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

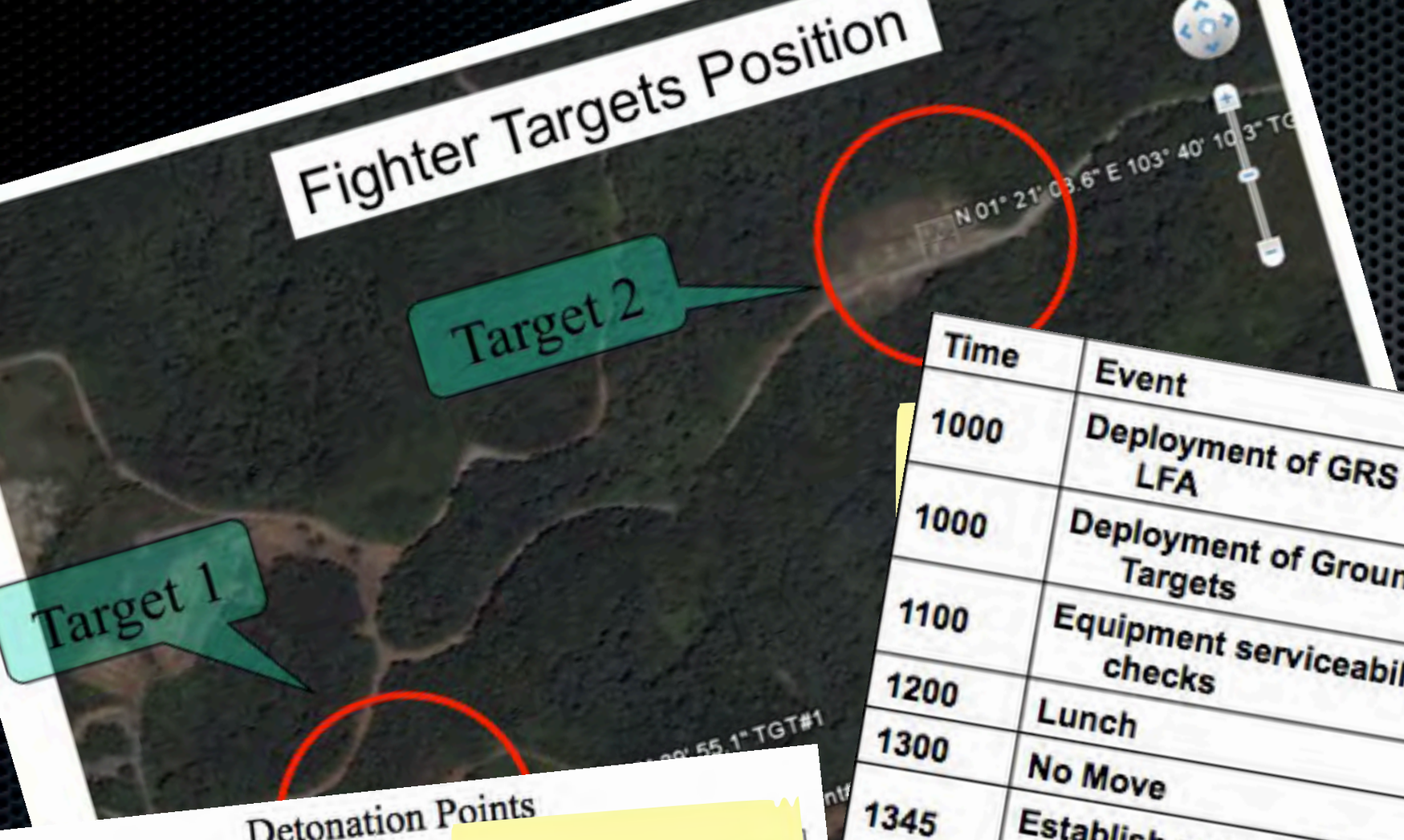
Who Am I

This is NOT going to be

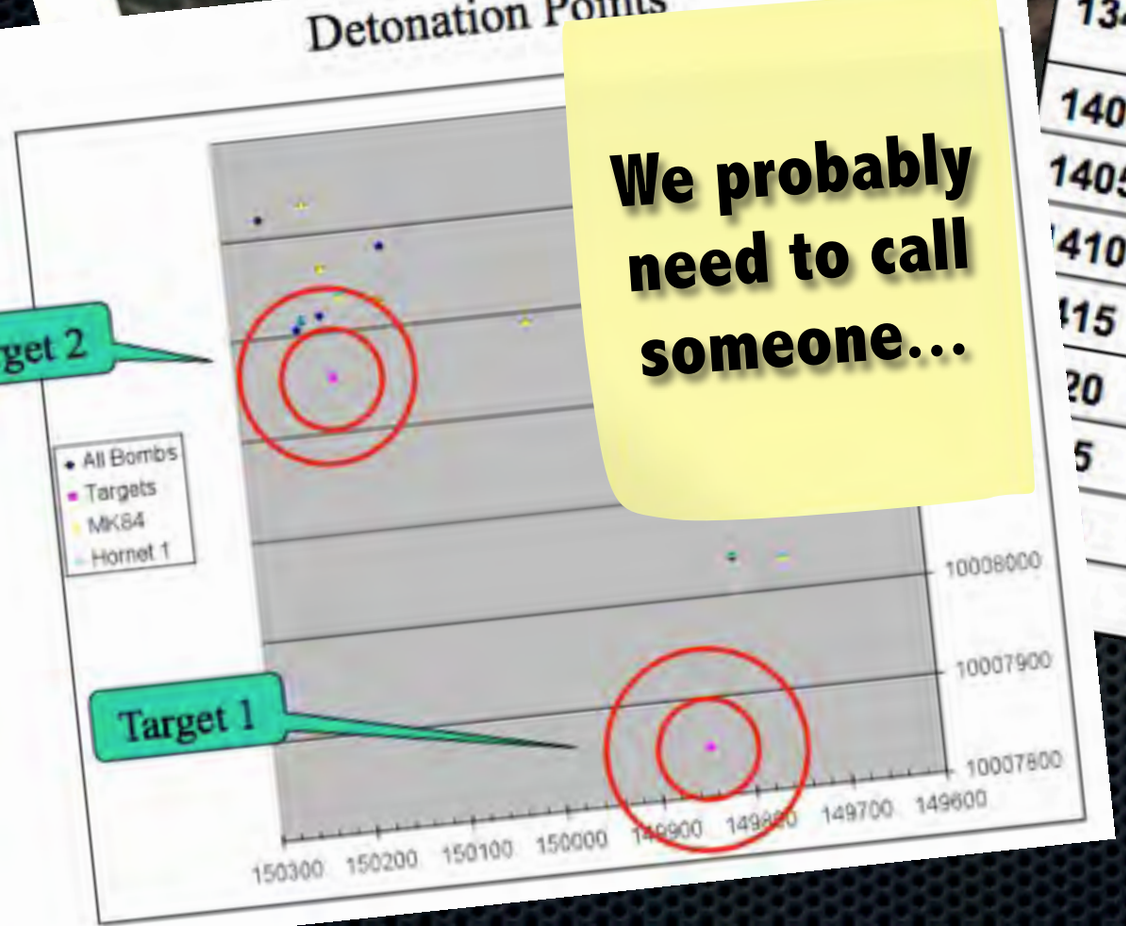
Picking up where we left off

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
20	Trial #3b
5	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
	drops on ground targets (Mk82,
	d engagements at ALIGN GRS
	und 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)

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!

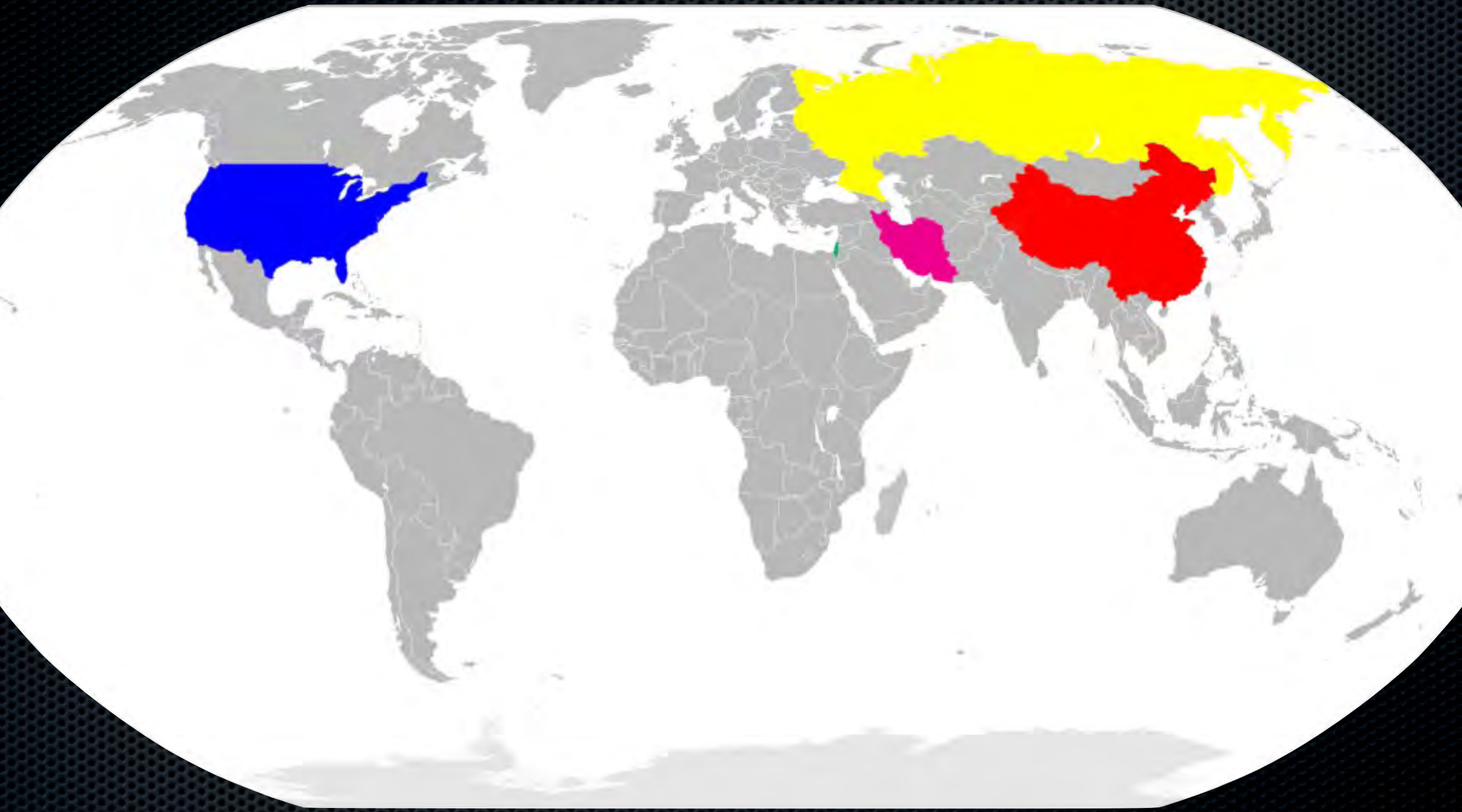
Many faces of how CyberWar is perceived...

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...

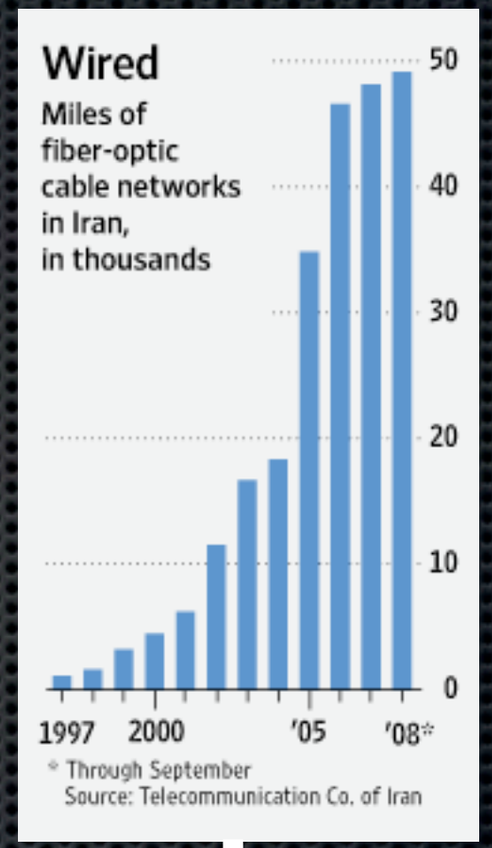
Russia

- 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)
  - 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

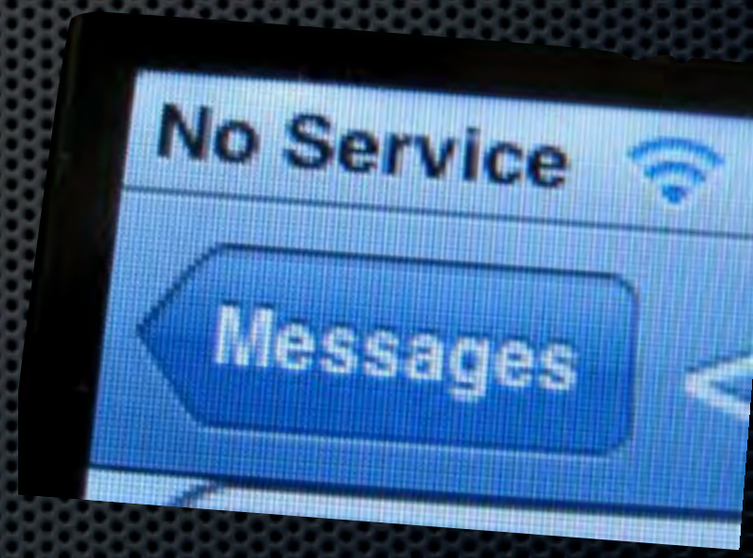
Israel

- 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...)

CyberWar - Attack

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

In conjunction with a **kinetic** attack



OR

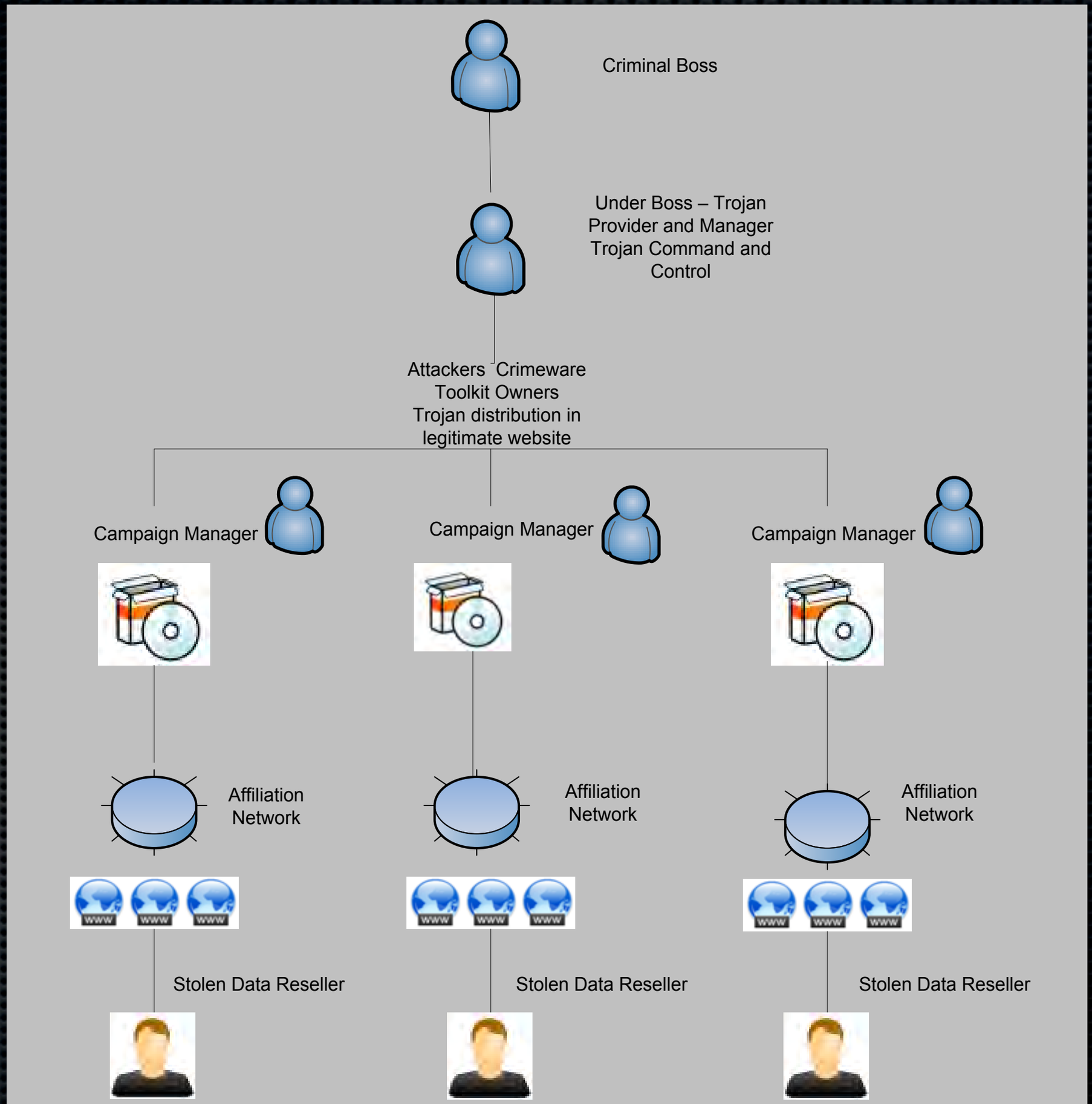
Massive **DDOS** in order to "black-out" a region, **disrupt** services, and/or push political agenda (**propaganda**)

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

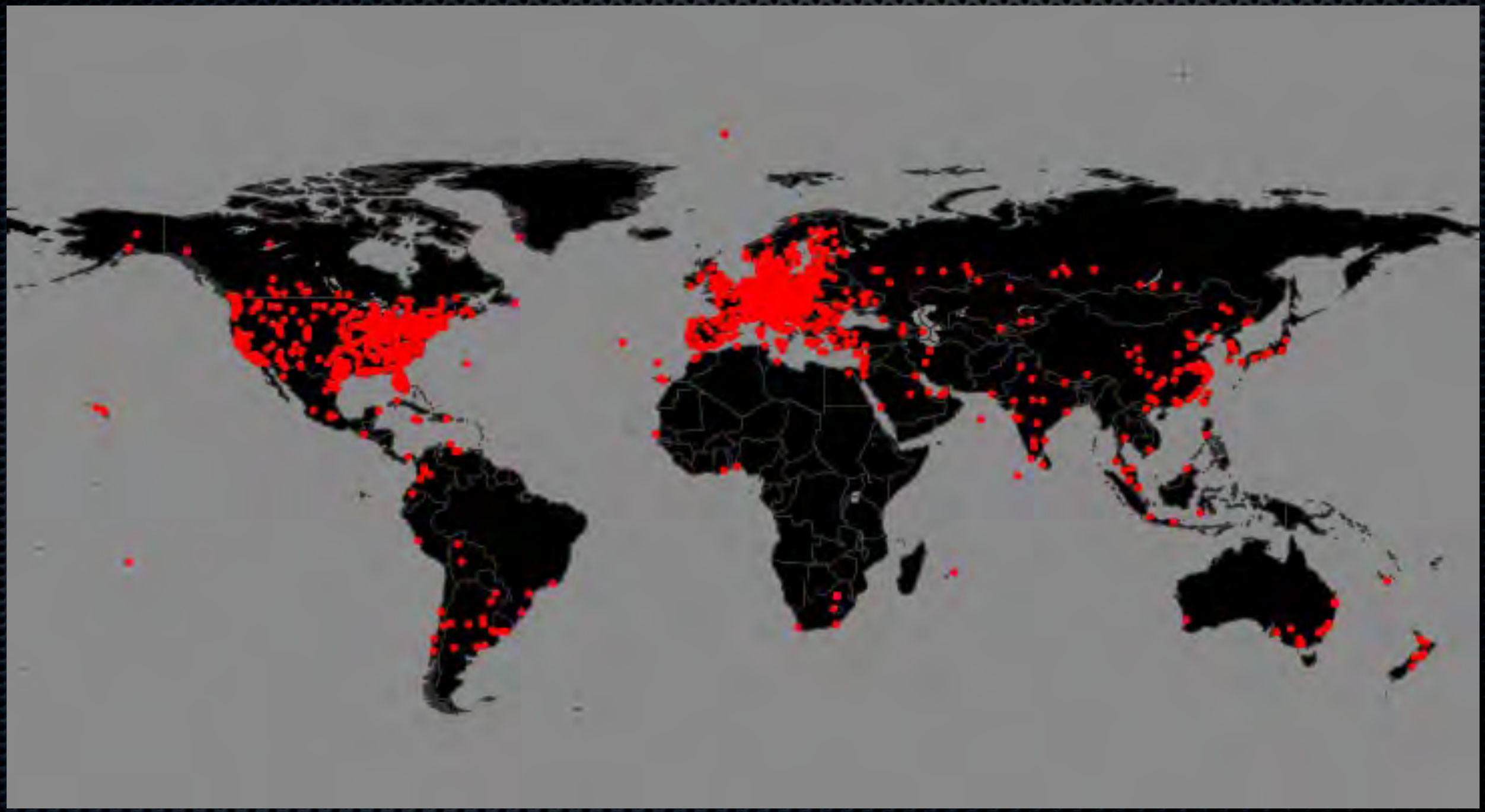
You want money, you gotta play like the big boys do...



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

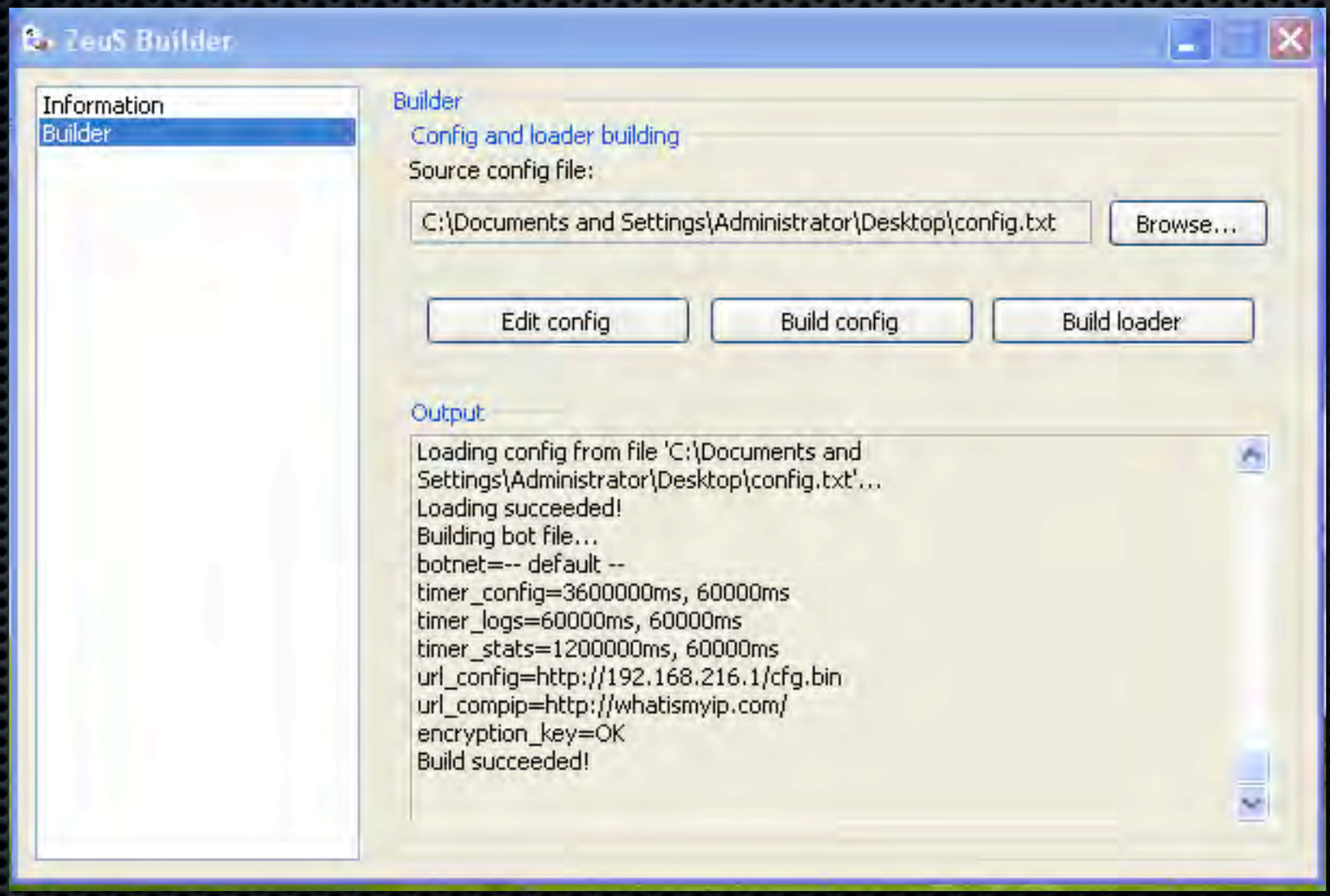
CyberCrime - target location



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:

→ Su

Botnet:

Onlin
Remo

Logs:

Searc
Searc
Uploa

System

Profil
Profil
Optio

Logou

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: US CompID's:
Botnets: IP's:
Type: Any Apply

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?

- 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

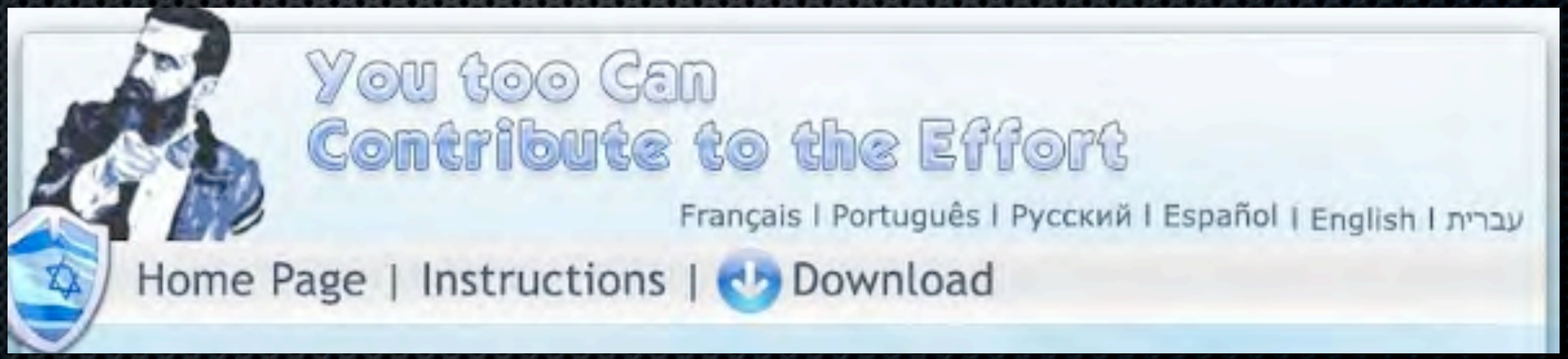
Cast led 2nd Lebanon war

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

Political post

Selling 1600 visa cards

Buying/Selling cards for 1/2 their balance

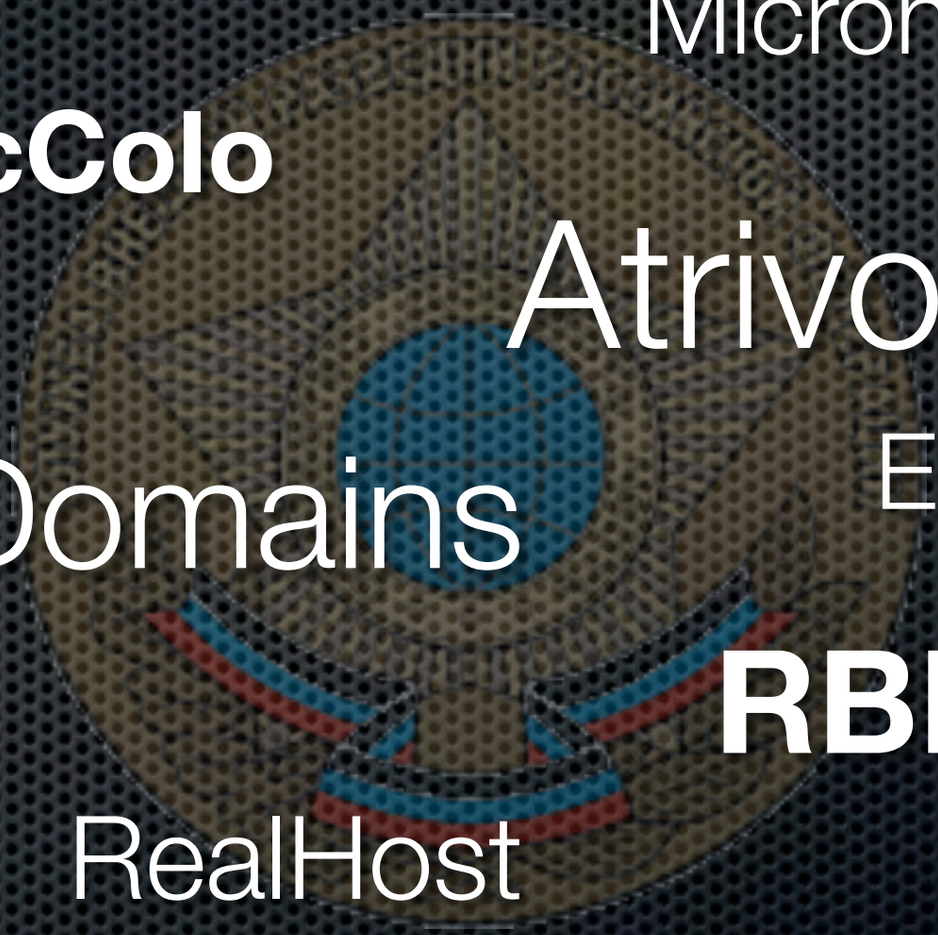
History - Revisited...

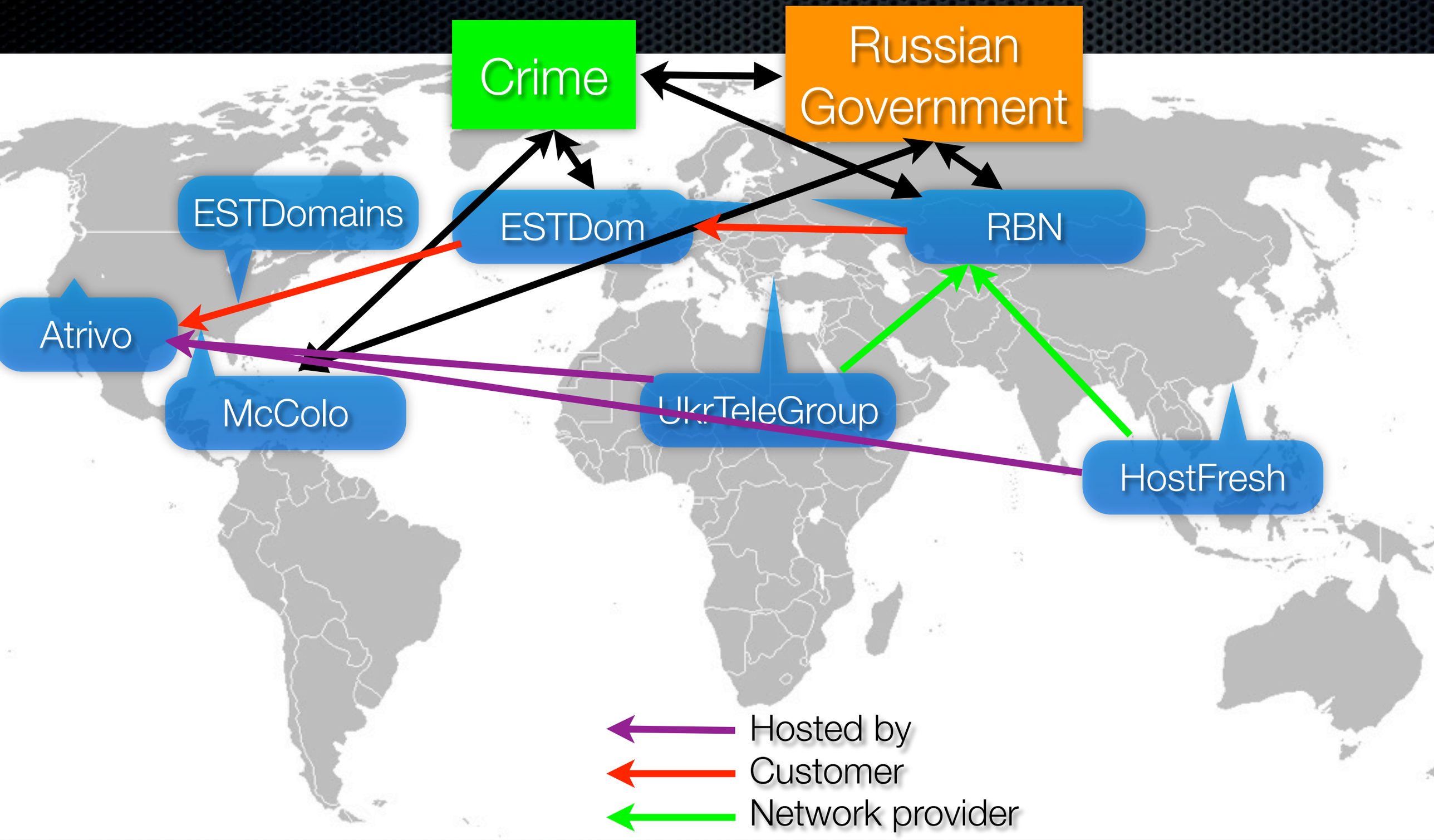
Georgia

More interesting...

Highly synchronized **Kinetic** and **Cyber** attacks
Targets still mostly **civilian**
Launched from **civilian** networks

Russian Crime/State Dillema




Crime
Russian Government
ESTDomains
ESTDom
RBN
Atrivo
McColo
UkrTeleGroup
HostFresh
Hosted by
Customer
Network provider

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

☆ IRANIAN CYBER ARMY ☆

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

IRANIAN.CYBER.ARMY@GMAIL.COM

twitter - Google Search

http://www.google.com/search?hl=en&source=hp&q=twitter&aq=f&oq=&aqi

Web Images Videos Maps News Shopping Mail more ▼

Google twitter Search Advanced Search

Web Show options... Results 1 - 10 of

This Web Site Has Been Hacked By Iranian Cyber Army - [Translate this page]
بنام خدا به عنوان یک ایرانی در پاسخ به دخالت های شیطنت آمیز این سرویس دهنده به دستور مقامات آمریکایی در امور داخلی کشورم) ...
twitter.com/ - Cached - Similar

Search
Blog
Help
Advanced Search
Status
API
Contesting account suspension

More results from twitter.com »

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://dln.nasa.gov/dln/
Web server: Apache

IP address: 209.235.106.124
Notifier stats

Your Box 0wn3z 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 0wn3z 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-Hezbolla 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

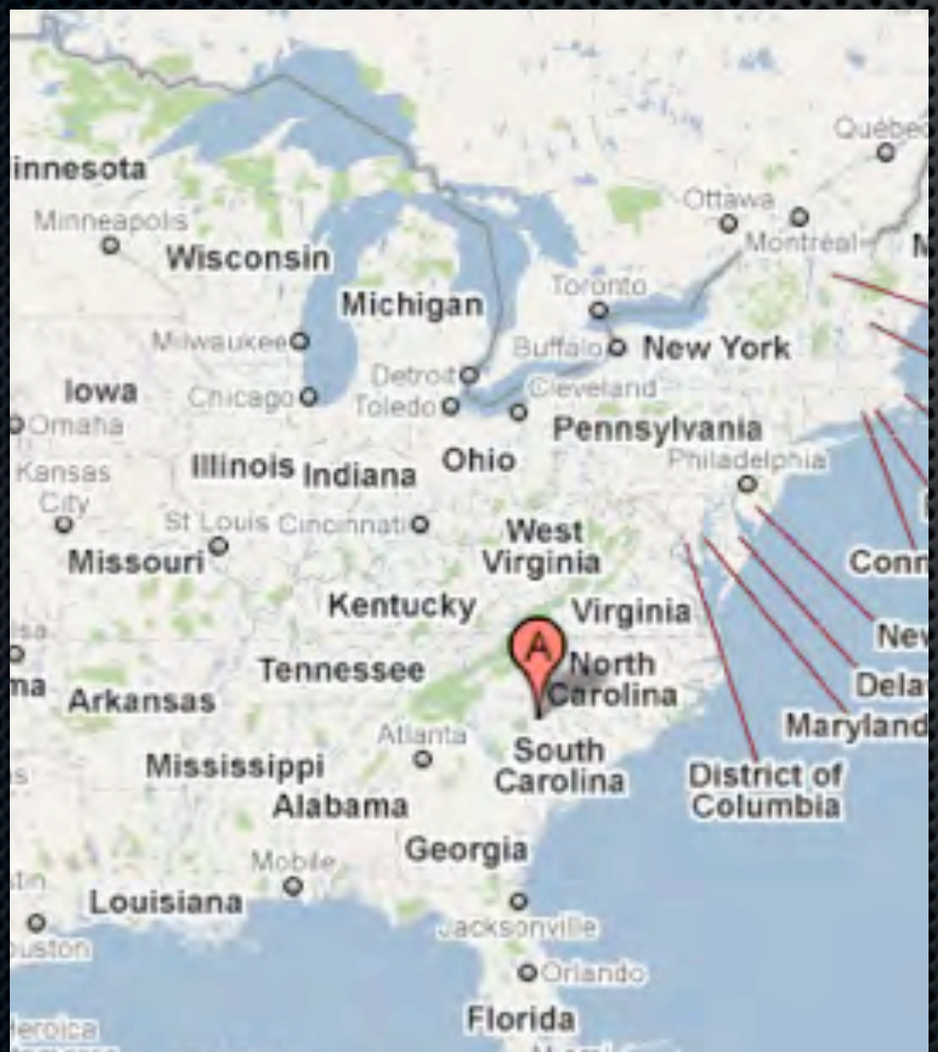
Let’s take a look at how Ashiyane operates...

On [Crime|War] training

Ashiyane forums

WarGames

Wargame 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

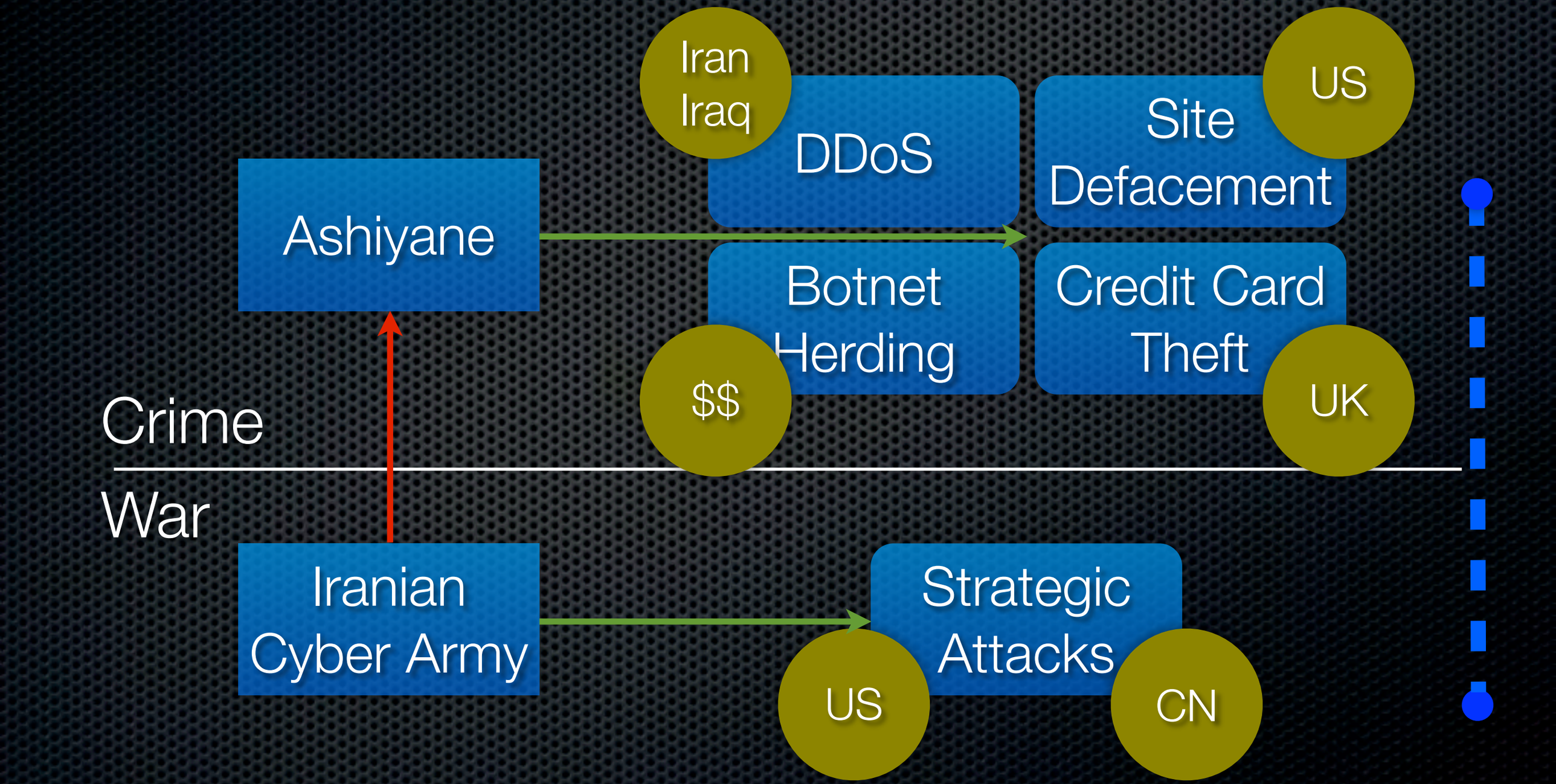
Iraq's Foreign Minister Says Well Along Disputed Southern Border Taken by Soldiers; Spokesman Says Iran Violated Sovereignty

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
- Bulletpfoof 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/iiamit

blog: iamit.org/blog