✧ Iranian Armed Forces



Israel

Israel Adds Cyber-Attack to IDF

Aviation Week's DTI | David Eshel | February 10, 2010

- ✦ This is going to be very boring... Google data only :-)
- ✦ IDF (Israel Defense Forces) add cyber-attack capabilities.
- ✦ C4I (Command, Control, Communications, Computers and Intelligence) branches in Intelligence and Air-Force commands
- ✦ Staffing is mostly homegrown - trained in the army and other government agencies.
- ✦ Mossad? (check out the jobs section on mossad.gov.il...)

מדינת ישראל • המוסד למודיעין ולתפקידים מיוחדים
STATE OF ISRAEL • ISRAEL SECRET INTELLIGENCE SERVICE



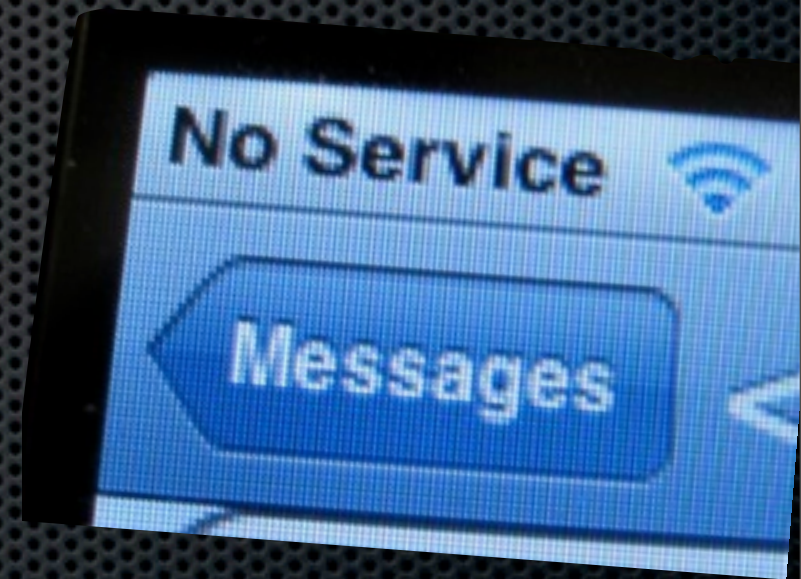
CyberWar - Attack

Highly selective targeting
of **military** (and **critical**)
resources

In conjunction with a
kinetic attack

OR

Massive **DDOS** in order to
“black-out” a region,
disrupt services, and/or
push political agenda
(**propaganda**)



CyberWar - Defense

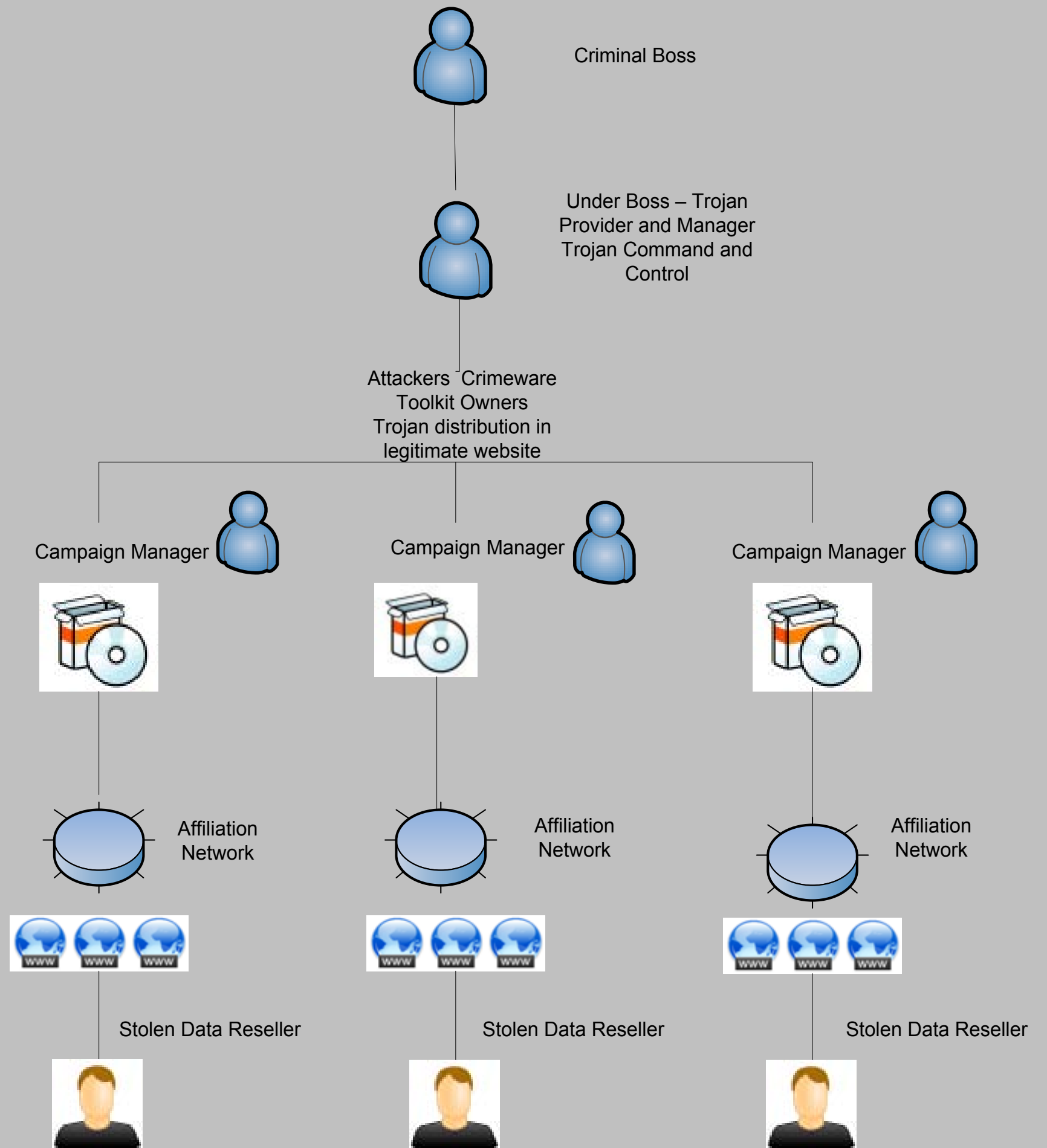
- ✦ Never just **military**
 - ✦ Targets will be **civilian**
- ✦ Physical and logical protections = last survival act
- ✦ **Availability** and **Integrity** of services
 - ✦ Can manifest in the cost of making services **unavailable** for most civilians



CyberCrime



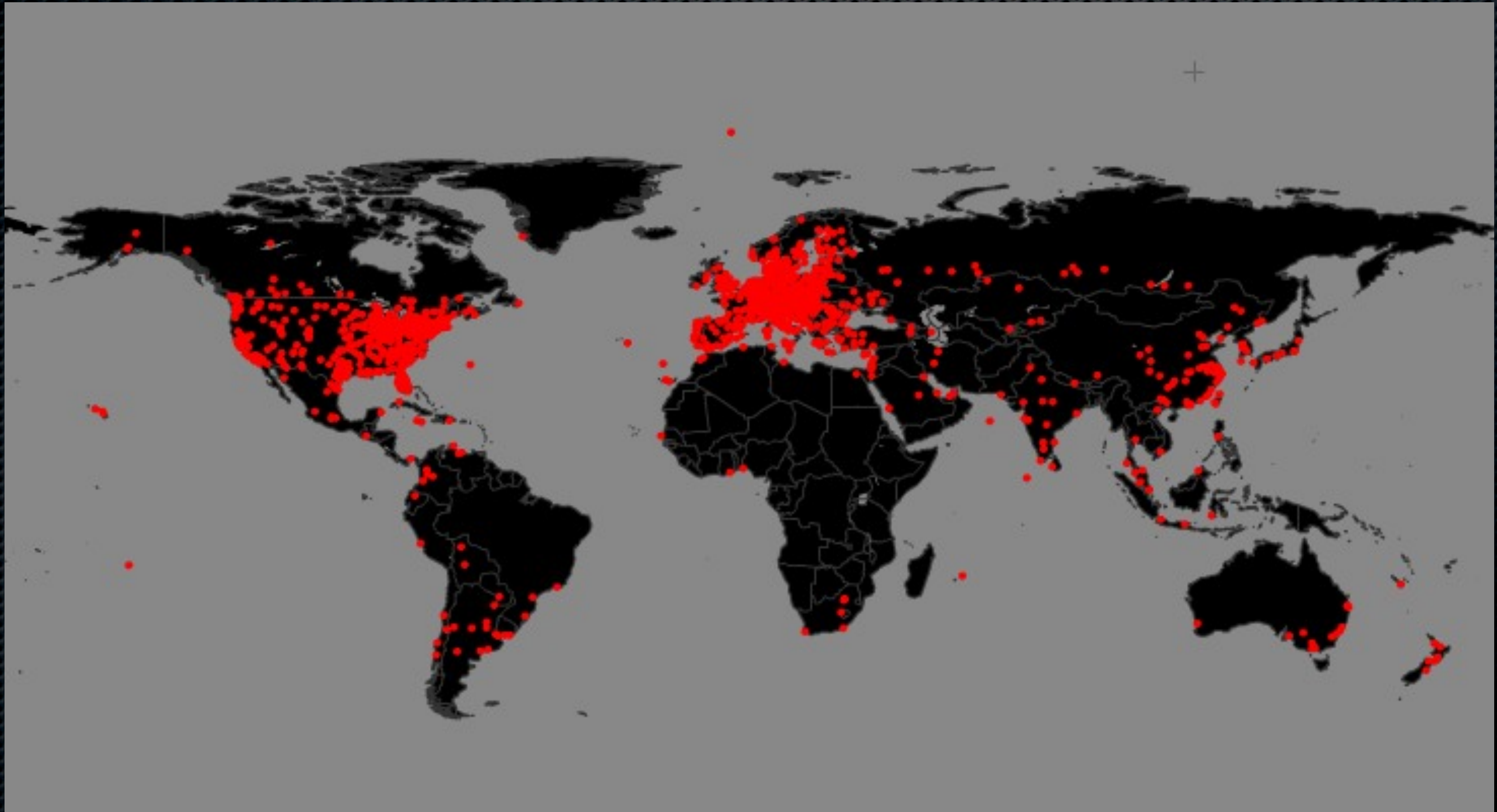
You want
money, you
gotta play like
the big boys
do...



CyberCrime - Attack

- ✦ Channels: web, mail, open services
- ✦ Targeted attacks on premium resources
 - ✦ Commissioned, or for extortion purposes
- ✦ Carpet bombing for most attacks
 - ✦ Segmenting geographical regions and market segments
- ✦ Secondary infections through controlled outposts
 - ✦ Bots, infected sites

CyberCrime - target location

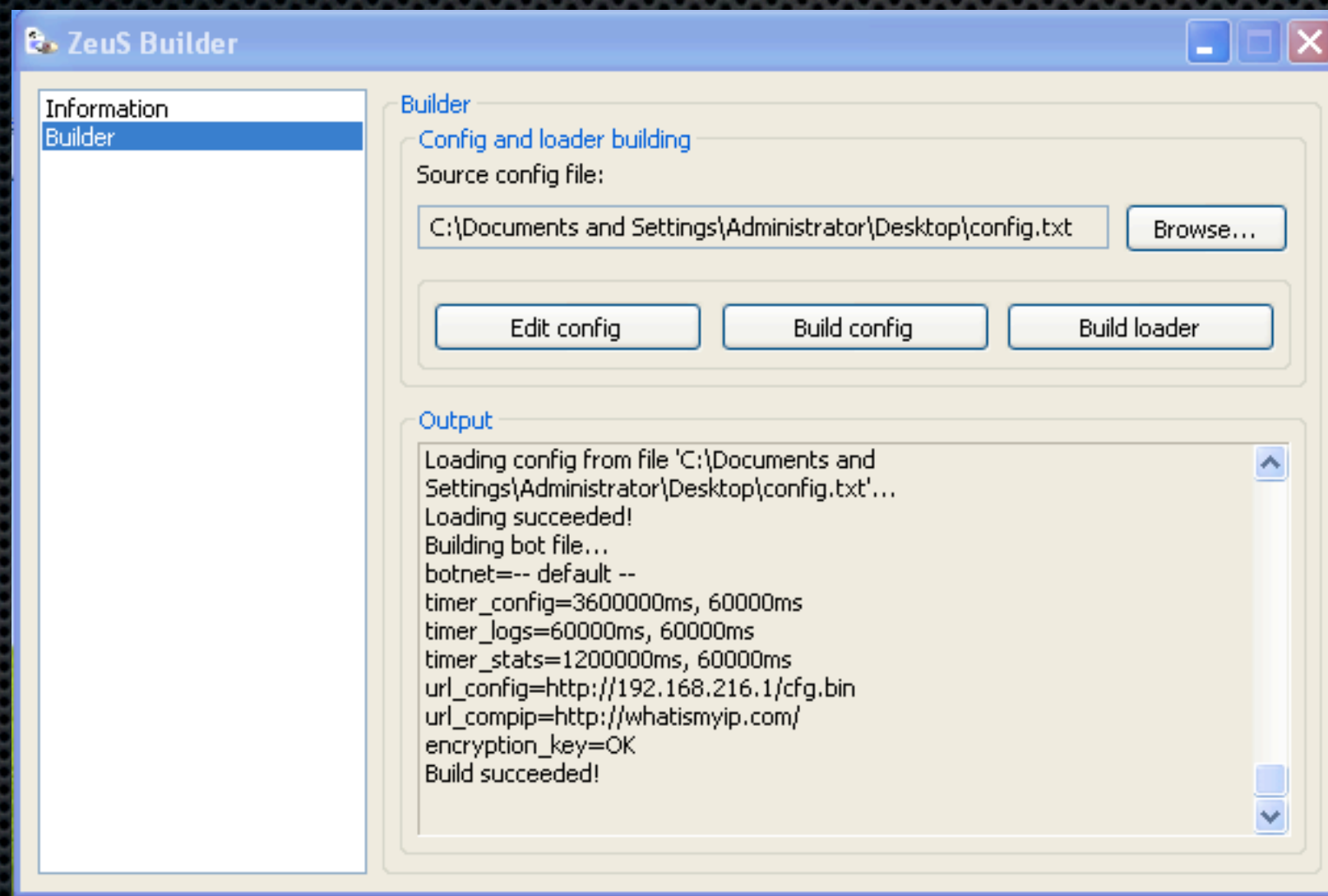


CyberCrime - Locations



Major Cybercrime group locations

CyberCrime - Ammunition



== APT

Zeus :: Statistics

Information:

Profile: icen
GMT date: 24.04.2008
GMT time: 22:11:51

Statistics:

→ Summary

Botnets:

Profile: icen
GMT date: 24.04.2008
GMT time: 22:14:03

Online:

Remote:

Logs:

Summary
→ Online bots
Remote commands
Uploads

System:

Search
Search with template
Uploaded files

Profile:

Options:

Profiles
Profile
Options

Logout:

Logout

Information

Total logs in database: **203**
Time of first install: **16:10:06 26.03.2008**
Total bots: **535**

Zeus :: Bots

Information:

Profile: icen
GMT date: 24.04.2008
GMT time: 22:14:03

Statistics:

Summary

Botnet:

→ Online bots
Remote commands

Logs:

Search
Search with template
Uploaded files

System:

Profiles
Profile
Options

Logout

Filter

Countries: CompID's:
Botnets: IP's:

Type:

Result:

#	CompID	Ver/Botnet	IP	Country	Socks	Proxy	Screenshot	Online time	Speed
1	home_5hm79aabb8_18ff5887	1.0.3.7/0	66.20.176.219	US	-	-	-	28:14:42	0
2	home_00e01ec4	1.0.3.7/0	70.189.43.6	US	-	-	-	28:14:49	0
3	e58aeb3f9a6342e_0005cf1f	1.0.3.7/0	76.6.28.134	US	-	-	-	00:59:12	1.015
4	s0026776334_03c9bf3f	1.0.3.7/0	71.88.41.203	US	-	-	-	11:00:04	0.172
5	home_cxl7f5jivt_3a19fa48	1.0.3.7/0	65.190.70.193	US	-	-	-	28:15:35	0
6	gabrail_00ebef3b	1.0.3.7/0	75.187.190.246	US	-	-	-	28:15:18	0
7	mvd_00151288	1.0.3.7/0	66.24.74.225	US	-	-	-	03:56:03	0
8	hicks_07ca460dc_0002c847	1.0.3.7/0	74.47.178.92	US	-	-	-	28:14:55	0
9	e519887_04d635e3	1.0.3.7/0	130.76.32.145	US	-	-	-	28:15:15	2.353
10	home_039e4185	1.0.3.7/0	67.49.216.74	US	-	-	-	24:28:25	0
11	your_co2y48tgdl_21540d33	1.0.3.7/0	70.180.173.188	US	-	-	-	03:28:31	0
12	wa5117d01_007de927	1.0.3.7/0	63.164.145.198	US	-	-	-	23:19:11	0
13	hewlett_lydtpep_000d1b7d	1.0.3.7/0	67.175.12.135	US	-	-	-	06:04:26	0
14	e107306_00a67fc7	1.0.3.7/0	130.76.32.182	US	-	-	-	28:14:16	2.484
15	judy_1f2c4509	1.0.3.7/0	74.227.149.82	US	-	-	-	25:44:29	0
16	cadet64204_77f68ea1	1.0.3.7/0	68.58.242.15	US	-	-	-	00:24:09	0
17	central_y7uq1of_03fc9672	1.0.3.7/0	206.71.208.121	US	-	-	-	07:03:20	0
18	bryan_pc_3e13a078	1.0.3.7/0	70.88.25.241	US	-	-	-	01:52:39	0.172
19	winxp_00023fa1	1.0.3.7/0	69.246.194.0	US	-	-	-	28:15:32	0.27
20	wa5117d02_0027e2a1	1.0.3.7/0	63.164.145.198	US	-	-	-	28:15:34	0
21	private_45878f3_000622ad	1.0.3.7/0	76.68.150.19	US	-	-	-	00:46:55	0
22	rekles_xtyg9nbe_17f5b01f	1.0.3.7/0	75.178.3.31	US	-	-	-	28:14:41	0
23	tony_f740f48227_00b21f7c	1.0.3.7/0	24.247.72.95	US	-	-	-	03:55:35	60.093
24	owner_f835edf4c_0003ffbe	1.0.3.7/0	65.12.138.38	US	-	-	-	03:14:38	0
25	take_2067du80ff_1c1dbf98	1.0.3.7/0	75.100.193.124	US	-	-	-	28:14:39	0
26	s0026403620_01f62ef5	1.0.3.7/0	74.197.114.250	US	-	-	-	00:02:54	0.219
27	lovefamily_000d186a	1.0.3.7/0	71.180.88.97	US	-	-	-	02:30:50	0
28	hub_lab_11_0000dadf	1.0.3.7/0	68.190.65.92	US	-	-	-	00:46:12	0
29	fariba_05744139	1.0.3.7/0	75.56.211.191	US	-	-	-	28:15:26	0
30	dorm_0002de02	1.0.3.7/0	74.170.82.94	US	-	-	-	08:40:34	0
31	d5wccbb1_0005840c	1.0.3.7/0	72.149.8.2	US	-	-	-	05:54:22	0

CyberCrime - Defense

- ✦ Anti [Virus | Malware | Spyware | Rootkit | Trojan]

- ✦ Seriously?

File 90a4ab818f492d67a8c1d5efae8e2147f received on 2010.03.16 16:58:07
(UTC)
Current status: **finished**
Result: **0/42 (0.00%)**

- ✦ Firewalls / IDS / IPS

- ✦ Seriously?

- ✦ Brought to you by the numbers 80, 443, 53...
 - ✦ SSL...

How do these connect?

Claim: **CyberCrime** is being *used* to
conduct **CyberWar**

Proof: Let's start with some *history*...

History - Revisited...

Estonia

You read all about it.

Bottom line: **civilian** infrastructure was targeted
Attacks originated mostly from **civilian** networks

History - Revisited...

Israel

Cast led

2nd Lebanon war

Palestinian TV hacked - propaganda



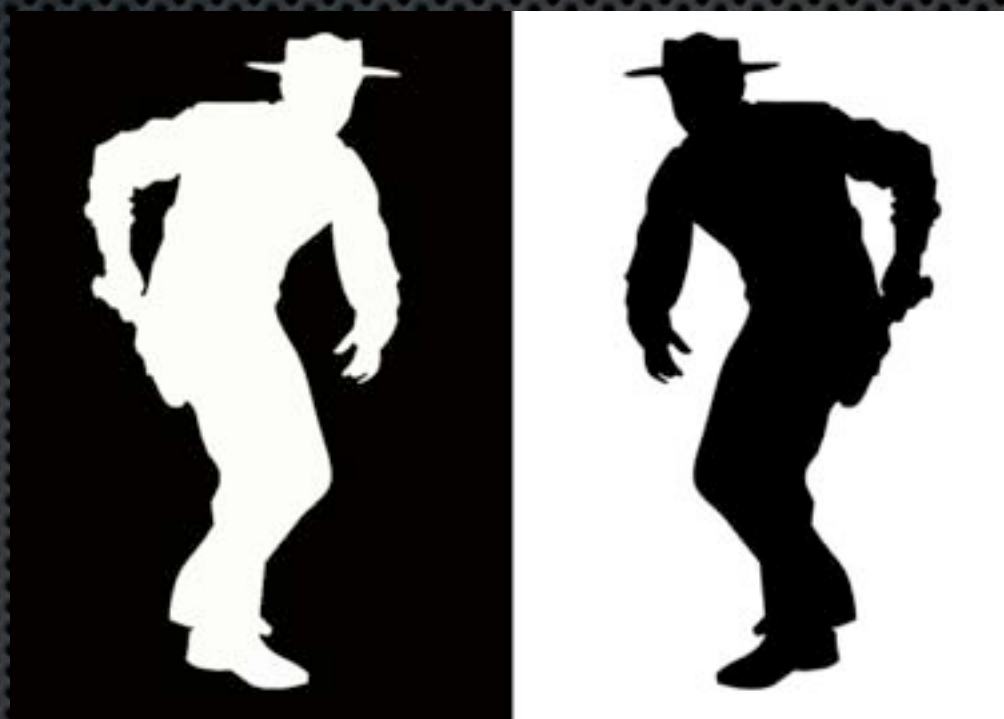
Cast-Led, 2nd Lebanon war (Israel and mid-east)

All **attacks** on $\frac{\text{Israeli}}{\text{Arabic}}$ targets
are **Attributed** to
Hacktivists



Mid-east crime-war links

ARHack



Hacker forum by day

Cybercrime operations by night



[تسجيل الخروج](#)
[خيارات سريعة](#)
[بحث](#)

أهلا وسهلا بك **palhacker0**
 آخر زيارة لك: 2010-06-01 الساعة 10:06 AM
 الرسائل الخاصة: 0 غير مقروء , 0 من مجموع 0 رسالة.

صفحة 1 من 2 1 2 <

أدوات الموضوع | بحث في الموضوع | تقييم الموضوع | طريقة عرض الموضوع

رقم المشاركة : 1

تم
 والله يا اخوان
 الحملة المسعورة
 بعد عنى سوى 500 متر على الاكثر
 و صورته من كمرتى

[تسجيل الخروج](#)
[خيارات سريعة](#)
[البحث](#)
[جديد المواضيع](#)
[التقويم](#)
[قائمة الأعضاء](#)
[تعليمات](#)
[لوحة التحكم](#)

أهلا وسهلا بك **palhacker0**
 آخر زيارة لك: 2010-06-01 الساعة 10:06 AM
 الرسائل الخاصة: 0 غير مقروء , 0 من مجموع 0 رسالة.

ArHaCk.Net :: .. منظمة الهكر العربي :: < ... الاقسام العامة :: < . : السوق السوداء : .
 اشتريه بغيزا مسروقة وخذ نصف سعره كالأش

صفحة 1 من 2 1 2 <

أدوات الموضوع | بحث في الموضوع | تقييم الموضوع | طريقة عرض الموضوع

رقم المشاركة : 1

PM 11:11 , 11-26-2009

اشتريه بغيزا مسروقة وخذ نصف سعره كالأش

يا اخواني في موقع استضافة اشترى منو مساحه الي يدك اياها وخذ نصف سعرها كاش احولك اياه ويستر نيون .
 كل ما كانت المساحة اكبر تحصل على مبلغ اكبر
 يعني لو اشتريت 300 دولار بغيزا مسروقة بحولك 150 دولار على الويستر نيون والله على ما اقول شهيد .
 واشترى كما تريد يعني لو اشتريت 100 مره انا ما يقول لا . واي عملية اتم بحولك الفلوس
 علما انو الشراء عن طريق بلايموس (plimus.com) .
 والي بدو روابط الشراء وحاد في الشغل يضع ايميه وسوف يتم الاضافة ان شاء الله حالا

Nov 2009 : الانتساب
 رقم العضوية : 25036
 المشاركات : 10
 بمعدل : 0.23 يومياً
 عدد النقاط : 10

Political post

Buying/Selling cards for 1/2 their balance

Selling 1600
visa cards

أدوات الموضوع | بحث في الموضوع | تقييم الموضوع | طريقة عرض الموضوع

رقم المشاركة : 1

PM 12:55 , 12-31-2009

1601 فيسا كارد بـ مقابل ؟؟؟؟؟؟؟؟؟

شباب اريد ابادل 1601 فيسا كارد كلهم صالحين و فيهم فلوس

هاكر 00
 .. تنضم جديد ..

History - Revisited...



Georgia

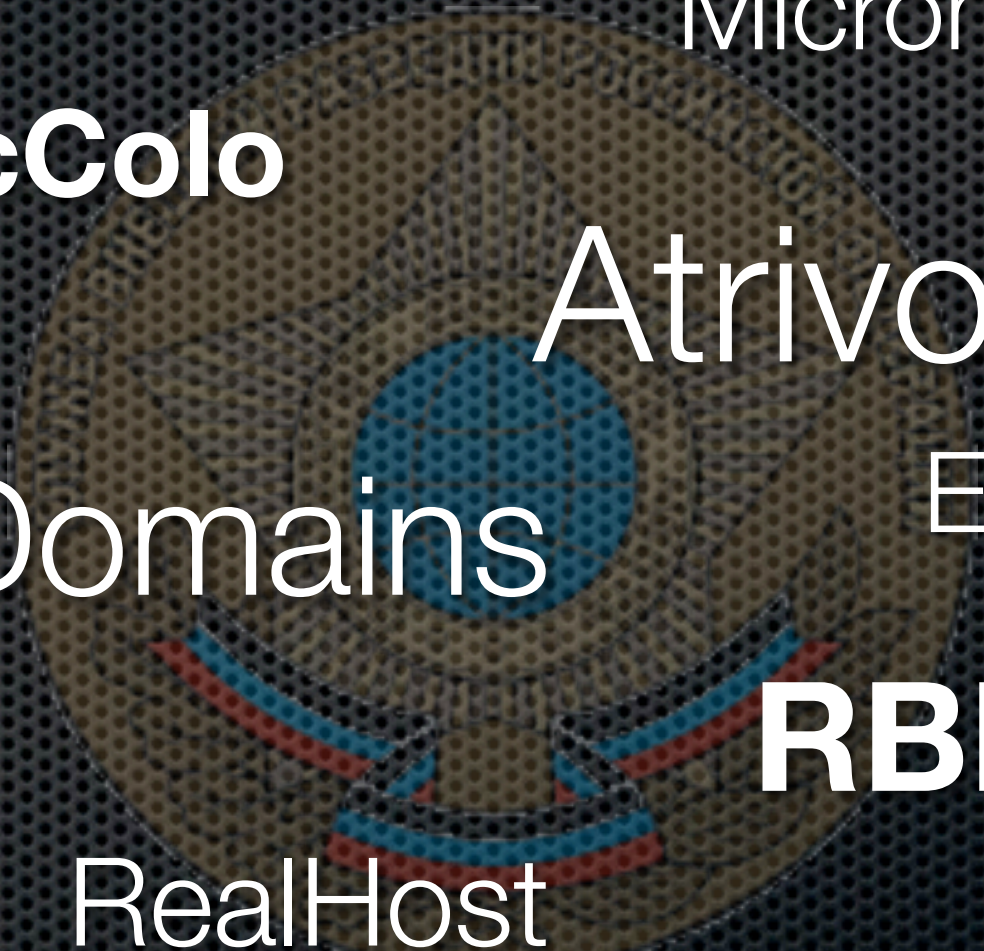
More interesting...

Highly synchronized **Kinetic** and **Cyber** attacks

Targets still mostly **civilian**

Launched from **civilian** networks

Russian Crime/State Dilemma



Micronnet

McColo

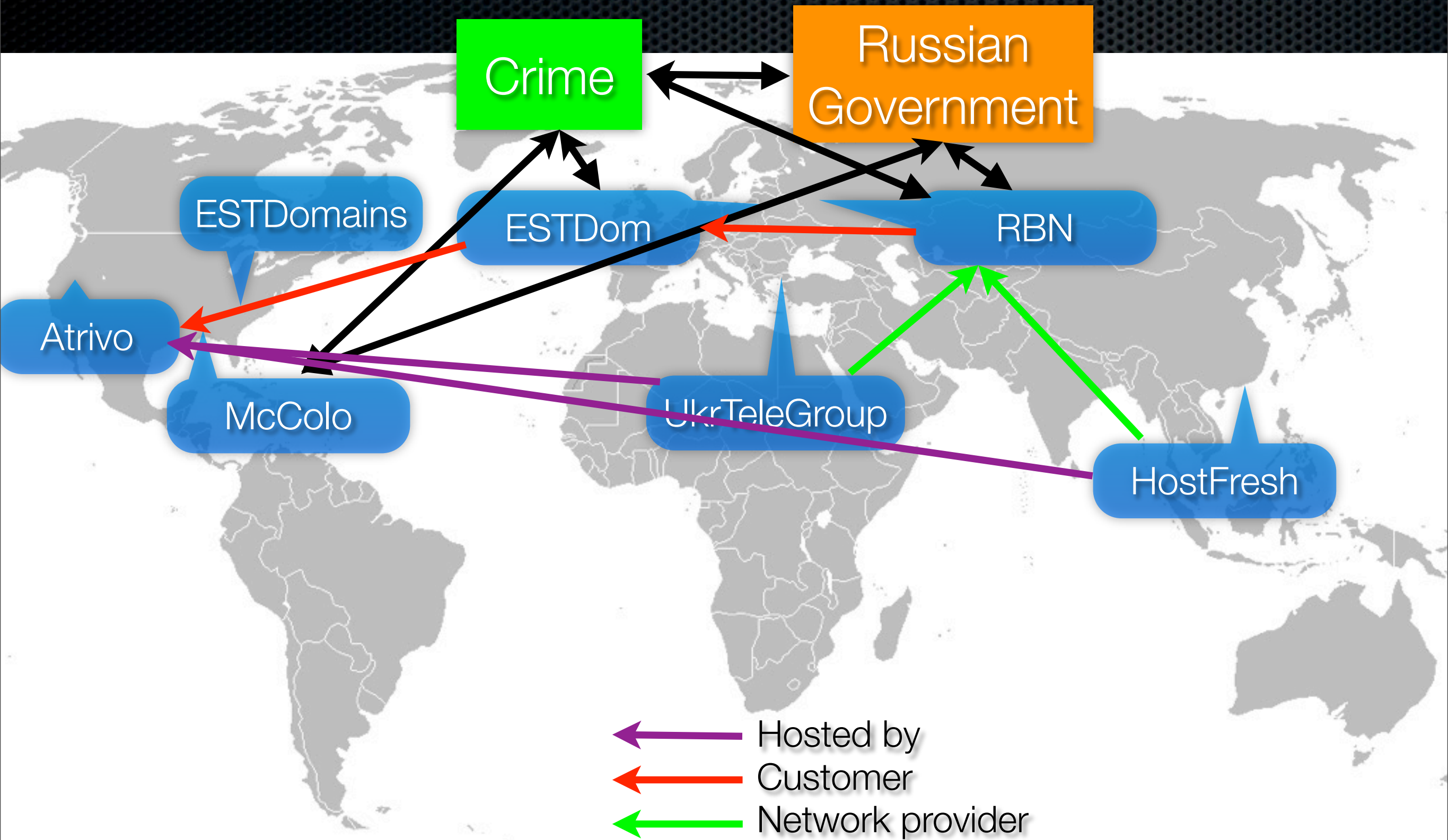
Atrivo

ESTDomains

Eexhost

RBN

RealHost



Remember Georgia?

- ✦ Started by picking on the president...

```
flood http www.president.gov.ge  
flood tcp www.president.gov.ge  
flood icmp www.president.gov.ge
```

- ✦ Then the **C&C** used to control the botnet was shut down as:
 - ✦ **Troops** cross the border towards Georgia
 - ✦ A few days of silence...

Georgia - cont.

- ✦ Six (6) new C&C servers came up and drove attacks at additional **Georgian** sites

www.president.gov.ge
www.parliament.ge
apsny.ge
news.ge
tbilisiweb.info

newsgeorgia.ru
os-inform.com
www.kasparov.ru
hacking.ge mk.ru
newstula.info

- ✦ BUT - the same C&C's were also used for attacks on **commercial** sites in order to extort them (botnet-for-hire)

Additional sites attacked:

- Porn sites
- Adult escort services
- Nazi/Racist sites

- Carder forums
- Gambling sites
- Webmoney/Webgold/etc...

History - Revisited...

Iran

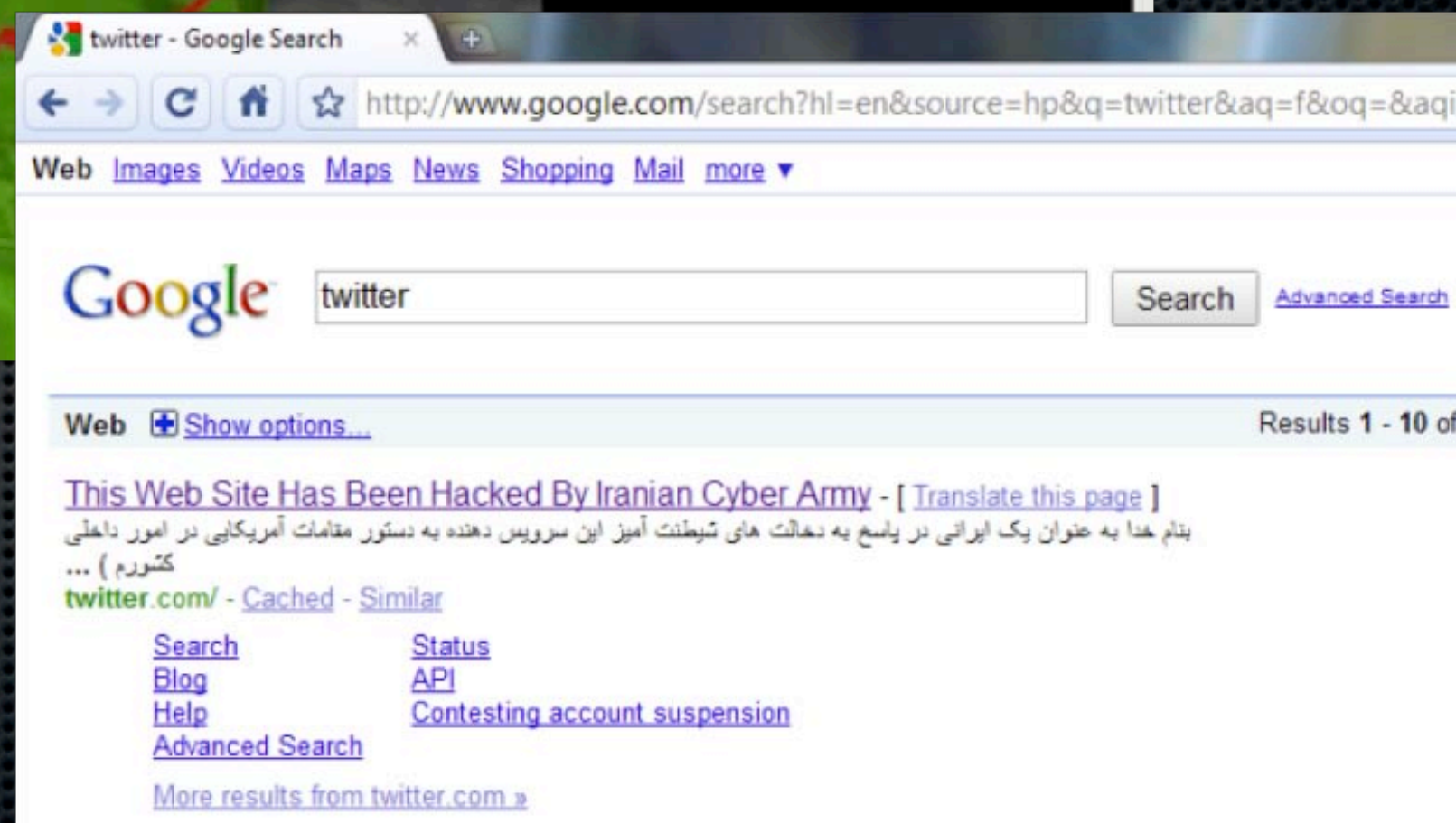
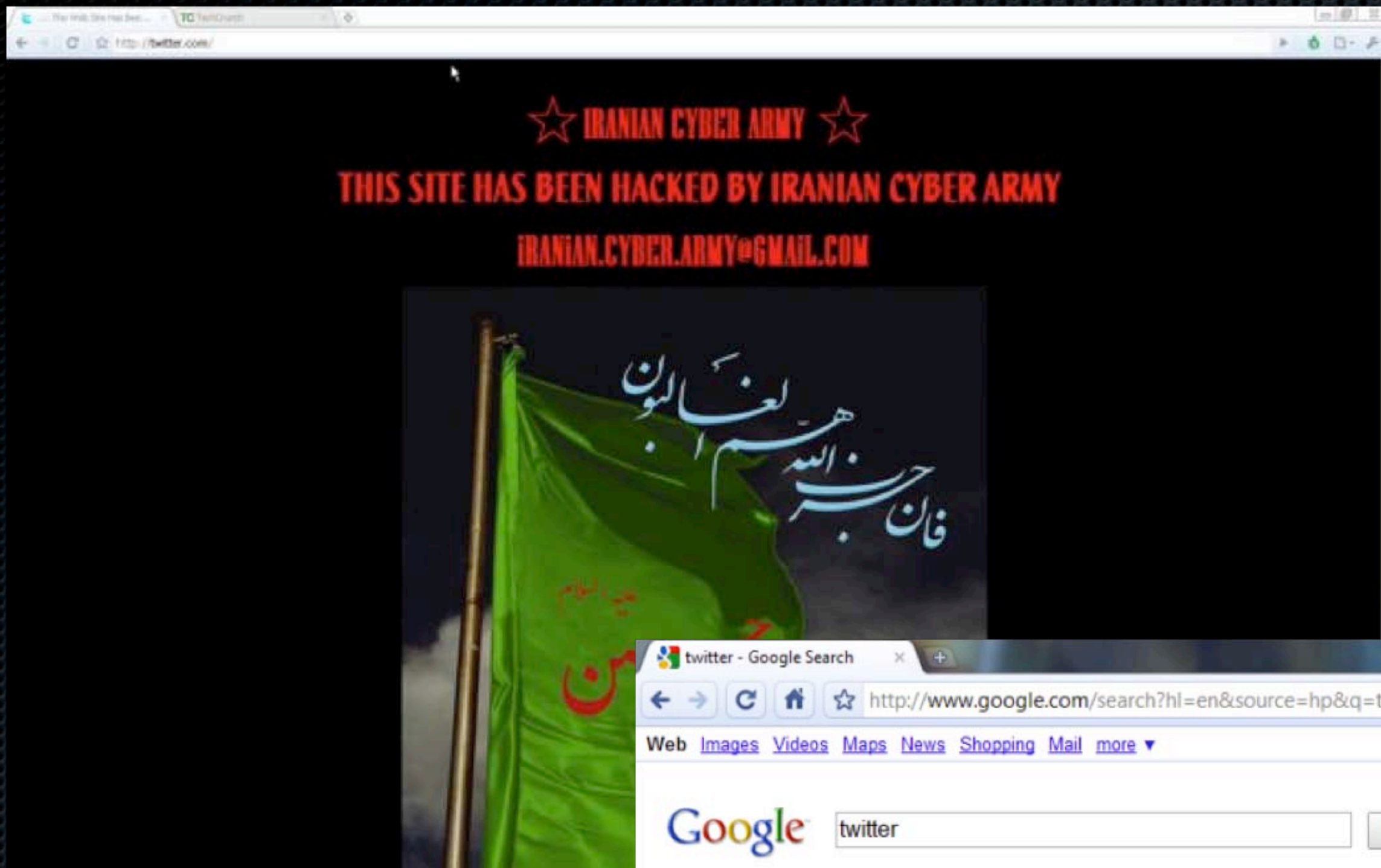
2009 **Twitter** DNS hack attributed to Iranian activity.

Political connections are too obvious to ignore (elections)

Timing was right on:

UN Council
Decisions

Protests by
leadership
opposition in
Tehran



Iran-Twitter connecting dots

- ✦ Twitter taken down December 18th 2009
- ✦ Attack attributed eventually to cyber-crime/vigilante group named “Iranian Cyber Army”
- ✦ Until December 2009 there was no group known as “Iranian Cyber Army”...
- ✦ BUT - “Ashiyane” (Shiite group) is from the same place as the “Iranian Cyber Army”

Mirror saved on: 2009-08-10 21:30:53

Notified by: Ashiyane Digital
Security Team
System: Linux

Domain: <http://dl.nasa.gov/dln/>

IP address: 209.235.106.124

Web server: Apache

[Notifier stats](#)

Your Box Own3z By
**Behrooz_Ice - Q7x - Sha2ow - Virangar - MagicCoder -
Mehdy007-Nitrojen26 - tHe.Mo3tafA - BodyGuard**

We Love Iran

Ashiyane Digital Security Team

Greetz: r00t_b0x - Azazel - 0261 - Jok3r - Ali_eagle - iNJECTOR
and All Ashiyane Defacers



effrontery of blasphemy to Imam Khomeini is what that only you can
do. This is just a warning to your governmental sites!

Your Box Own3z By

**Behrooz_Ice -Q7x -Sha2ow -Virangar -Nitrojen26 -BodyGuard -tHe.Mo3tafA
MagicCoder -0261 -Ali_Eagle -PLUS -Jok3r -System.Fehler**

We Love Iran

Ashiyane Digital Security Team

Greetz: Azazel -mahrud -N4H and All Ashiyane Defacers



Iran-Twitter - Ashiyane

- ✦ Ashiyane was using the same pro-Hezbollah messages that were used on the Twitter attack with their own attacks for some time...
- ✦ AND the “Iranian Cyber Army” seems to be a pretty active group on the Ashiyane forums
www.ashiyane.com/forum

Let's take a look at how Ashiyane operates...

On [Crime|War] training

Ashiyane forums WarGames

Wargame

Sha2ow
Godfather

target : <http://www.chestergas.com/news.asp?id=13>

و جدول رو Edit کنه

#1

AM 11:38 , 09-07-2008

BIG WareGame

سلام ،
گفتم آخر های تابستون هست یه وارگیم بزرگ بزارم واسه بچه ها ، این یه وارگیم بزرگ است برای تست قدرت بچه ها در دیفیس و گرفتن دسترسی ، خوبیش برای شما این هست که هیچ محدودیتی برای نوع و کشور سایت ندارید ...
قوانین :
1- باید حتماً صفحه دیفیس در سایت قرار بدید و یا در صفحه تغییراتی ایجاد کنید که قابل ثبت در سایت Zone-h.org باشد (سایت قبلاً ثبت نشده باشه)
2- سایت باید به اسم تیم آشیانه " Ashiyane Digital Security Team " دیفیس شده باشه ،
3- لینک تایید + ادرس سایت + روش هک + فیلم آموزشی (این آخری برای ترفیع درجه خیلی مهمه ، البته اگر نباشه ایرادی نداره) رو باید در پستتون قرار بدید ،
4- کسانی که سایت های GOV بتونند دیفیس و به اسم آشیانه ثبت کنند ترفیع خواهند گرفت ، (سوتفاهم نشه منظور امتیازشون 2 برابر سایت های معمولی هست)
5- پست بی مورد و اسپم کردن تاپیک ممنوع است ،
6- می تونید در بخش سوال و جواب یک تاپیک بزنید و اونجا به همدیگر کمک کنید و یا سوالاتتون رو بپرسید ، در این تاپیک فقط موارد ذکر شده در قانون 3 رو قرار بدید ،
7- در پایان چند نفر از شرکت کنندگان ارتقا درجه خواهند گرفت (بهترین ها)
8- آخرین مهلت 5 مهر
یا علی
====
مشکلات و سوالات فقط در بخش سوال و جواب

محتوای قوانین سایت ممکن است به مرور زمان و یا در شرایط خاص بروز رسانی شود، لذا آگاهی از جدید ترین محتوای این بخش وظیفه شما بعنوان کاربر این فروم میباشد

قوانین فعالیت در سایت بروز رسانی شد (12 شهریور)

پیشنهادهای و انتقادات برای بهبود وضعیت سایت

بانک مقالات/آموزشی سایت آشیانه

به مدت نیستم به دلیل خدمت سربازی (ماهشهر اهواز)



ERroR

کلانتر سایت



تاریخ عضویت: Aug 2005
محل سکونت: زاندارمری سایت
پست: 1,159
Thanks: 671
399 بار تشکر شده در 159 پست

Y!

Wargame targets includes:





Chester County
natural gas authority
The "Natural" Solution



**WELCOME TO CHESTER COUNTY
NATURAL GAS AUTHORITY**

[Who We Are](#)
[Why Natural Gas](#)
[Customer Service](#)
[Appliances](#)
[Rate Notifications](#)
[Industrial Customers](#)
[Partners](#)
[Community](#)
[Contacts](#)

[F.A.Q.](#) [NEWS](#) [BILL PAY](#) [LINKS](#) [HOME](#)

**CHESTER COUNTY
NATURAL GAS AUTHORITY**

The Chester County Natural Gas Authority was created on April 23, 1954 under Act 806 of the Acts and Joint Resolution of the State of South Carolina of 1954 and commenced the distribution of natural gas in 1957. The service area for the Authority is defined as being Chester County, Lockhart School District in Union County, and the Mitford and Blackstock area in Fairfield County.

A five member Board of Directors governs the Authority. Members of the Board are appointed by the Governor of South Carolina, two upon recommendation of the legislative delegation in the county, two upon recommendation from the City of Chester and one upon recommendation from the Town of Great Falls. Each director serves for a term of six years and can be reappointed. The Board of Directors is not active in the day-to-day management of the Gas Authority.

WHY NATURAL GAS?

GETTING CONNECTED

**LEARN ABOUT
THE NEWEST
GAS APPLIANCES
FOR YOUR HOME**
[LET'S GO](#)

Back to [Crime|War] Links:

What **else** happened on the 18th?

Iranians seize Iraqi oil well on border, Iraq says
Baghdad in talks to decide next move with Tehran over oil well No. 4

BAGHDAD, Dec. 18, 2009

Iraq: Iranian Troops Seized Oil Well

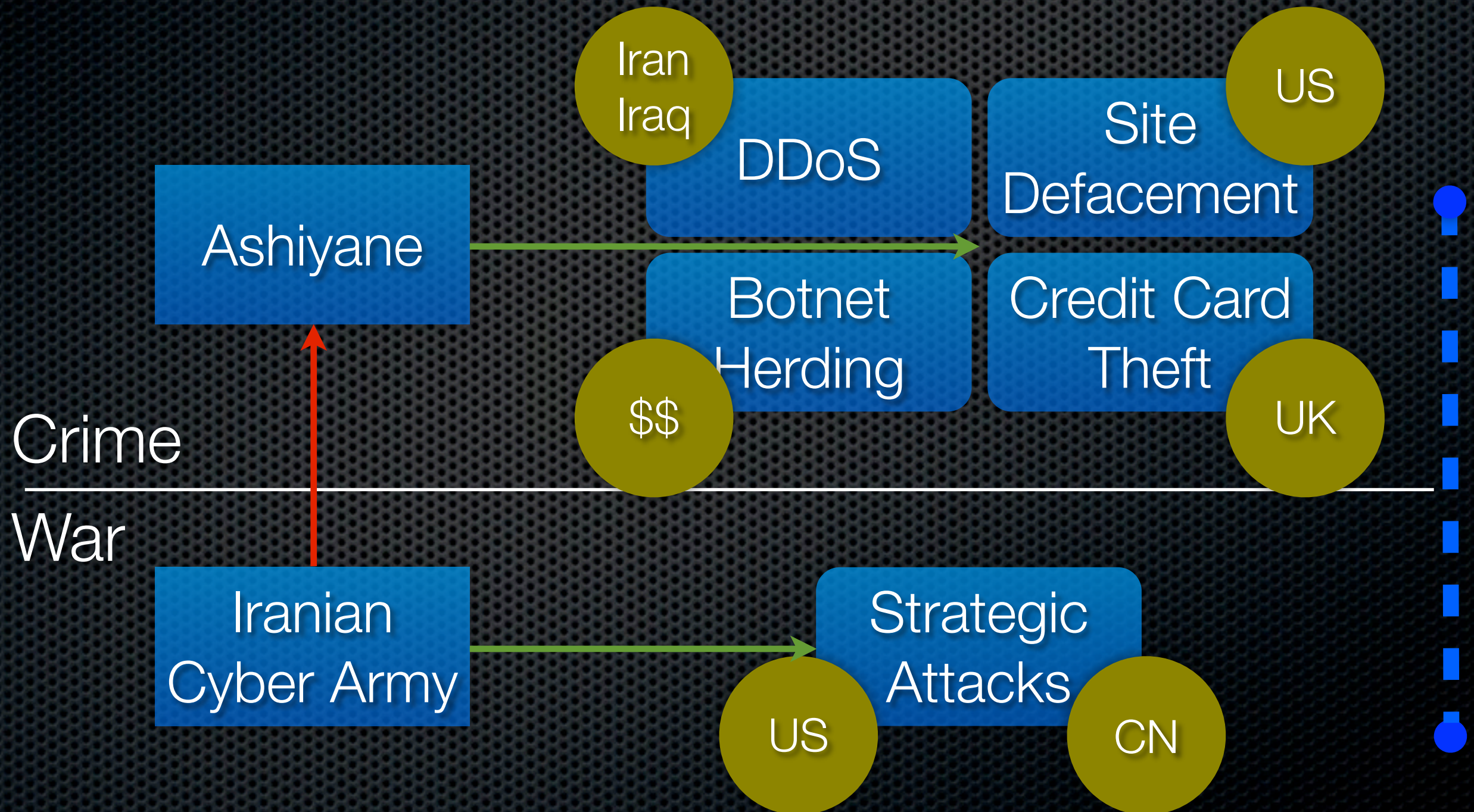
Iraq's Foreign Minister Says Well Along Disputed Southern Border Taken by Soldiers; Spokesman Says Iran Violated Sovereignty

BUSINESS | DECEMBER 19, 2009

Iranian Troops Occupy Oil Field in Iraq, Stoking Tension

More recently - Baidu taken down
with the same MO (credentials)

Mapping Iran's [Crime|War]



History - Revisited...



China

- ✦ Great Chinese Firewall doing an OK job in keeping information out.
- ✦ Proving grounds for many cyber-attackers
- ✦ Bulletproof hosting (after RBN temporary closure in 2008 China provided an alternative that stayed...)

China ... connecting the dots

January 12th - Google announces it was hacked by China

Not as in the “we lost a few minutes of DNS”
hacked...

*“In mid-December we detected a **highly sophisticated and targeted attack** on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google” (David Drummond, SVP @Google)*

China ... connecting the dots.

January 12th - Adobe gets hacked. By China.

*“Adobe became aware on January 2, 2010 of a computer security incident involving a **sophisticated coordinated attack** against corporate network systems managed by Adobe and other companies” (Adobe official blog)*

Same **MO**: 0-day in Internet Explorer to get into Google, Adobe and more than 40 additional companies

China ... connecting the dots..

The only problem so far - the attacks all have the sign of a CyberCrime attack. All the evidence points to known crime groups so far.

*“It was an attack on the technology infrastructure of major corporations in sectors as diverse as **finance, technology, media, and chemical**”* (Google enterprise blog)

China ... connecting the dots...

Criminal groups attack companies in order to get to their data so they can sell it (whether it was commercial or government data!)

US Response: *“We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy.”* (Hillary Clinton, Secretary of State)

China ... connecting the dots....

The China move:

Use of criminal groups to carry out the attacks provides the perfect deniability on espionage connections (just like in the past, and a perfect response to clinton).

Targets are major US companies with strategic poise to enable state interest espionage

Information sharing at its best:

STATE ↔ **Crime**
Win - Win

THE FUTURE (Illustrated)



Summary

Good

Formal training on
cybersecurity by
nations

Bad

Commercial
development of
malware still reigns

Ugly

Good meet Bad: money changes hands,
less tracks to cover, criminal ops already
creating the weapons...

Summary

THE FUTURE

LACK OF LEGISLATION AND COOPERATION ON MULTI-NATIONAL LEVEL IS CREATING DE-FACTO "SAFE HAVEN" FOR CYBERCRIME. <- FIX THIS!

TREATIES AND ANTI-CRIME ACTIVITIES MAY PROVE TO BE BENEFICIAL. <- NUKES?

Thanks!

Q & A

iamit@iamit.org

pro: iamit@securityandinnovation.com

twitter: twitter.com/iamit

blog: iamit.org/blog