

# Cyber [Crime|War]

Connecting the dots

**Iftach Ian Amit**

Managing Partner, Security & Innovation



# Agenda

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



# Who Am I





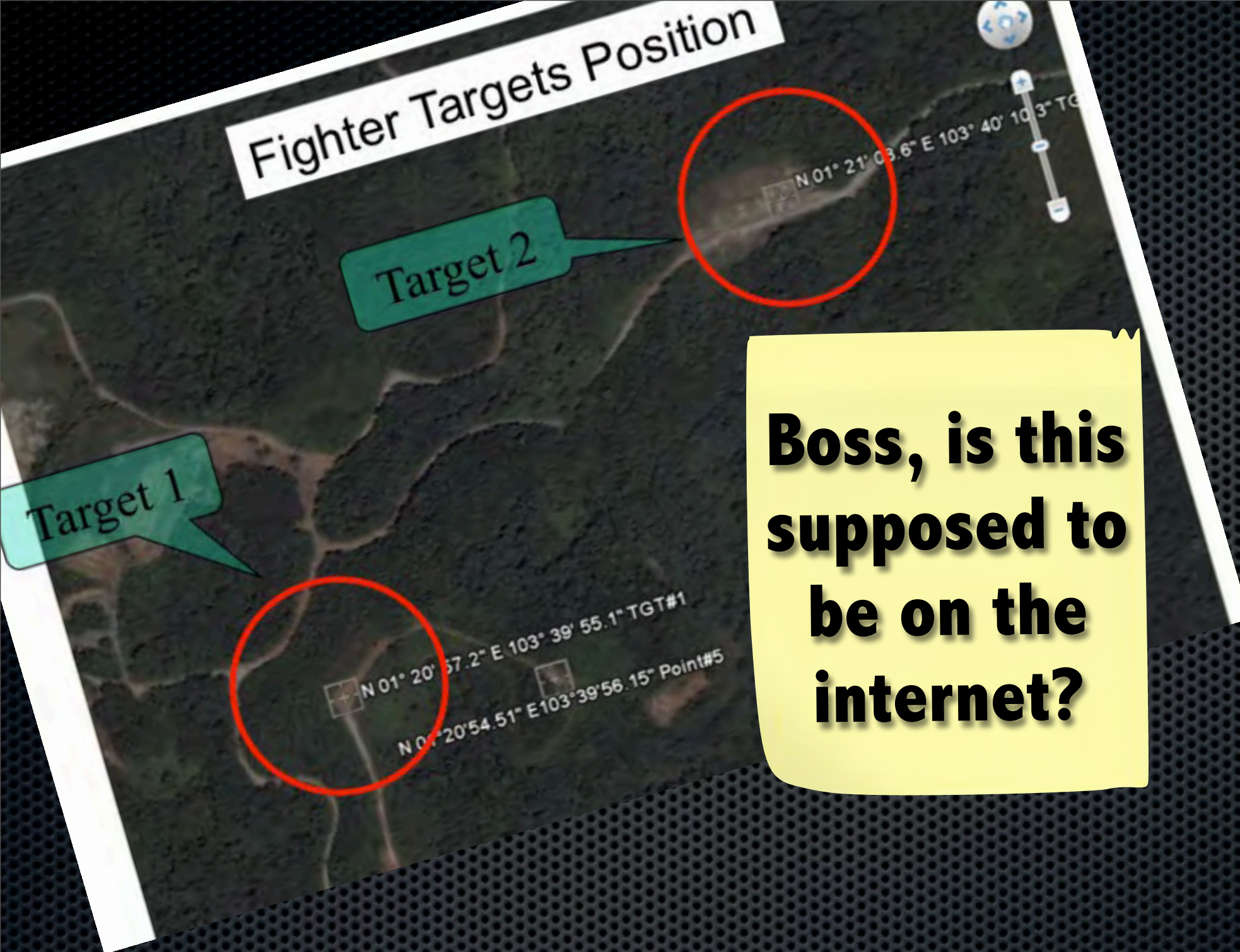
This is NOT going to be



# Picking up where we left off

At least as far as BlackHat is concerned...

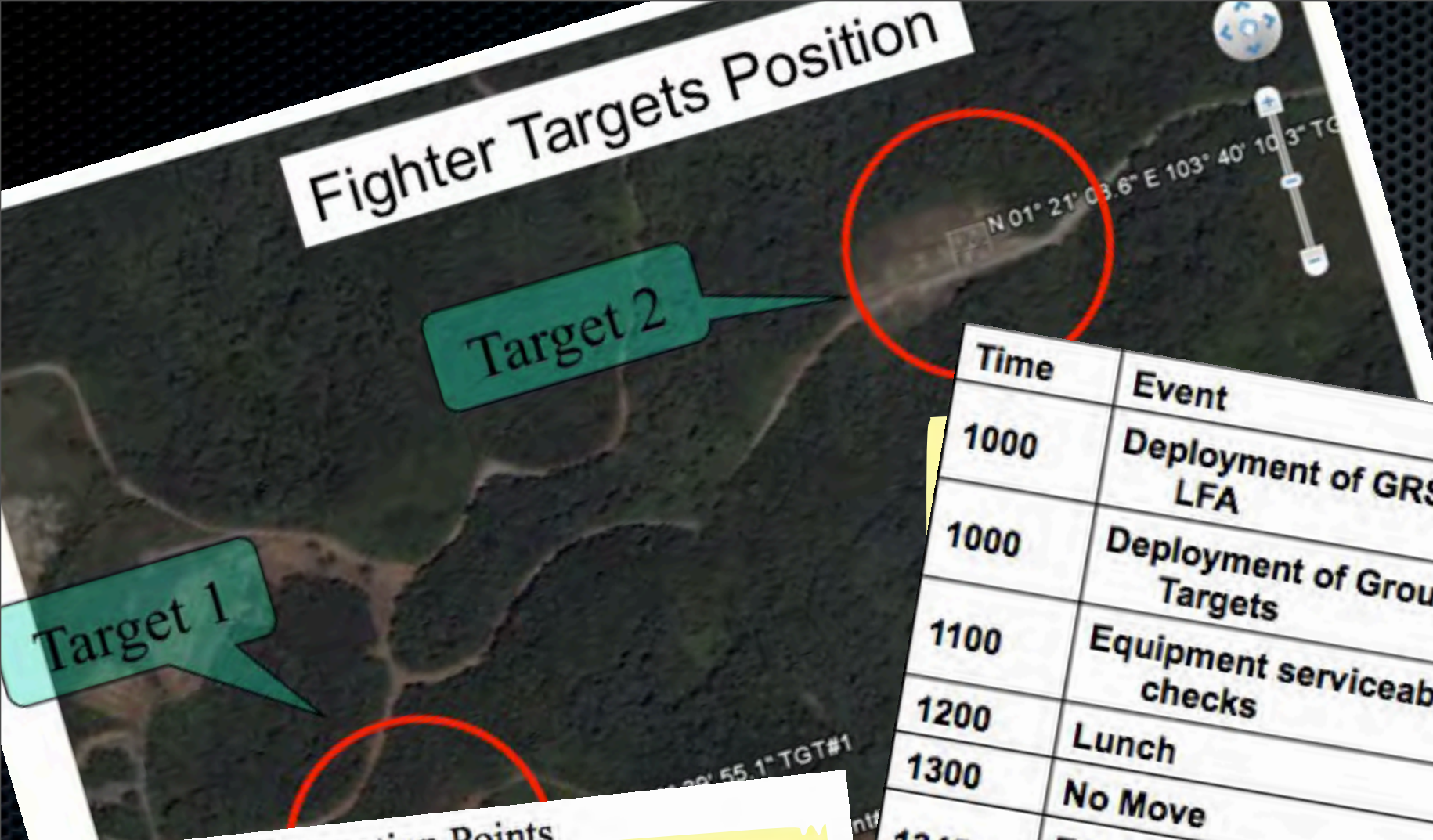




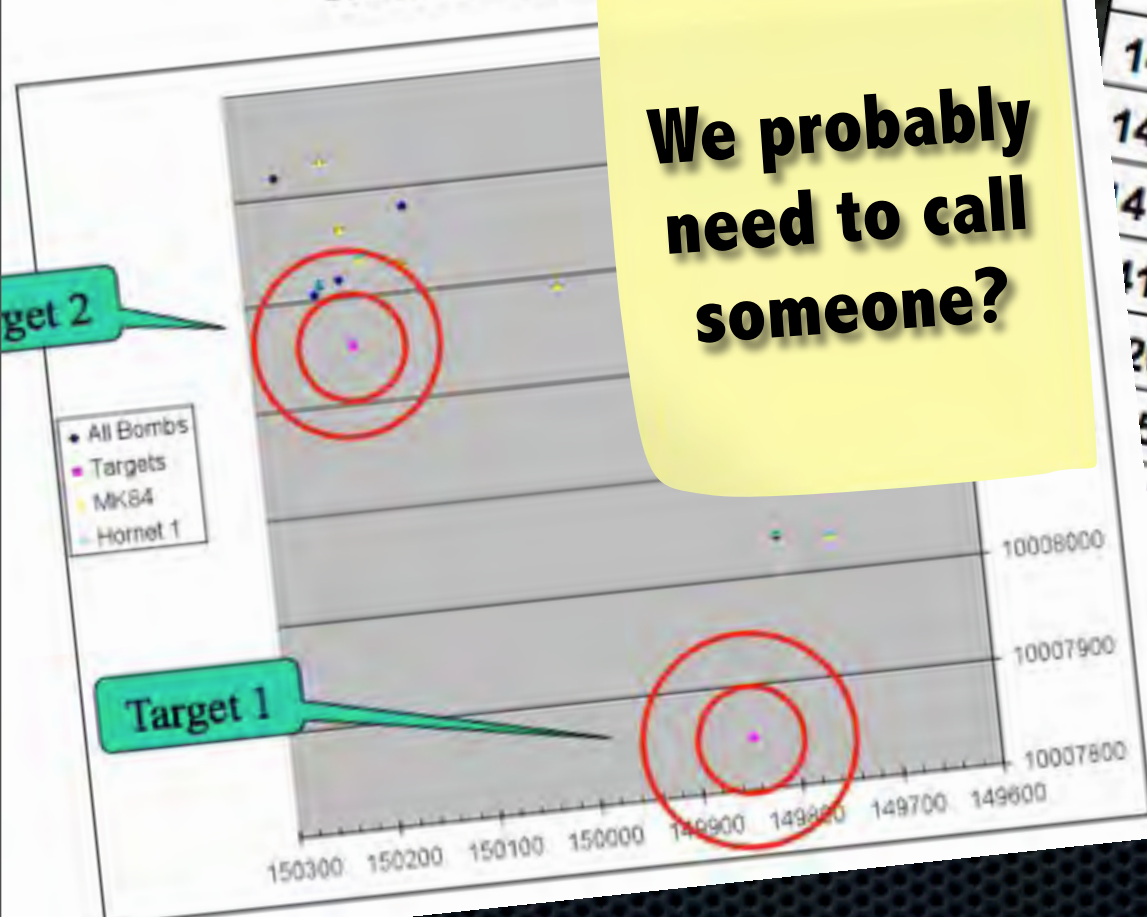
**Boss, is this  
supposed to  
be on the  
internet?**



# Fighter Targets Position



## Detonation Points



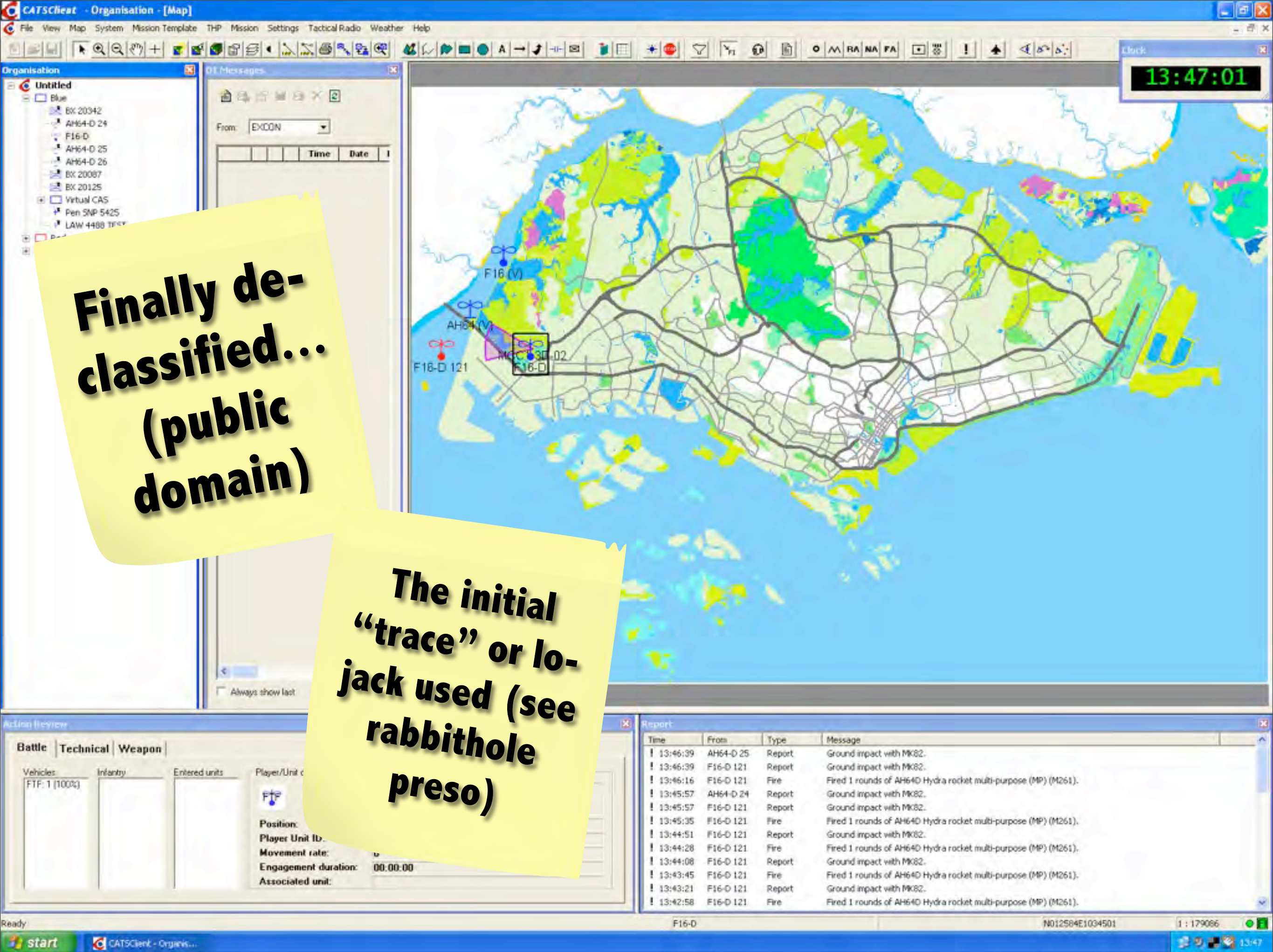
**We probably need to call someone?**

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  
preso)**

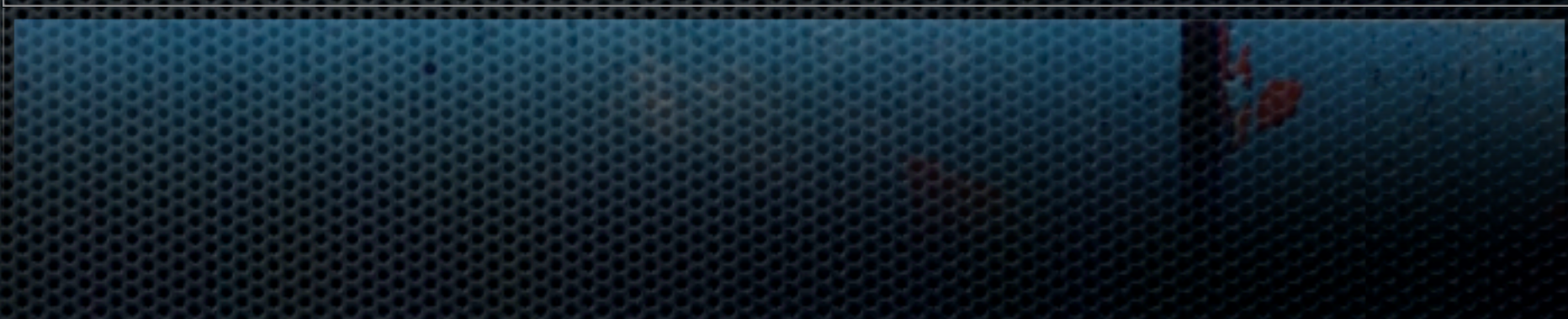


# Hungry yet?

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?







This is not the **only** way!



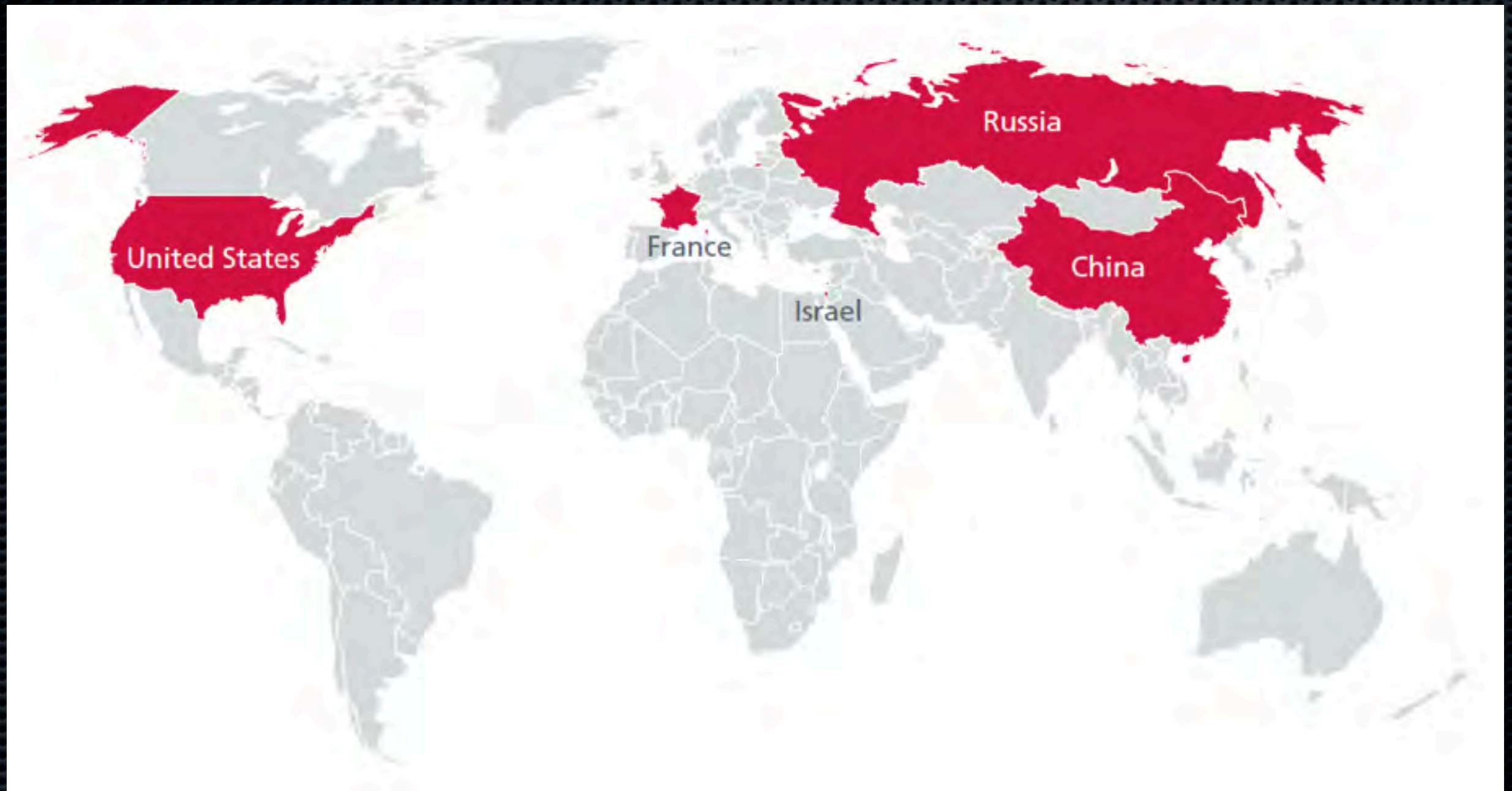
Neither is this...



But civilian are  
**always** at stake!



# Many faces of how CyberWar is perceived...



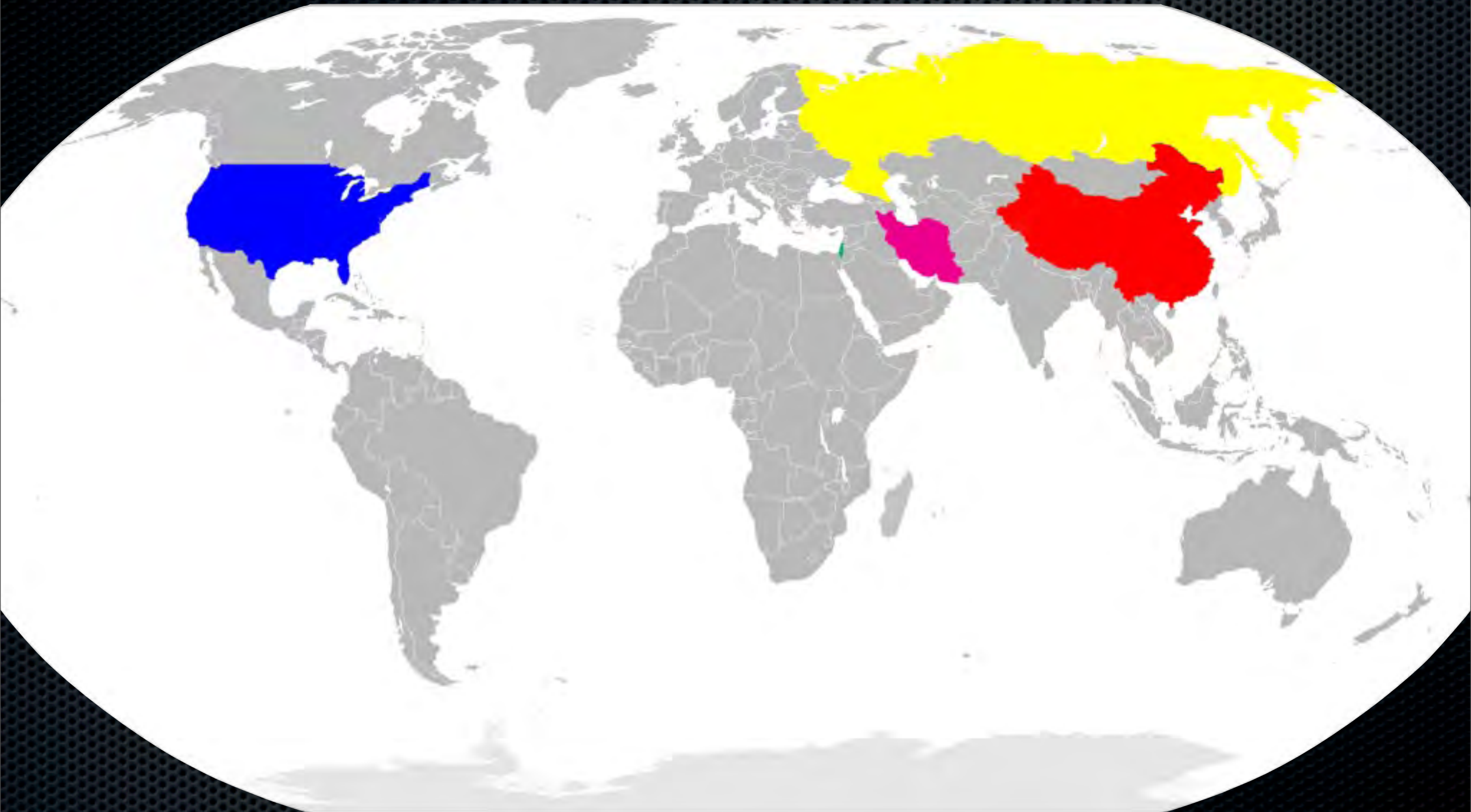
From McAfee's "Virtual Criminology Report 2009"

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)
- ✦ Yes... Titan Rain...





# 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](http://mossad.gov.il)...)

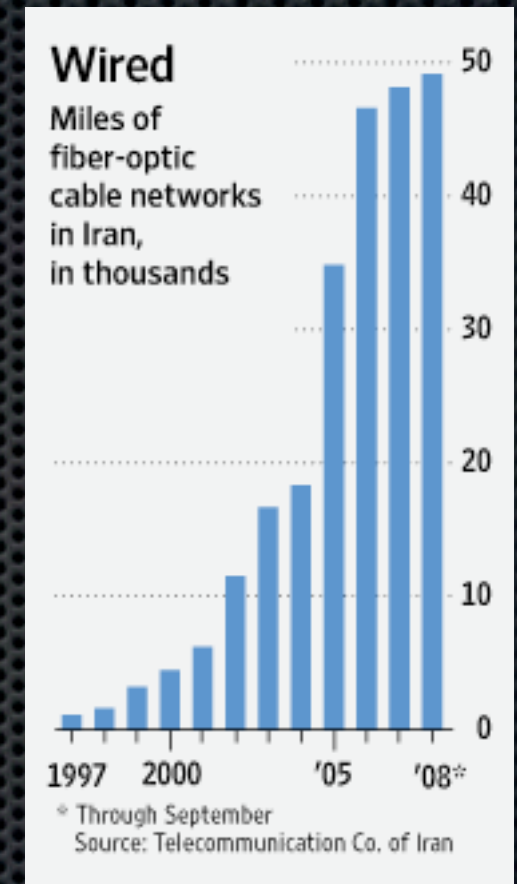
מדינת ישראל • המוסד למודיעין ולתפקידים מיוחדים  
STATE OF ISRAEL • ISRAEL SECRET INTELLIGENCE SERVICE





# Iran

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





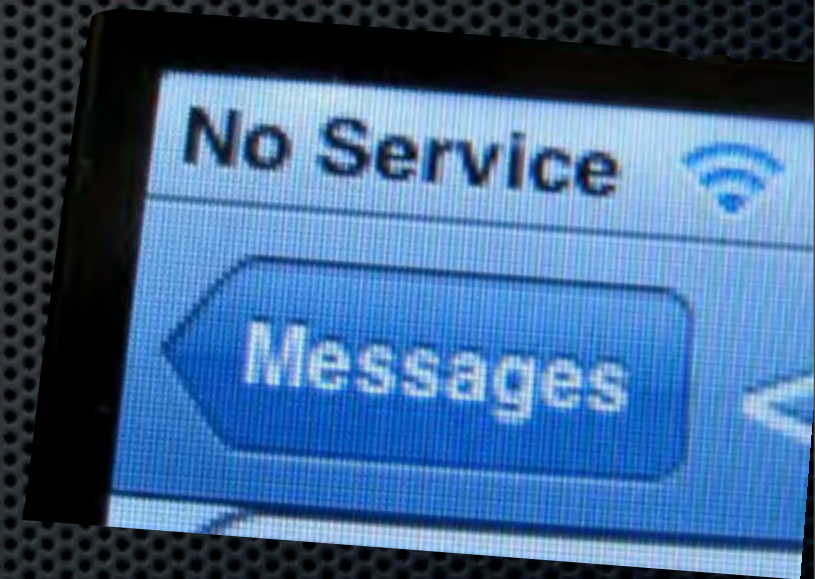
# CyberWar - Attack

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



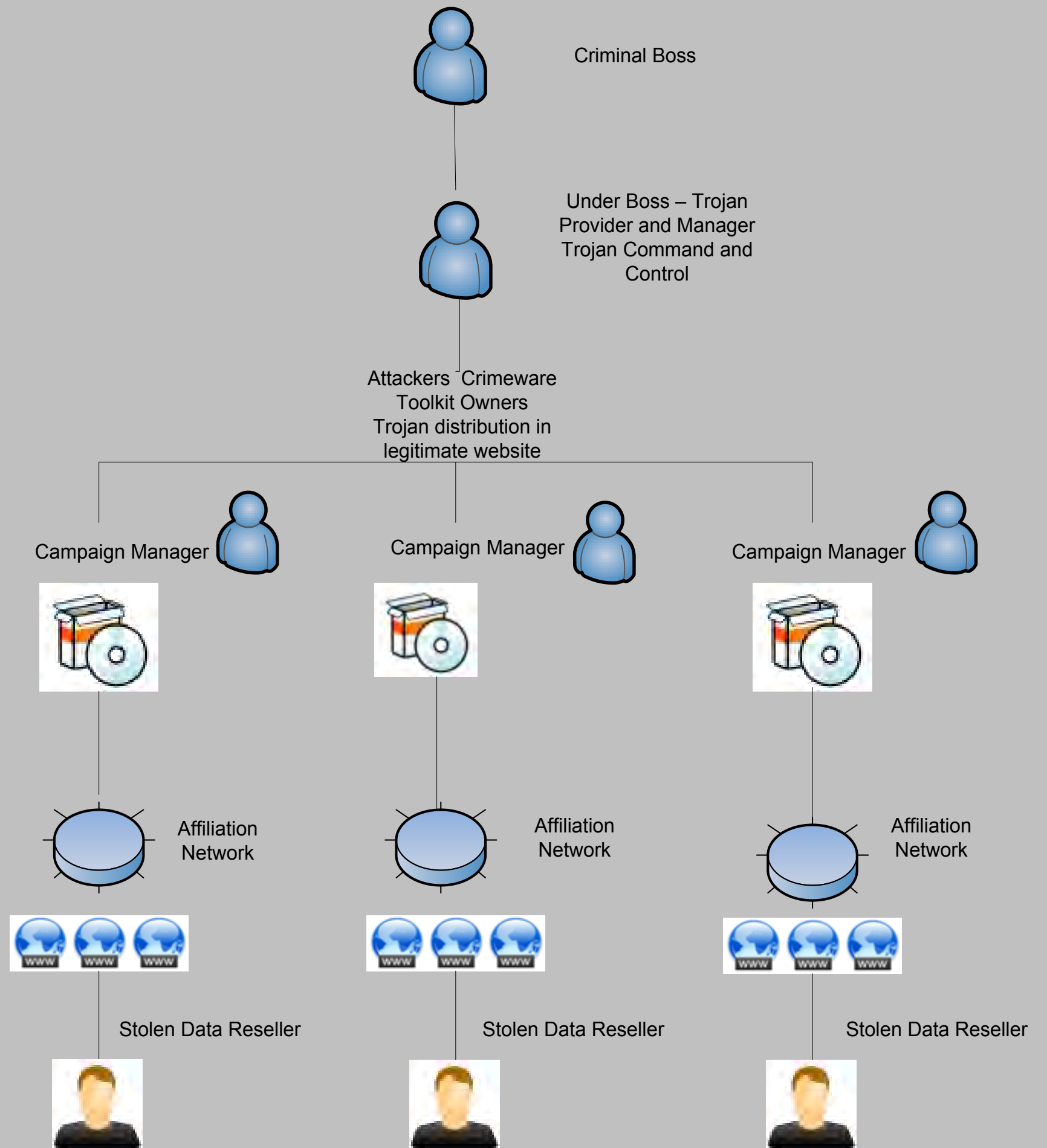


# CyberCrime





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

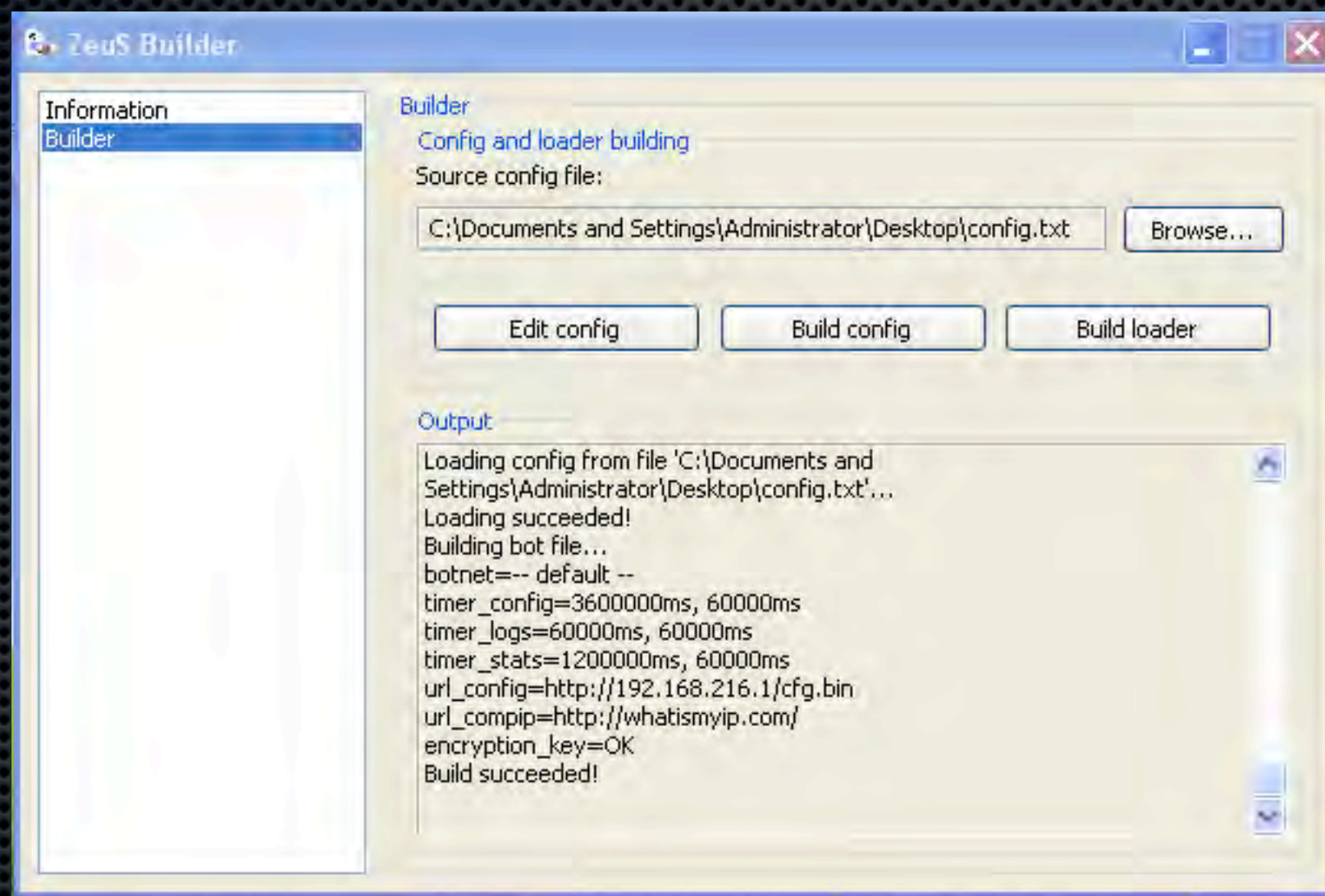


# CyberCrime - target location





# CyberCrime - 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:

Search  
Search  
Upload

### 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:

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_cxl7f5jvt_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

Add graphics of Anti-X  
Show VirusTotal success  
rates (fail)

- ✦ 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...



# CyberCrime - Locations





# 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

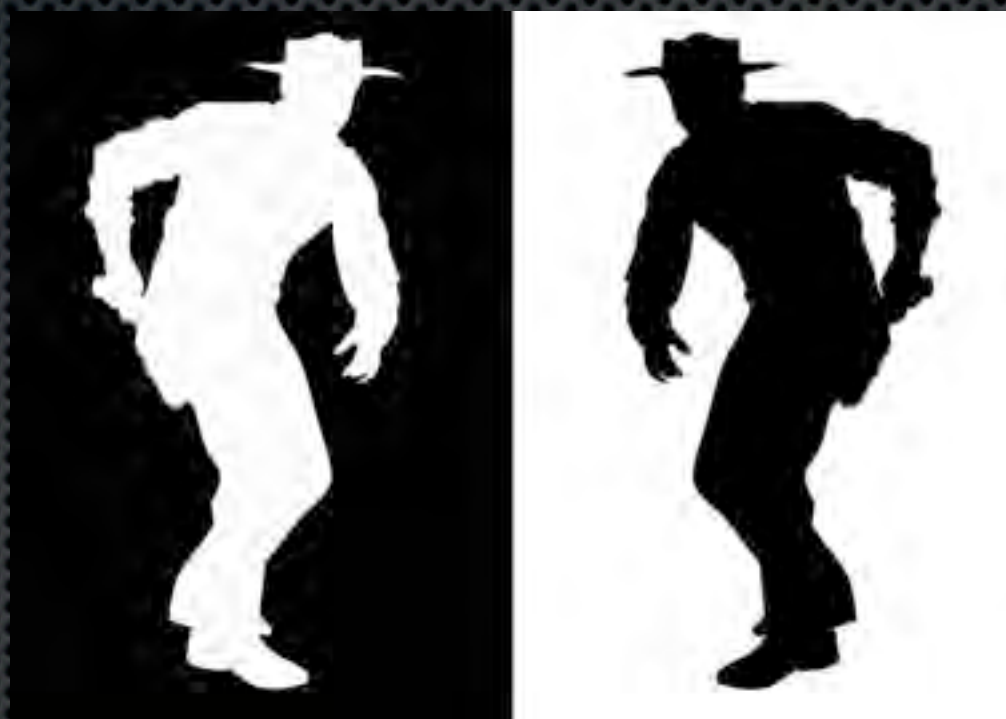
Palestinian TV hacked - propaganda





# Mid-east crime-war links

**ARHack**



**Hacker** forum by day

**Cybercrime** operations by night





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

صفحة 1 من 2 1 2 <

وات الموضوع ▼ البحث في الموضوع ▼ تقييم الموضوع ▼ طريقة عرض الموضوع ▼

رقم المشاركة : 1

كم

والله يا اخوان

الحملة المسعورة

يعد عني سوى 500 متر على الاكثر

و صورته من كمرتي

www.arhack.net

لوحة التحكم تعليمات قائمة الأعضاء التقييم جديد المواضيع البحث خيارات سريعة تسجيل الخروج

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

ArHack.Net:: .. :: منظمة الهكر العربي :: .. < ... الاقسام العامة ... > . : السوق السوداء : .  
اشترية بغيزا مسروقة وخذ نصف سعره كالاش

صفحة 1 من 2 1 2 <

أدوات الموضوع ▼ البحث في الموضوع ▼ تقييم الموضوع ▼ طريقة عرض الموضوع ▼

رقم المشاركة : 1

PM 11:11, 11-26-2009

اشترية بغيزا مسروقة وخذ نصف سعره كالاش

يا اخواني في موقع استضافة اشترى منو مساحة الي يدك اياها وخذ نصف سعرها كاش احولك اياه ويستر نيون .  
كل ما كانت المساحة اكبر تحصل على مبلغ اكبر  
يعني لو اشترت 300 دولار بغيزا مسروقة بحولك 150 دولار على الويستر نيون والله على ما اقول شهيد .  
واشترى كما تريد يعني لو اشترت 100 مره انا ما بقول 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

معلومات العضو

**ابوشهاب**  
.. :: تنضم جديد :: ..

احصائية العضو

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

Buying/Selling cards for 1/2 their balance

أدوات الموضوع ▼ البحث في الموضوع ▼ تقييم الموضوع ▼ طريقة عرض الموضوع ▼

رقم المشاركة : 1

PM 12:55, 12-31-2009

1601 فيسا كارد ب مقابل ??????????

شباب اريد ابادل 1601 فيسا كارد كلهم صالحين و فيهم فلوس

معلومات العضو

**هاكر 00**  
.. :: تنضم جديد :: ..

Political post

Selling 1600  
visa cards



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

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





# History - Revisited...

## Georgia

More interesting...

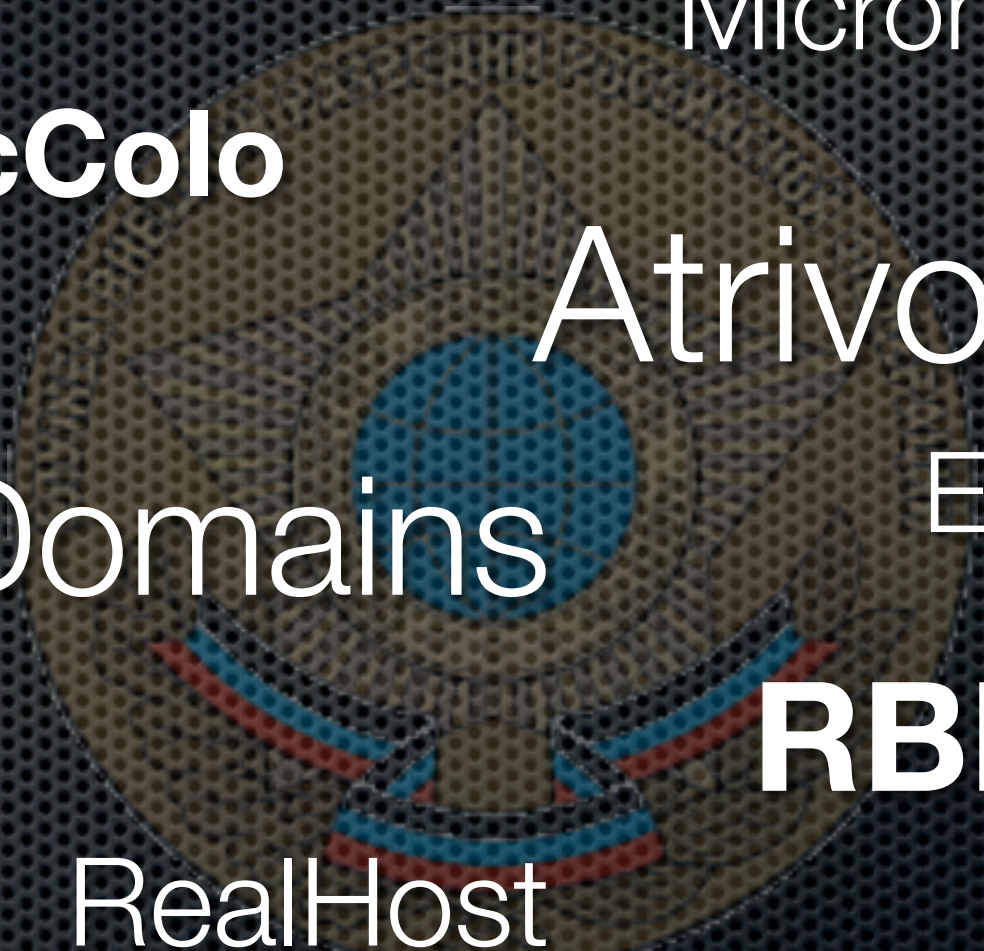
Highly synchronized **Kinetic** and **Cyber** attacks

Targets still mostly **civilian**

Launched from **civilian** networks



# Russian Crime/State Dilemma



Micronnet

**McColo**

Atrivo

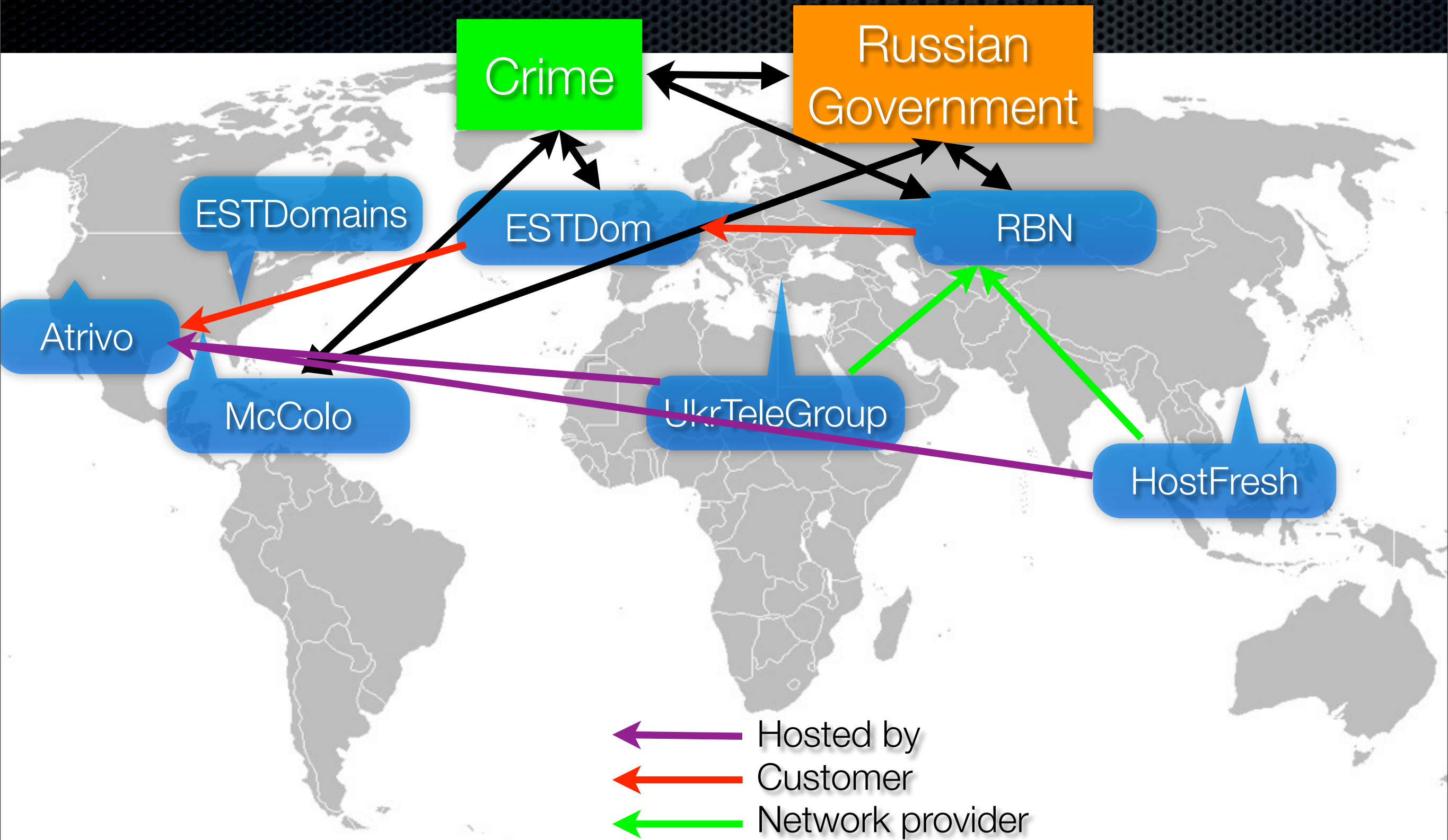
ESTDomains

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 region as the “Iranian Cyber Army”
- And 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](http://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 به وارگیم بزرگ بزارم واسه بچه ها . این به 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 باشد .  
3 - لینک تایید + ادرس سایت + روش هک + فیلم آموزشی ( این اخری 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 با سوالاتون 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 - اخرین 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 نایستم 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:





# 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

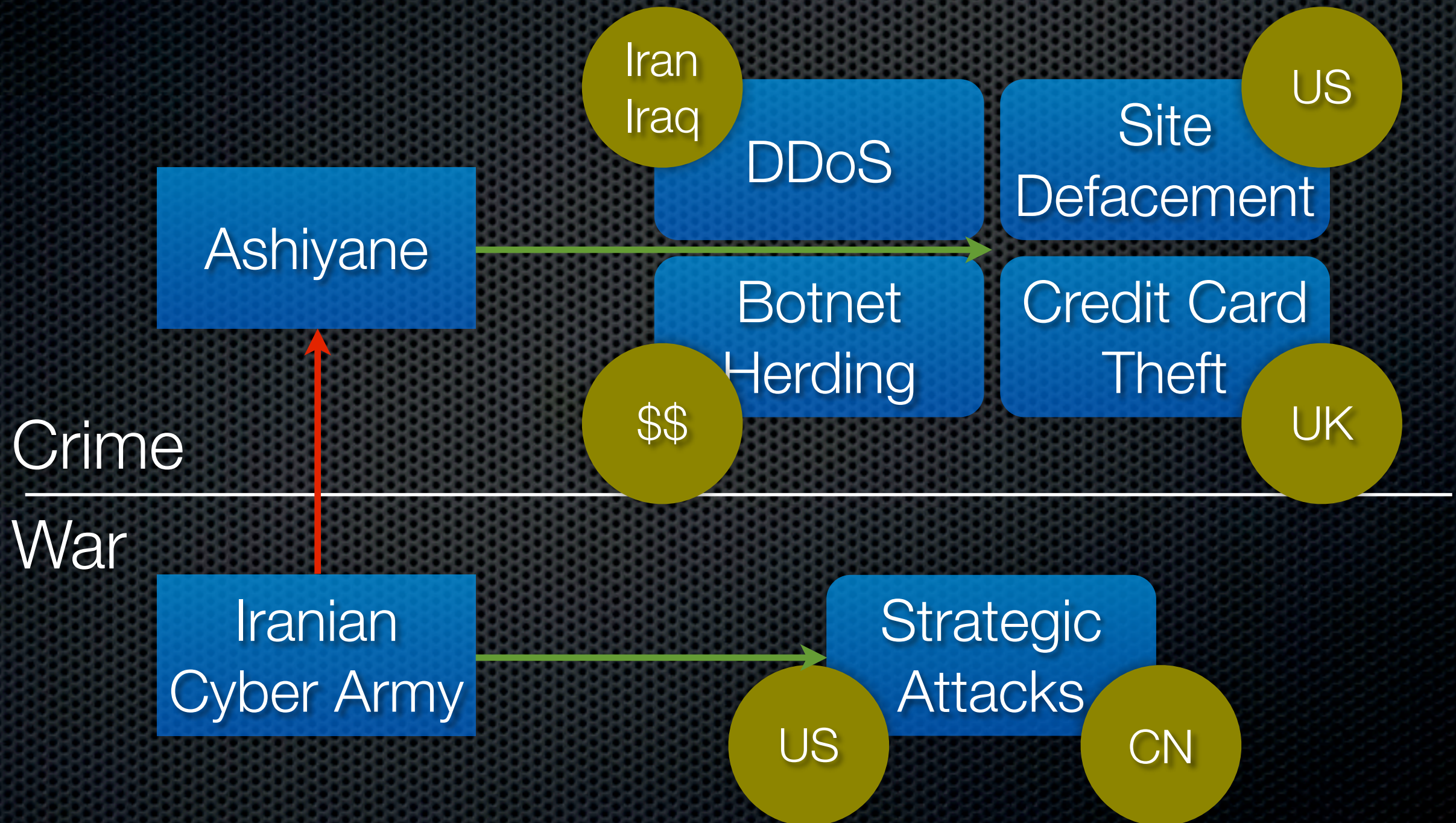
BUSINESS | DECEMBER 19, 2009

**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 IE and Acrobat 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**



# 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**

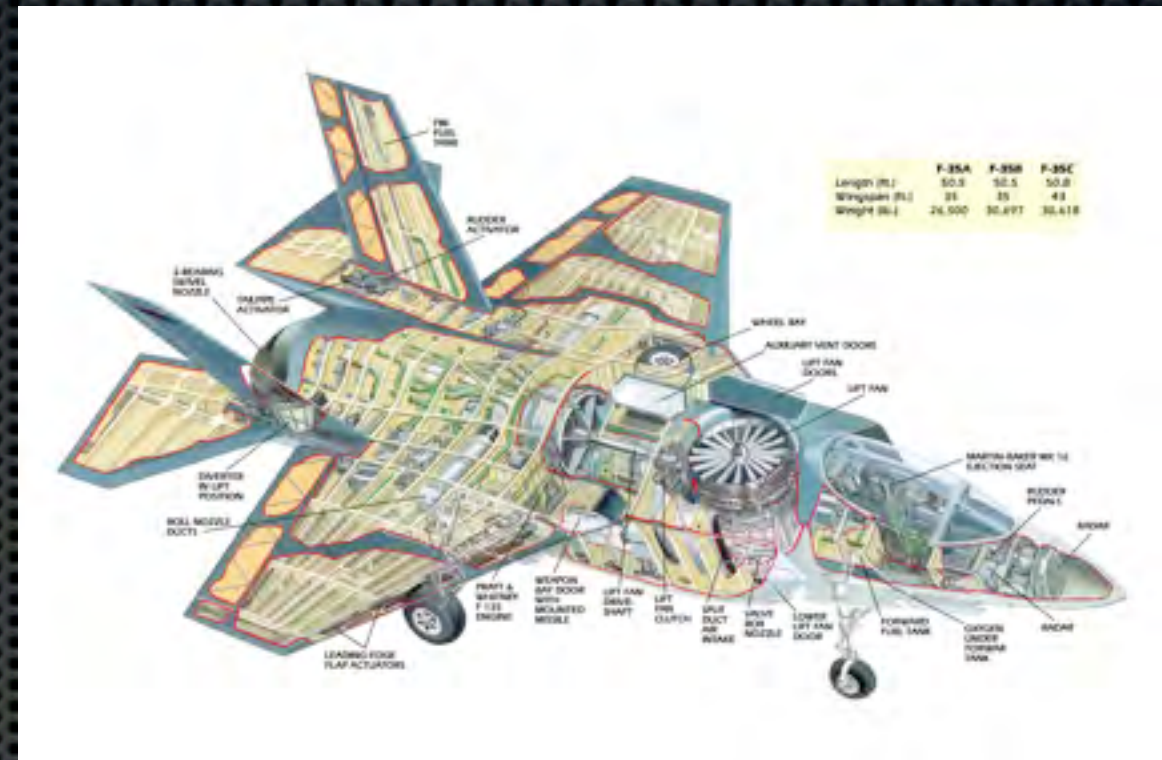
Win - Win



# History - cont.

## USA

- ✦ Breach of the F-35 plans
- ✦ The “North-Korean” DDoS attack...
- ✦ Twitter DDoS related to Iran (already covered)
  - ✦ Probably in retaliation to the tweeting during the Iran elections





# Future

- ✦ Landscape highly unclear!
- ✦ Where does that put “developing” nations
  - ✦ Africa? OLPC + zero enforcement of licensing = largest infected PC population in the world!
- ✦ Arms race is on. Government/military commissioned attacks more likely, but mainly surgical strikes
  - ✦ No Cybergeddon for you so far...
- ✦ Massive connectivity is still the WMD of CyberWar (and is a commodity)
  - ✦ No problem getting it from questionable “arms dealers” (bot herders) - just like we do now with conventional weapons....



# Summary

- ✦ The Good
  - ✦ Formal training on cybersecurity by nations
- ✦ The Bad
  - ✦ Commercial development of malicious computer software (weapons manufacturers)
- ✦ The Ugly
  - ✦ Good meets Bad - money changes hands, less tracks to cover (politically), criminal organizations already manufacturing arms...
- ✦ The Future
  - ✦ Looks good, but pretty ugly now. Lack of legislation and cooperation on multi-national level is creating de-facto “safe haven” for cybercrime



# Thanks!

## Q & A

[iamit@iamit.org](mailto:iamit@iamit.org)

pro: [iamit@securityandinnovation.com](mailto:iamit@securityandinnovation.com)

twitter: [twitter.com/iamit](https://twitter.com/iamit)

blog: [iamit.org/blog](http://iamit.org/blog)