



# Cyber[Crime|War]

## Connecting the Dots

Iftach Ian Amit

VP Consulting, Security Art

Board Member - CSA Israel

IL-CERT Dreamer

DC9723



# Agenda

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



# Who Am I



# Picking up where we left off

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



# We took a trip down the rabbit hole

Only to find that we are facing a business as organized as a Fortune 500 one





Time: US 07:07 UK 13:07 RUS 16:07  
Date: 10 July

www **ROBOTRAFF** .COM

MAIN NEWS STOCK EXCHANGE FEEDBACK INFO

No	ID	Name	Price, 1K	Daily / Hourly	Wanted	Force/free force	Value/force	Emission	Invest plan	Creator ID
7	653	Туристический RU	6.5	118/9	6653	0/0	1000	N/A	N/A	2679 Unchk
8	603	Женское белье	5.2	44/6	5609	0/0	1000	N/A	N/A	1480 Unchk
9	722	Euro Fun redirect	3.9	235/9	3890	1/1	30000	24%	75.9%	1078 Unchk
10	624	SE	2.6	783/47	2702	0/0	0	N/A	N/A	2621 Unchk
11	670	E-Commerce RU	6.5	350/13	2642	0/0	1000	N/A	N/A	2679 Trust
12	733	100% Украин!!!	9.1	562/27	1044	0/0	1000	N/A	N/A	2040 Trust

AverageVisitors/month -1 | ID: 641 AverageVisitors/month -1377 | ID: 653 AverageVisitors/month -33 | ID: 670 AverageVisitors/month -1

RoboAnalytics  
Analytic reviews and articles

BALANCE: 0 LOGOUT  
LOGIN: icen STATUS: User

STATISTIC  
My Orders My Threads  
MY PROFILE  
CREATE ORDER  
SELL TRAFFIC  
SERVICES  
Tags Proof Calc  
Links Test  
FINANS  
Add Funds Get Funds Transactions  
TICKETS  
New Read  
SYSTEM MESSAGES

TOP 5 WANTED TRAFFIC

Name	Price	Wanted
RoboAnalytics	3.9	16,522
Myk Traff	3.3	15,535
RoboAnalytics	2.6	14,188
RoboAnalytics	6.5	11,113

Turnover per day  
50,3058  
36,63941  
22,97301

WebTraffic (further the traffic) - is a stream of visitors on web-resource.  
Robotraff.com is the first automated stock exchange of the traffic, here you can buy the traffic by criteria interesting you and also to sell - under the price favorable to you.  
Tasks of our resource include creations of comfortable conditions both for sellers and for buyers, maintenance of the account of the traffic, money resources, guarantees for buyers of receipt of the traffic, and for sellers of duly payment.  
Features:  
• The automated service 24/7/365: "Has paid - has received"  
• Support of English and Russian languages  
• Support-service, will allow you not to forget about people presence  
• The flexible system of registration of the order allows to satisfy the most refined needs of the buyer  
• Simple and clear system for sale of the traffic on a stock exchange  
• The detailed statistics including not only on - country the contents but also such parameters as, speed of a stream of the traffic, percentage of the version of browsers, etc.  
• Opportunity of payment by various payment means: from electronic currencies up to

With markets for each aspect of the business to cater for tools, services and even bringing in leads

**ROBOTRAFF, The description of a principle of force and value of force**

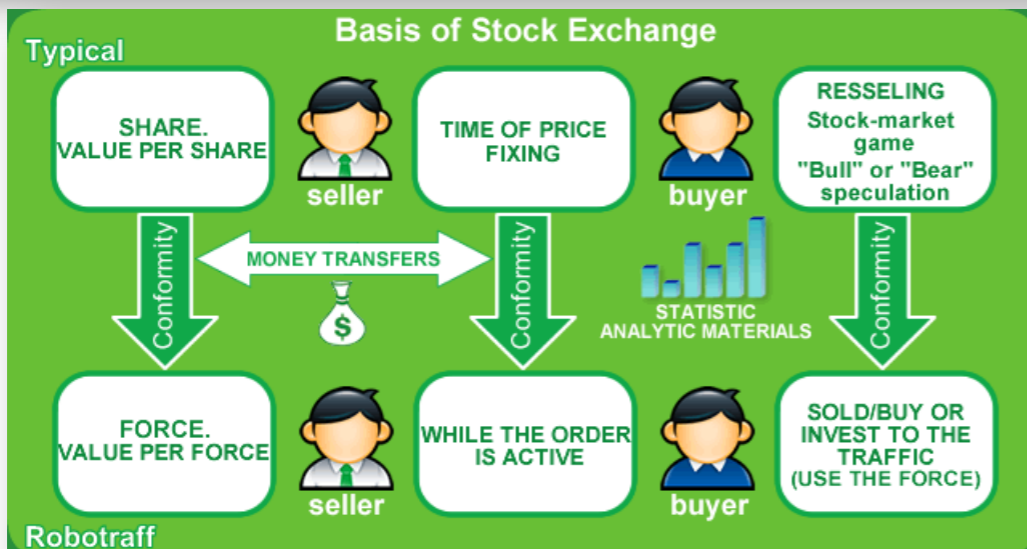
Thread of the traffic Goes with force of 8 threads ( value of force and their amount defines the seller at creation of a threads)  
**In the given example:**  
Forces: 8  
Value of force: 50 000

Some buyer who has bought the traffic with force equal 3-threads (for volume in 150 000 units). Thus, these threads go only one given order. So if to take, that the traffic speed is 5000 units per hour, the speed of the traffic on the given order will be:  
**(5000/8) \* 3 = 1875 units per hour**

Overall forces: 8  
Value of force: 50 000  
Speed of traffic: 5000/hour  
Amount of the orders: 11

The rest basic thread of the traffic which goes to other users, with force equal 5-threads. Thus, these 5 threads are distributed in regular intervals on all other orders. Under the same conditions for 10 other orders, speed equal will be:  
**((5000/8)\*5)/10 = 390 units per hour**

**The given principle allows:**  
1. To define to the seller at what volume to give the buyer the big speed. - **ISSUE of the TRAFFIC**  
2. To define to the buyer of a ratio of volume of purchase (at a constant price) and a share of possession above a thread - **BUYING UP of the TRAFFIC**  
3. Allows to the buyer having though only force of a stream to resell the traffic in volume equal bought, that is a basis of stockjobbing - **RESELLING**



# BUT!

Something didn't make too much sense in the data



Iftach Ian Amit | November 2011





# Fighter Targets Position

Target 2

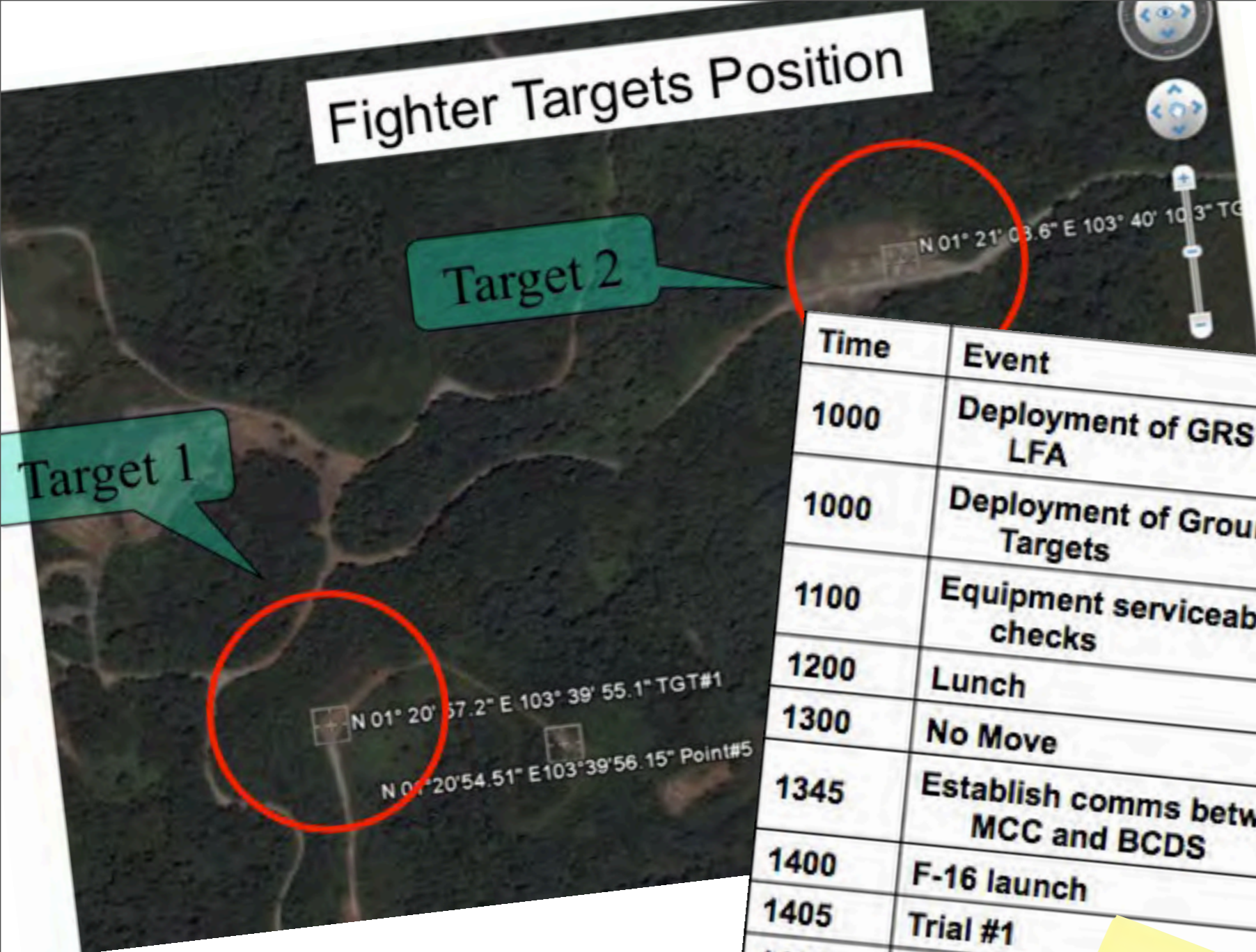
Target 1

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





# Fighter Targets Position



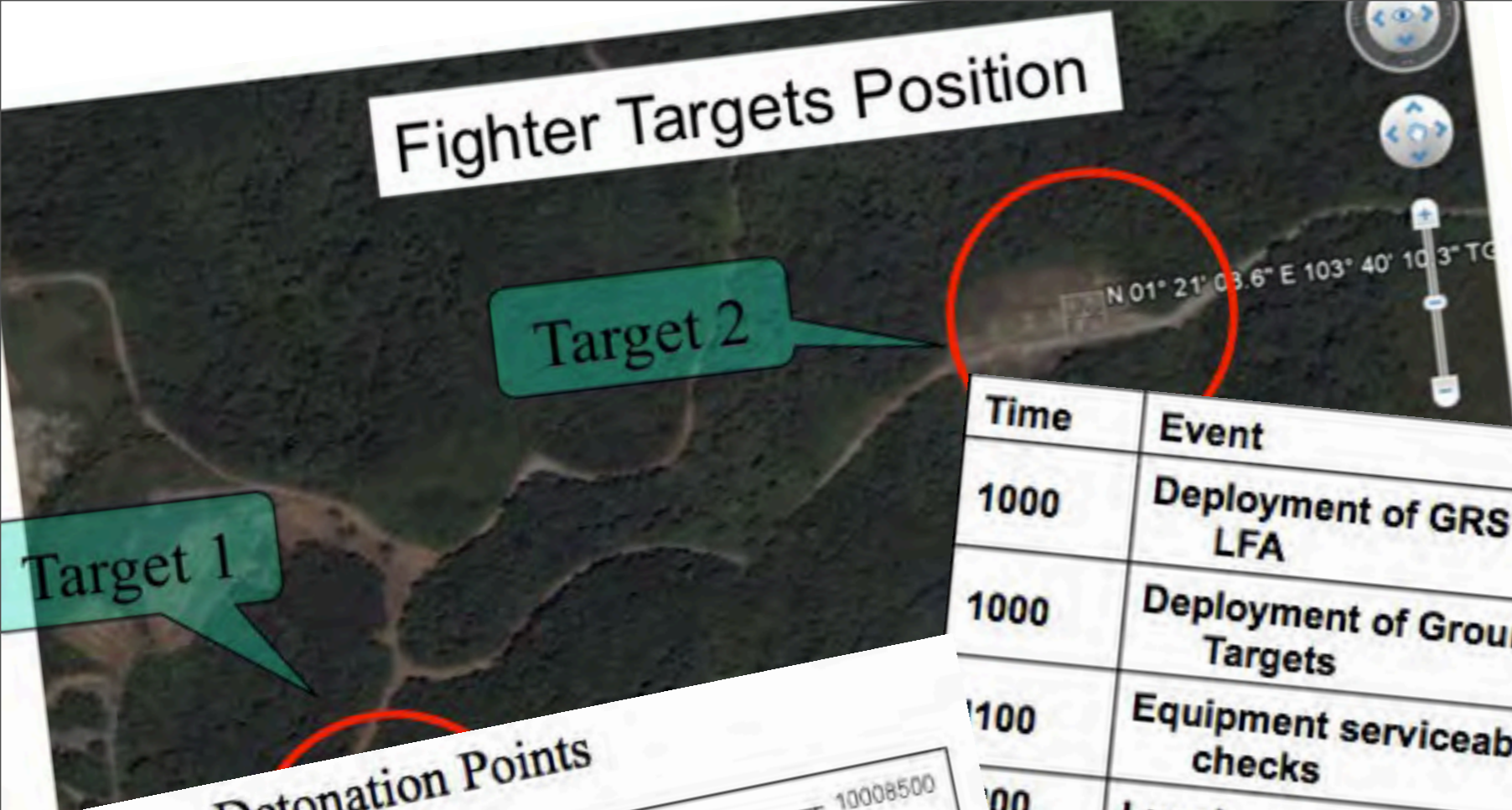
Time	Event
1000	Deployment of GRS #9 to LFA
1000	Deployment of Ground Targets
1100	Equipment serviceability checks
1200	Lunch
1300	No Move
1345	Establish comms between MCC and BCDS
1400	F-16 launch
1405	Trial #1
1410	Trial #2
1415	Trial #3a
1420	Trial #3b
1425	Trial #3c
1430	Recover
1530	Debrief

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 GR
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!**



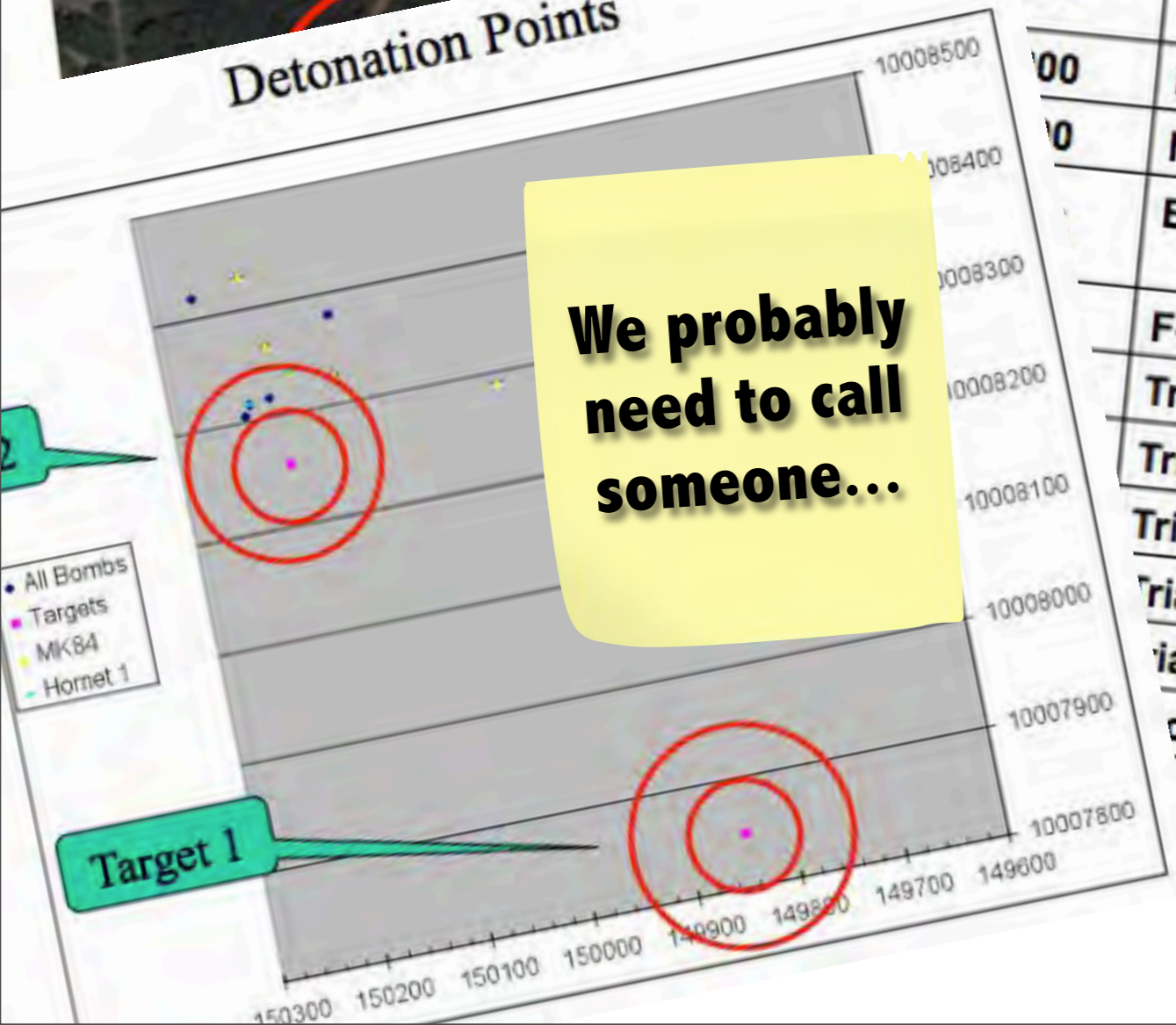
# Fighter Targets Position



Time	Event
1000	Deployment of GRS #9 to LFA
1000	Deployment of Ground Targets
1100	Equipment serviceability checks
1200	Lunch
1300	No Move
1400	Establish comms between MCC and BCDS
1500	F-16 launch
1600	Trial #1
1700	Trial #2
1800	Trial #3a
1900	Trial #3b
2000	Trial #3c
2100	cover
2200	rief

Pac kage	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

## Detonation Points



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

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



Organisation

Untitled

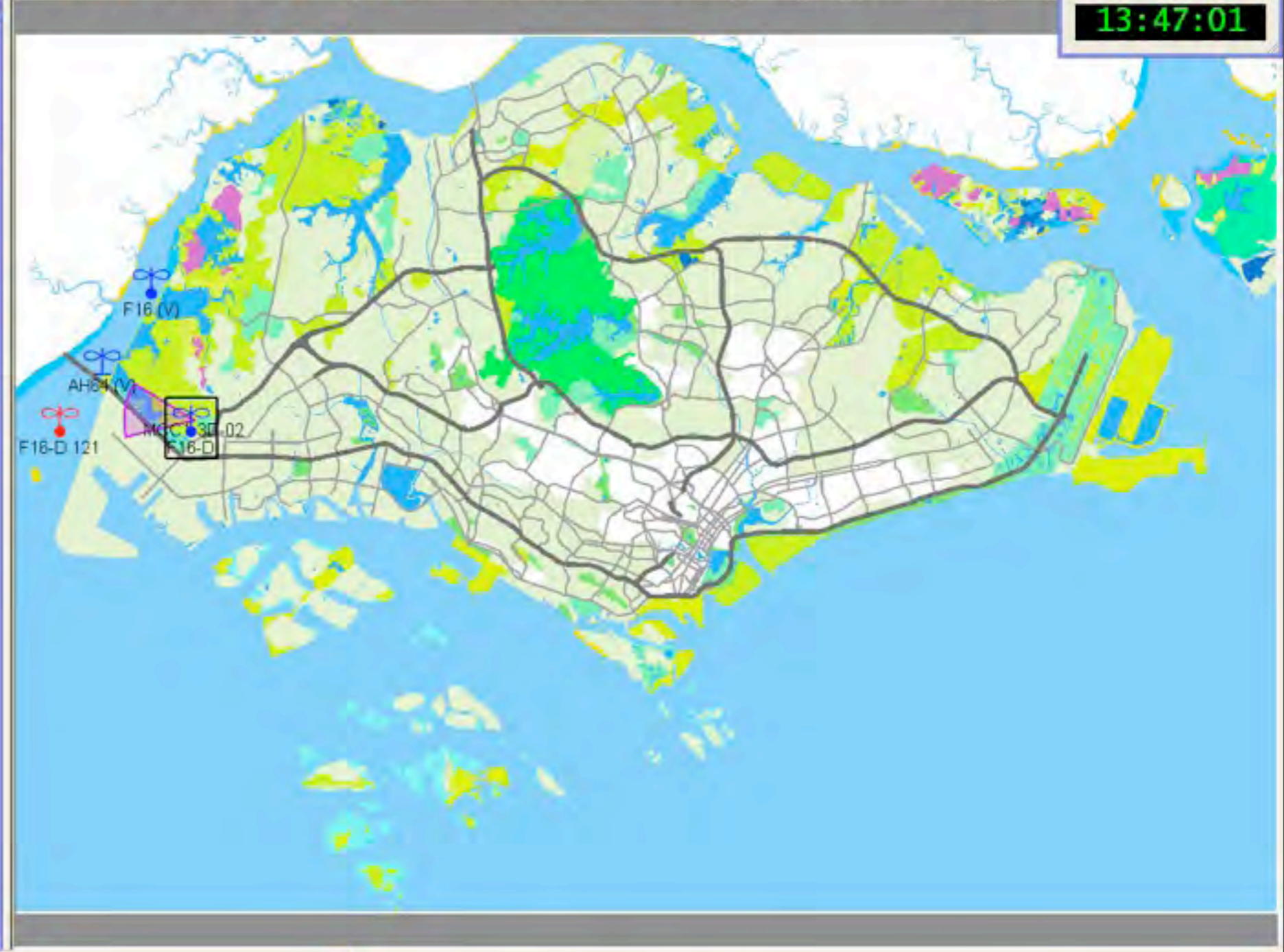
- Blue
  - BK 20342
  - AH64-D 24
  - F16-D
  - AH64-D 25
  - AH64-D 26
  - BK 20087
  - BK 20125
  - Virtual CAS
    - Pen SNP 5425
    - LAW 4488 TEST
- Red
- Virtual

01 Messages

From: EXCON

	Time	Date	

Always show last



Action Review

Battle | Technical | Weapon

Vehicles: FTF: 1 (100%)

Infantry:

Entered units:

Player/Unit details:

**F16-D**

Position: N012008E1034036

Player Unit ID: 171

Movement rate: 0

Engagement duration: 00:00:00

Associated unit:

Report

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).





**Technical | Weapon**

Infantry Entered units

Player/Unit details

 **F16-D**

**Position:** N012008E1034036

**Player Unit ID:** 171

**Movement rate:** 0

**Engagement duration:** 00:00:00

**Associated unit:**

Report

Time	F
! 13:46:39	A
! 13:46:39	F
! 13:46:16	F
! 13:45:57	A
! 13:45:57	F
! 13:45:35	F
! 13:44:51	F
! 13:44:28	F
! 13:44:08	F
! 13:43:45	F
! 13:43:21	F
! 13:42:58	F

F16-D





### Report

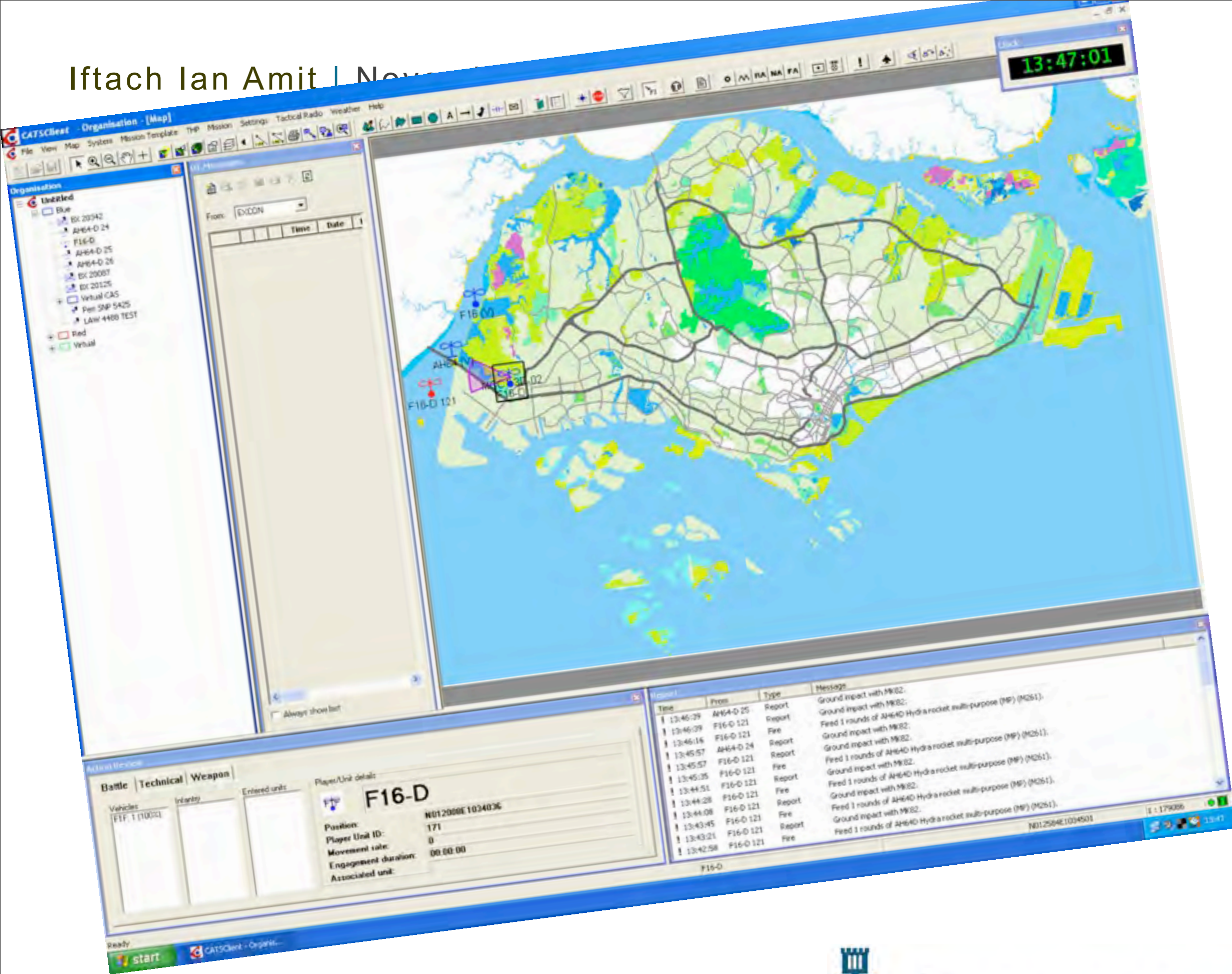
Time	From	Type	Message
! 13:46:39	AH64-D 25	Report	Ground impact with MK82.
! 13:46:39	F16-D 121	Report	Ground impact with MK82.
! 13:46:16	F16-D 121	Fire	Fired 1 rounds of AH64D Hydra rocket multi-purpose (MP) (M261).
! 13:45:57	AH64-D 24	Report	Ground impact with MK82.
! 13:45:57	F16-D 121	Report	Ground 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).

F16-D

N012584E1034501







# Hungry yet?

That was just the appetizer..





# Question 1: What is **this**?



# 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 (org. 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?





# It **did not** happen yet RSA      being an exception?



# It **did not** happen yet RSA being an exception?







This is not the **only** way!



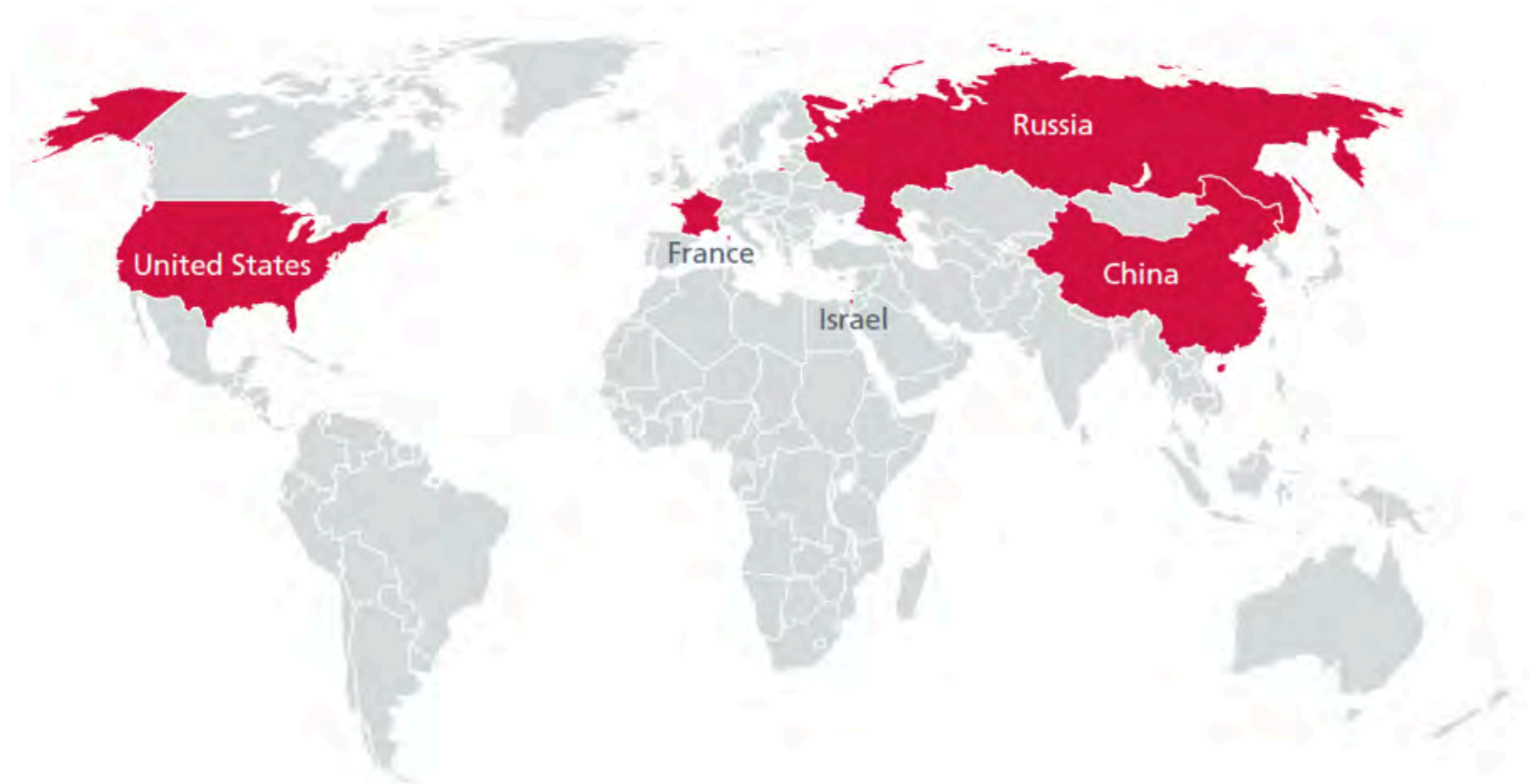
Neither is this...



But civilian are **always** at stake!



# Many faces of how CyberWar is perceived..



From McAfee's "Virtual Criminology Report"

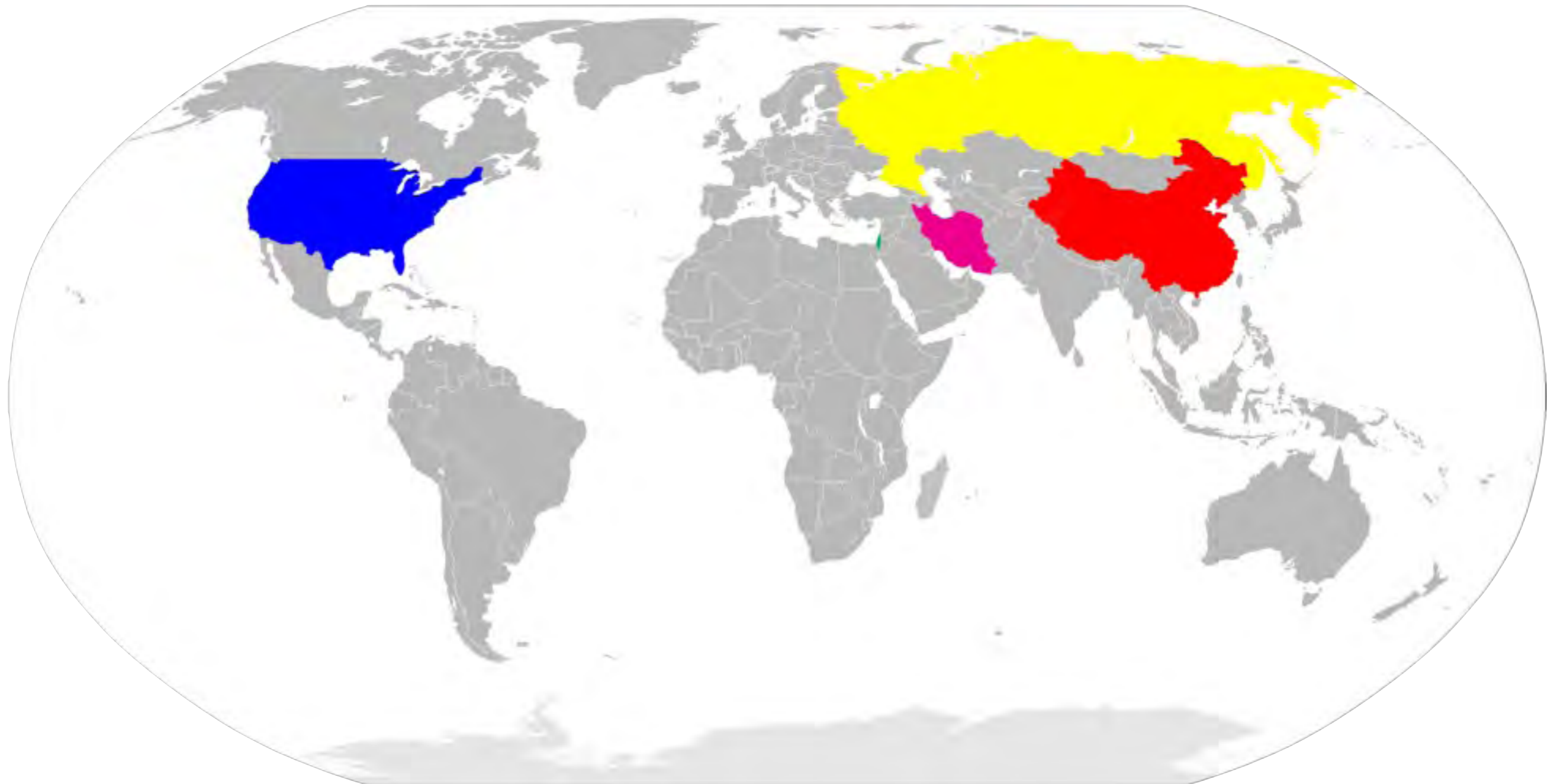
Image caption:

*"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...



*Going above and beyond traditional security*



# 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



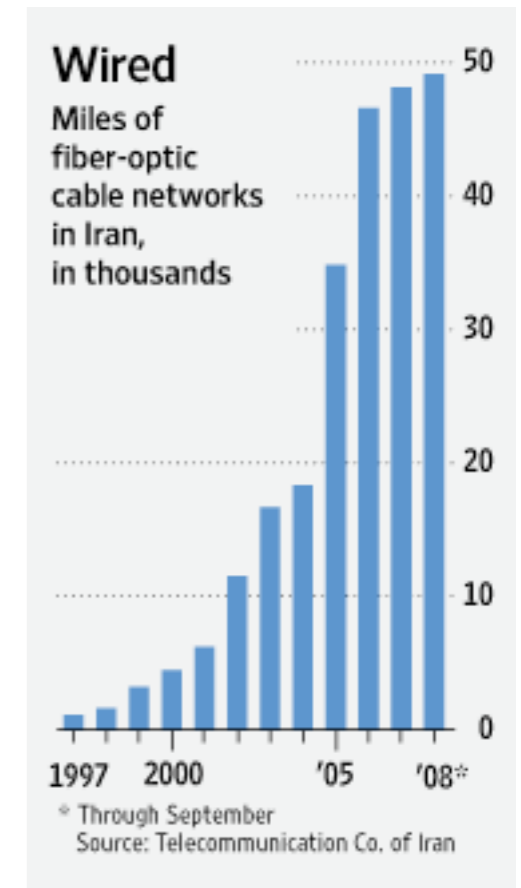
- PLA (People's Liberation Army)
- Homework: read the Northrop Grumman, and the "Project 2049 Institute" reports!
- General Staff Department 4th Department - Electronic Countermeasures == Offense
- GSD 3rd Department - Signals Intelligence == Defense
- Yes...Titan Rain...





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





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

**Israel Adds Cyber-Attack to IDF**

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



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

**Israel Adds Cyber-Attack to IDF**

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





# CyberWar - Attack

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

In conjunction with a **kinetic** attack



# CyberWar - Attack

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

In conjunction with a **kinetic** attack

**OR**





# 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



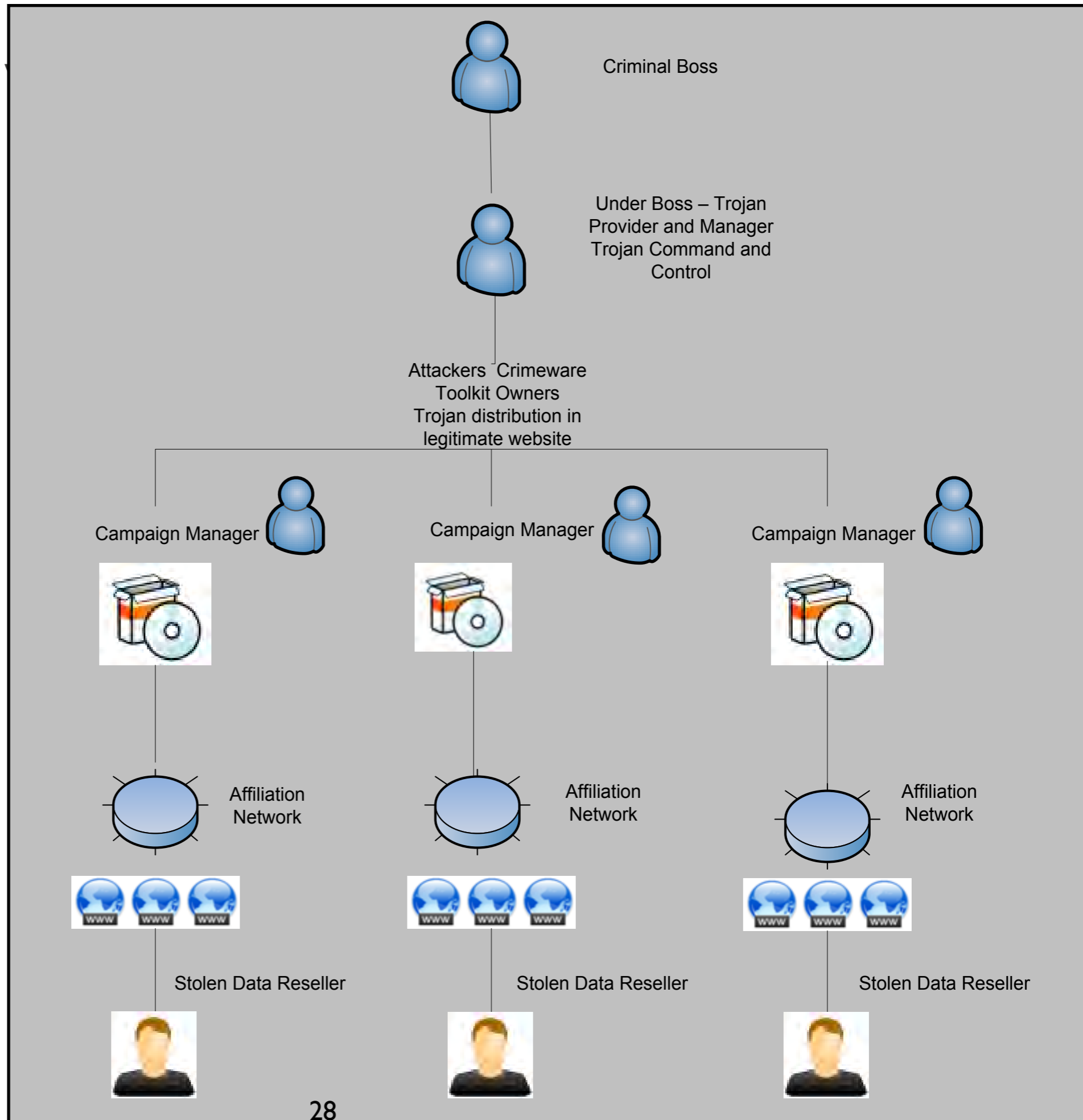


# CyberCrime





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

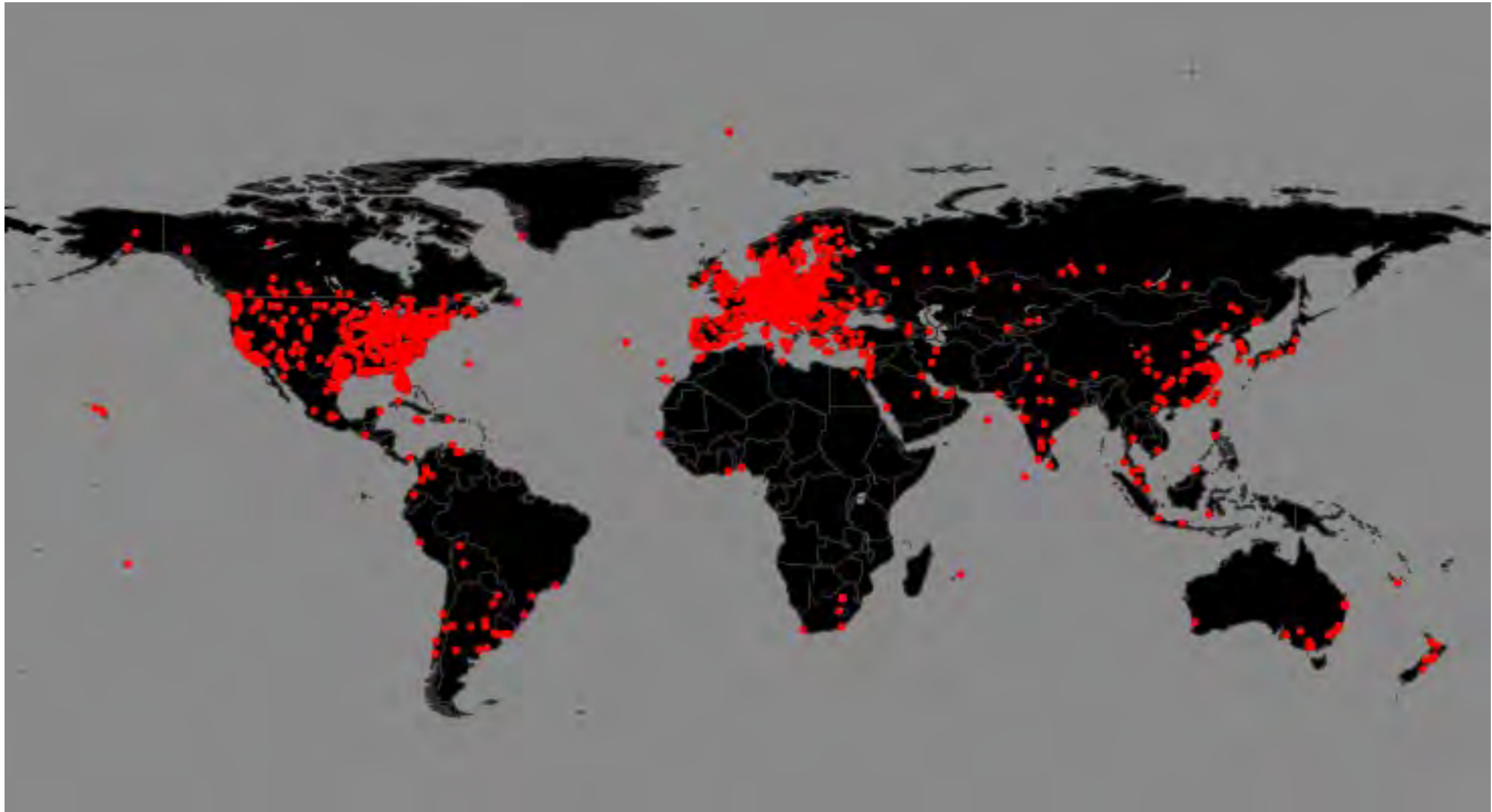


# CyberCrime - Attack

- 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 locations



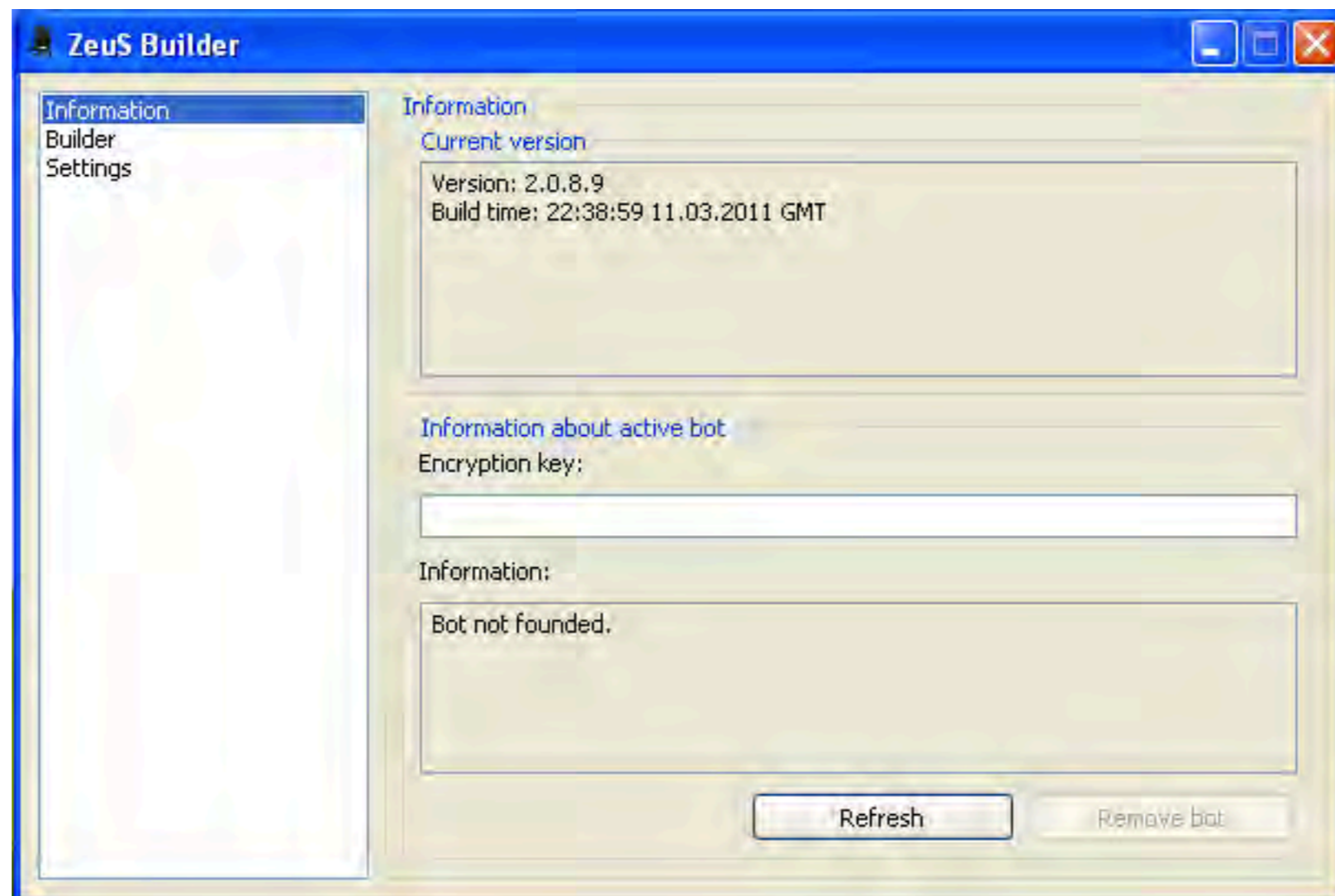


# CyberCrime - Locations

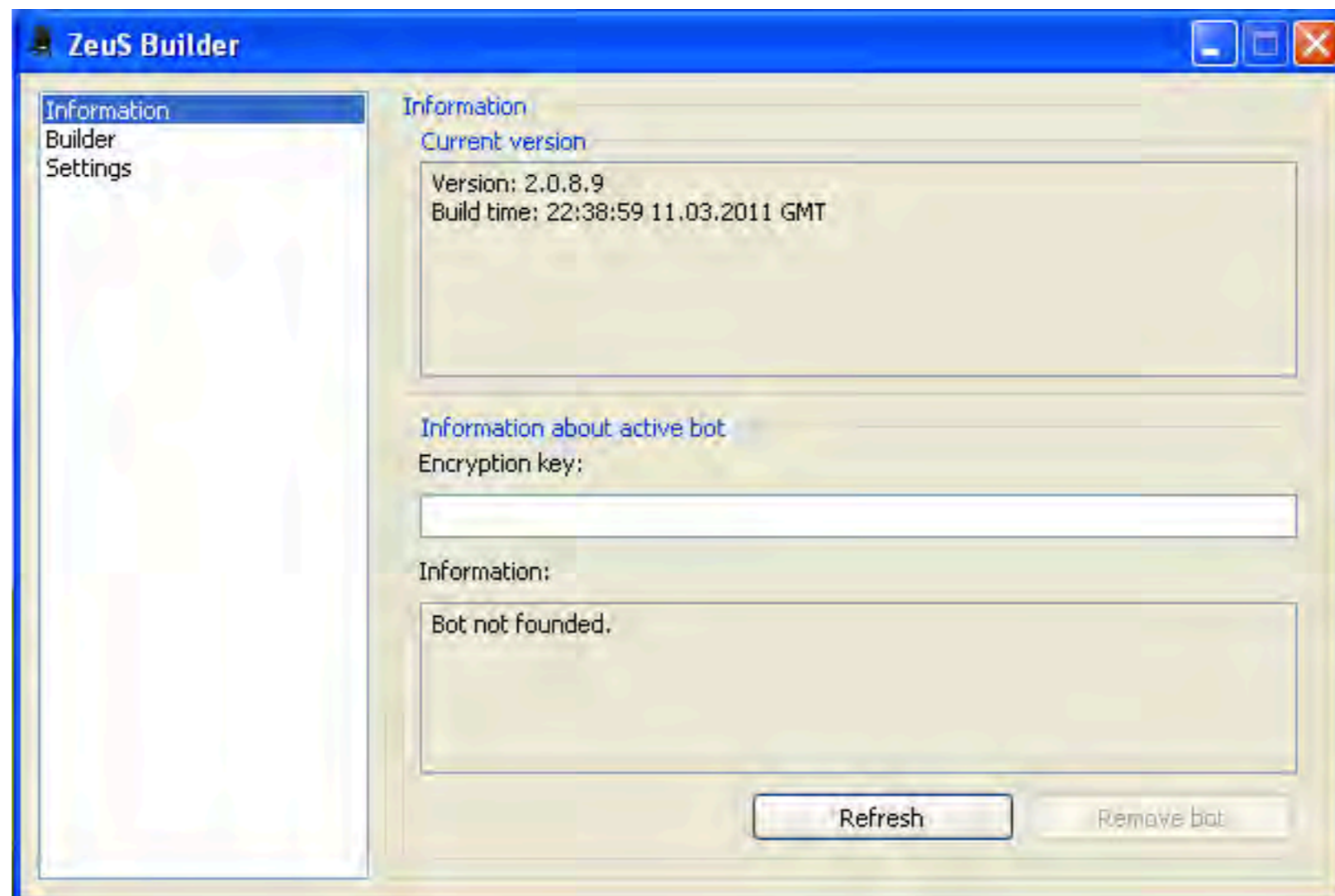


Major Cybercrime group locations

# CyberCrime - Ammunition



# CyberCrime - Ammunition

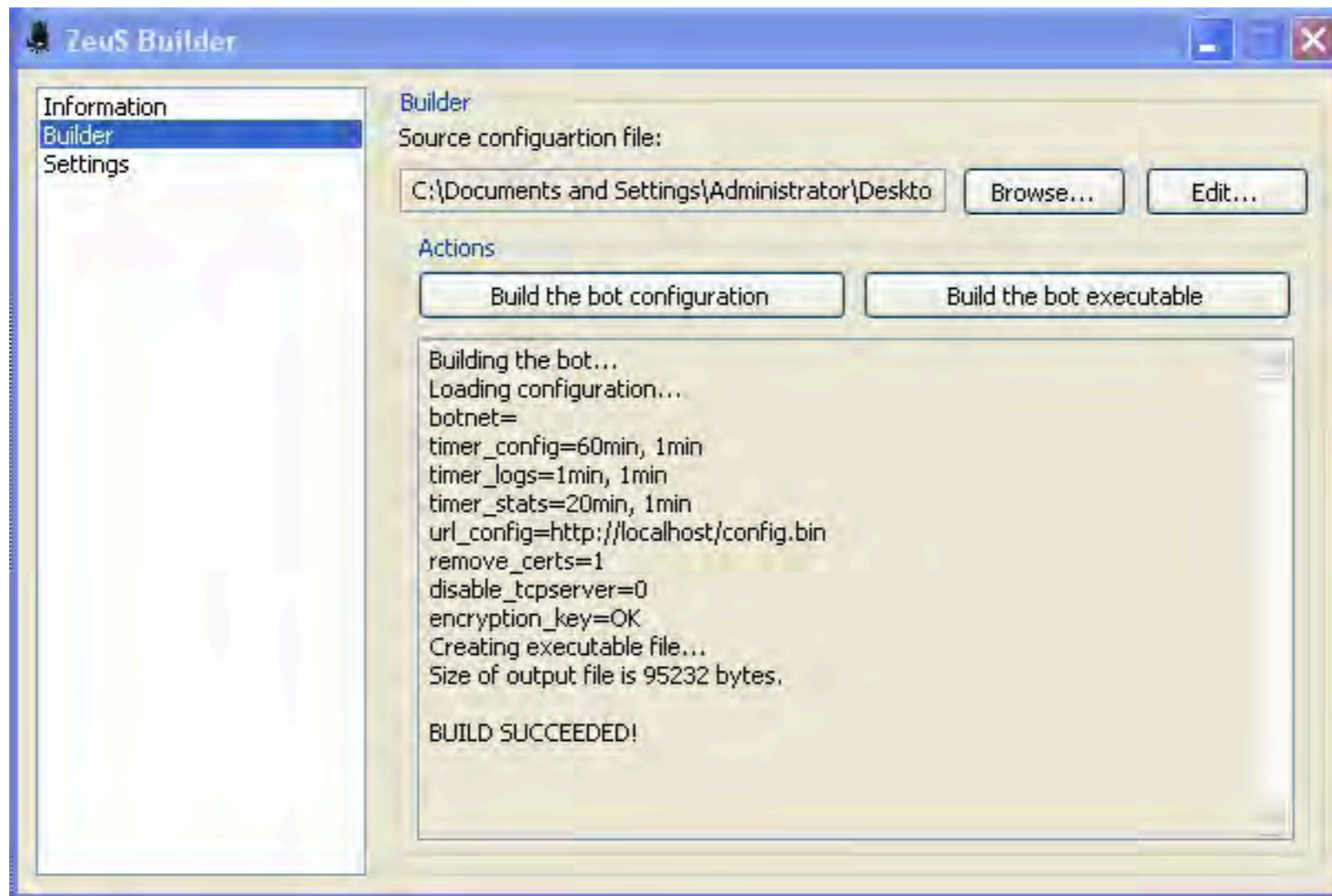


=  $\approx$  APT





# CyberCrime - Ammunition



=  $\approx$  APT



## Zeus :: Statistics

### Information:

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

### Statistics:

→ Summary

### Botnet:

Online bots  
Remote commands

### Logs:

Search  
Search with template  
Uploaded files

### System:

Profiles  
Profile  
Options  
Logout

### Information

Total logs in database:	203
Time of first install:	16:10:06 26.03.2008
Total bots:	535
Total active bots in 24 hours:	364

Botnet: Any >>

Installs (253)	Reset	Online bots (104)	Reset
US	67	US	43
--	48	--	15
MX	16	BR	9
AU	15	MX	9
IN	9	RU	4
DE	9	BH	3
ES	6	PE	2
UK	6	UA	2
PL	5	FR	1
IR	5	IN	1
PK	4	VN	1
BR	4	PT	1
CO	4	ES	1
RU	4	TH	1



## Zeus :: Statistics

### Information:

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

### Statistics:

→ Summary

### Information

Total logs in database:	203
Time of first install:	16:10:06 26.03.2008
Total bots:	535
Total active bots in 24 hours:	364

## CP :: Search in database

### Information:

Current user: admin  
GMT date: 15.04.2011  
GMT time: 17:59:15

### Statistics:

Summary

### OS

### Botnet:

Bots  
Scripts

### Reports:

→ Search in database  
Search in files

### System:

Information  
Options  
User  
Users

### Filter

Search from date (dd.mm): --.-- to date: --.--

Bots:

Botnets:

IP-addresses:

Countries:

Search string:

Type of report:

- Case sensitive.  
 Exclude retries of contents (for one day only).  
 Show only reports (don't show names of bots).  
 Show as text (text/plain).

Reset form

Search

Remove





# CyberCrime - Defense



# CyberCrime - Defense

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



# CyberCrime - Defense

- Anti [ Virus | Malware | Spyware | Rootkit | Trojan ]
- Seriously?





# CyberCrime - Defense

- Anti [ Virus | Malware | Spyware | Rootkit | Trojan ]
- Seriously?



# CyberCrime - Defense

- Anti [ Virus | Malware | Spyware | Rootkit | Trojan ]
- Seriously?

File name:	<b>bot.exe</b>
Submission date:	<b>2011-04-15 18:16:04 (UTC)</b>
Current status:	<b>finished</b>
Result:	<b>0 / 42 (0.0%)</b>



# CyberCrime - Defense

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

- Seriously?

File name:	<b>bot.exe</b>
Submission date:	<b>2011-04-15 18:16:04 (UTC)</b>
Current status:	<b>finished</b>
Result:	<b>0 / 42 (0.0%)</b>

- Firewalls / IDS / IPS





# CyberCrime - Defense

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

- Seriously?

File name:	<b>bot.exe</b>
Submission date:	<b>2011-04-15 18:16:04 (UTC)</b>
Current status:	<b>finished</b>
Result:	<b>0 / 42 (0.0%)</b>

- Firewalls / IDS / IPS

- Seriously?



# CyberCrime - Defense

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

- Seriously?

File name:	<b>bot.exe</b>
Submission date:	<b>2011-04-15 18:16:04 (UTC)</b>
Current status:	<b>finished</b>
Result:	<b>0 / 42 (0.0%)</b>

- Firewalls / IDS / IPS

- Seriously?

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



# CyberCrime - Defense

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

- Seriously?

File name:	<b>bot.exe</b>
Submission date:	<b>2011-04-15 18:16:04 (UTC)</b>
Current status:	<b>finished</b>
Result:	<b>0 / 42 (0.0%)</b>

- 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.

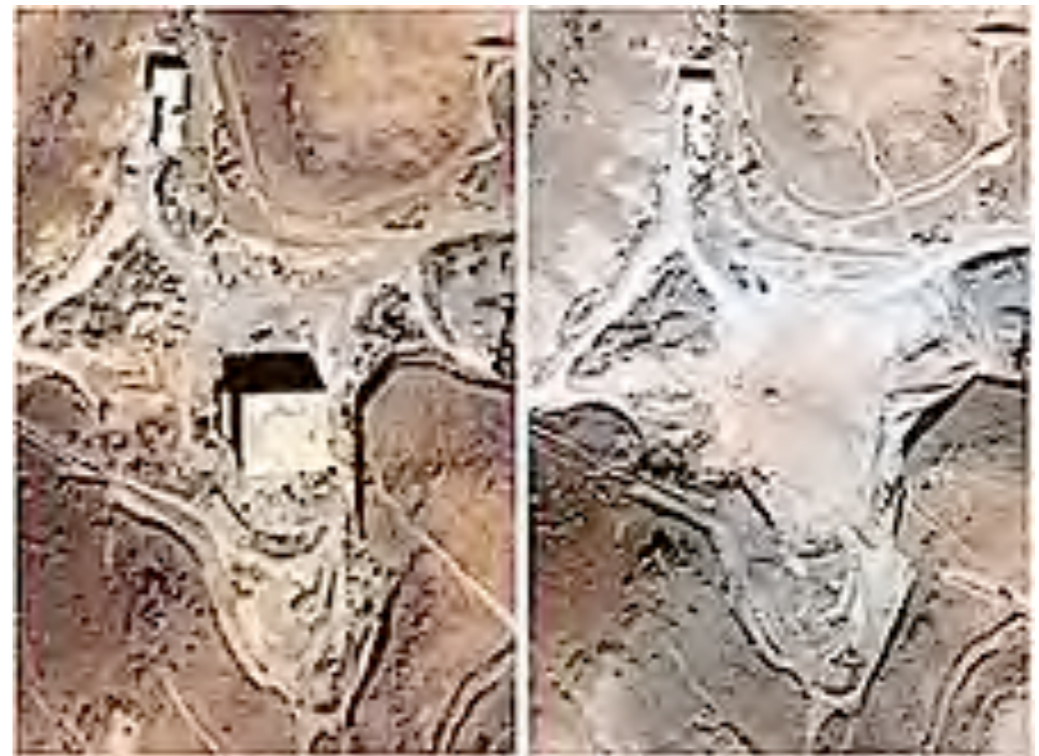
Bottom line: **civilian** infrastructure was targeted  
Attacks originated mostly from **civilian** networks



# History - Revisited...

## Israel

## Operation Orchard



Source: Der Spiegel

September 6th, 2007

Source: [http://en.wikipedia.org/wiki/Operation\\_Orchard](http://en.wikipedia.org/wiki/Operation_Orchard)





# History - Revisited...

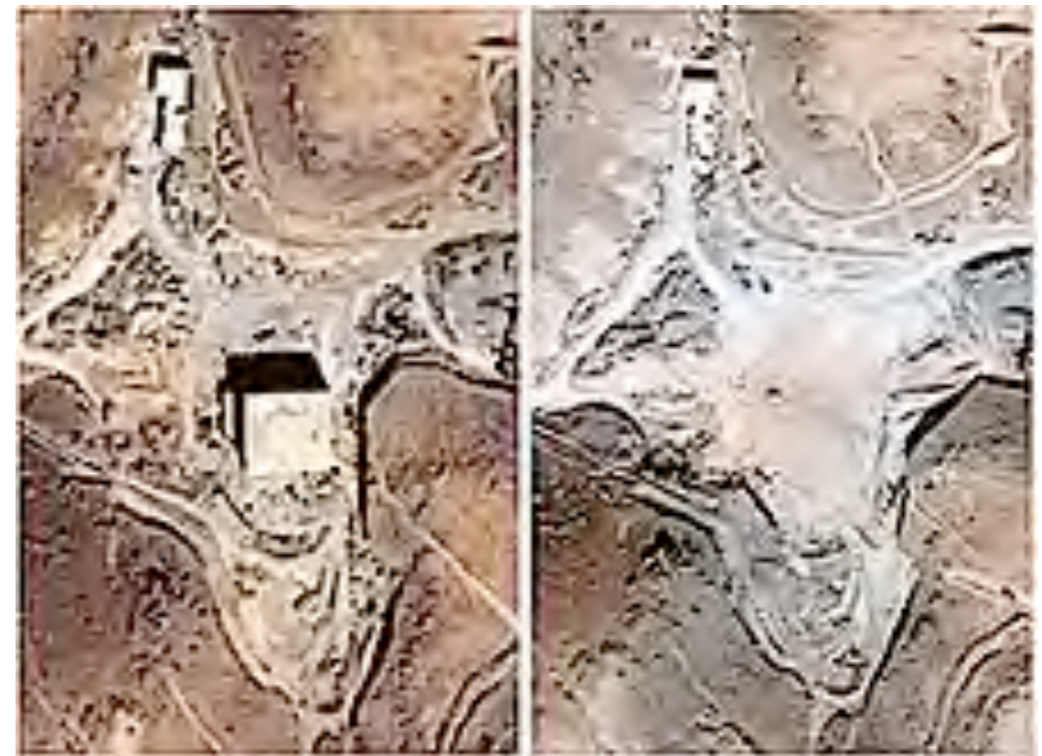
## Israel

## Operation Orchard



September 6th, 2007

Source: [http://en.wikipedia.org/wiki/Operation\\_Orchard](http://en.wikipedia.org/wiki/Operation_Orchard)



Source: Der Spiegel



# 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.

ArHack.Net: .. منظمة الهكر العربي :: .. < ... الأقسام العامة :: ... < ... قسم فلسطين :: ...  
من كمرتي بالفيديو شوف القصف في غزة (اقسم بالله دمار × دمار)

صفحة 1 من 2 < 1 2

POST REPLY

أدوات الموضوع البحث في الموضوع تقييم الموضوع طريقة عرض الموضوع

رقم المشاركة: 1

PM 01:47, 12-27-2008

من كمرتي بالفيديو شوف القصف في غزة (اقسم بالله دمار × دمار)

معلومات العضو

السلام عليكم

حرب بما معنى الكلمة والله يا اخوان

نرجو منكم الدعاء بزوال هذه الحملة المسعورة

والله بكتب لكم الموضوع والقصف شغال ولا يبعد عنى سوى 500 متر على الاكثر

لان اترككم مع التحميل لفيديو صورته من كمرتي

لتحميل



## Political post



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 | ابحث في الموضوع | تقييم الموضوع | طريقة عرض الموضوع

رقم المشاركة: 1

**كم**

**والله يا اخوان**

**الجملة المسعورة**

**يبعد عنى 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

ArHack.NET :: منظمة الهكر العربي :: < > :: الاقسام العامة :: < > :: السوق السوداء : .  
اشترته بغيزا مسروقة وخذ نصف سعره كالبش

صفحة 1 من 2 < 1 2

أدوات الموضوع | ابحث في الموضوع | تقييم الموضوع | طريقة عرض الموضوع

رقم المشاركة: 1

اشترته بغيزا مسروقة وخذ نصف سعره كالبش

يا اخواني في موقع استضافة اشترى منو مساحة الي بدك اياها وخذ نصف سعرها كاش احولك اياه ويسترن نيون .  
كل ما كانت المساحة اكبر تحصل على مبلغ اكبر  
يعني لو اشتريت 300 دولار بغيزا مسروقة بحولك 150 دولار على الويبستر نيون والله على ما اقول شهيد .  
واشترى كما تريد يعني لو اشتريت 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

PM 11:11, 11-26-2009

معلومات العضو

**ابوشهاب**  
عضو جديد :: ..

احصائية المسر

الاتساب : Nov 2009
رقم العضوية : 25036
المشاركات : 10
بمعدل : 0.23 يومياً
عدد التفاعل : 10

Political post

Buying/Selling cards for 1/2 their balance







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**

**الجملة المسعورة**

**يبعد عنى سوى 500 متر على الاكثر**

**و صورته من كمرتي**

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

أدوات الموضوع | البحث في الموضوع | تقييم الموضوع | طريقة عرض الموضوع

رقم المشاركة: 1

اشترته بغيرا مسروقة وخذ نصف سعره كالأش

يا اخواني في موقع استضافة اشترى منو مساحة الي بدك اياها وخذ نصف سعرها كاش احولك اياه ويسترن نيون . كل ما كانت المساحة اكبر تحصل على مبلغ اكبر يعني لو اشترت 300 دولار بغيرا 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

PM 11:11 , 11-26-2009

معلومات العضو

**ابوشهاب**  
عضو جديد ..

احصائية العضو

الاتساب : Nov 2009
رقم العضوية : 25036
المشاركات : 10
بمعدل : 0.23 يوميا
عدد التقاط : 10

Political post

Buying/Selling cards for 1/2 their balance

Selling 1600 visa cards

أدوات الموضوع | البحث في الموضوع | تقييم الموضوع | طريقة عرض الموضوع

رقم المشاركة: 1

شباب اريد ابادل 1601 فيسا كارد ب مقابل ???????????

شباب اريد ابادل 1601 فيسا كارد كلهم صالحين و فيهم فلوس

PM 12:55 , 12-31-2009

معلومات العضو

**هاكر 00**  
عضو جديد ..



# History - Revisited...

## Georgia

More interesting...

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

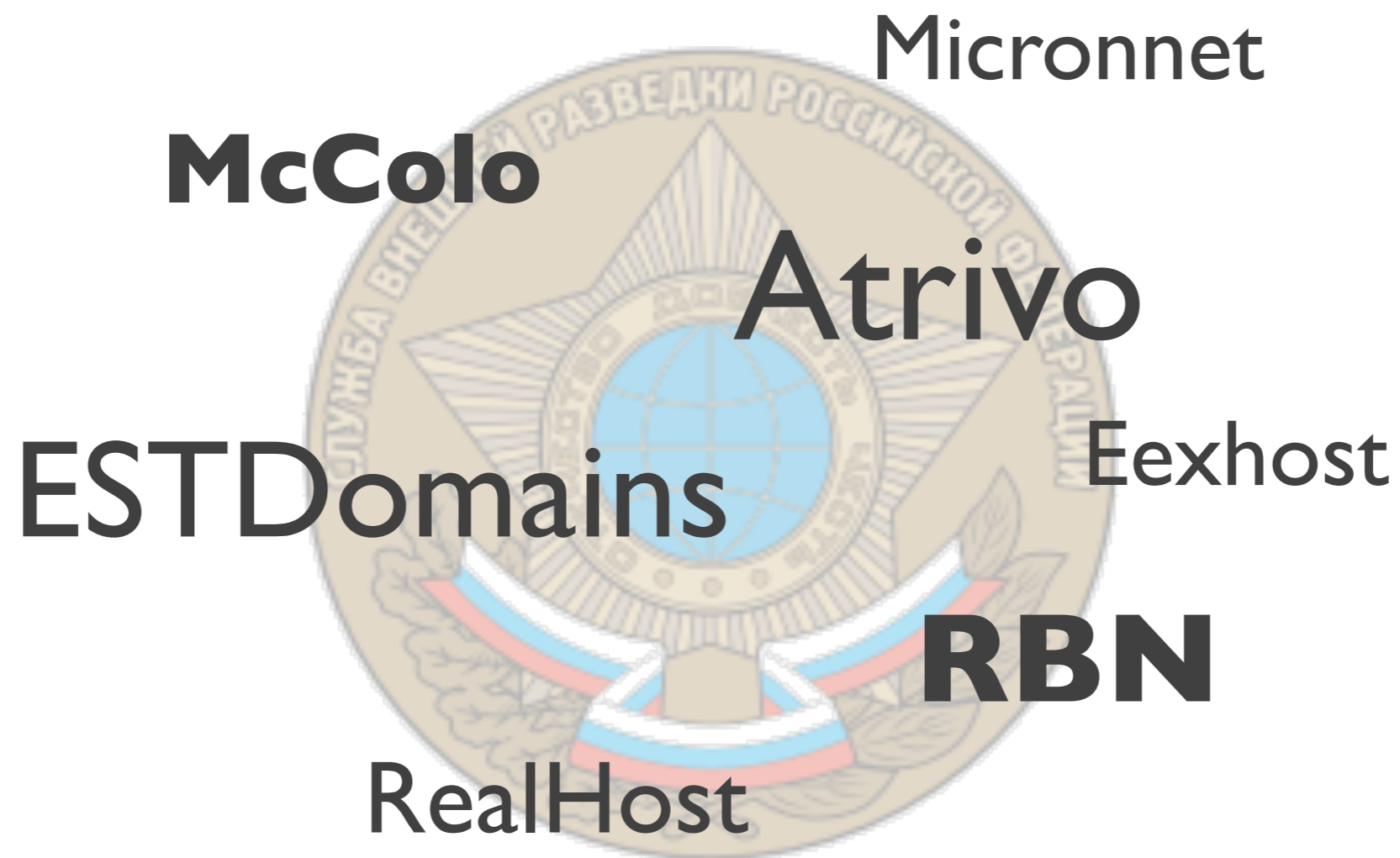
Targets still mostly **civilian**

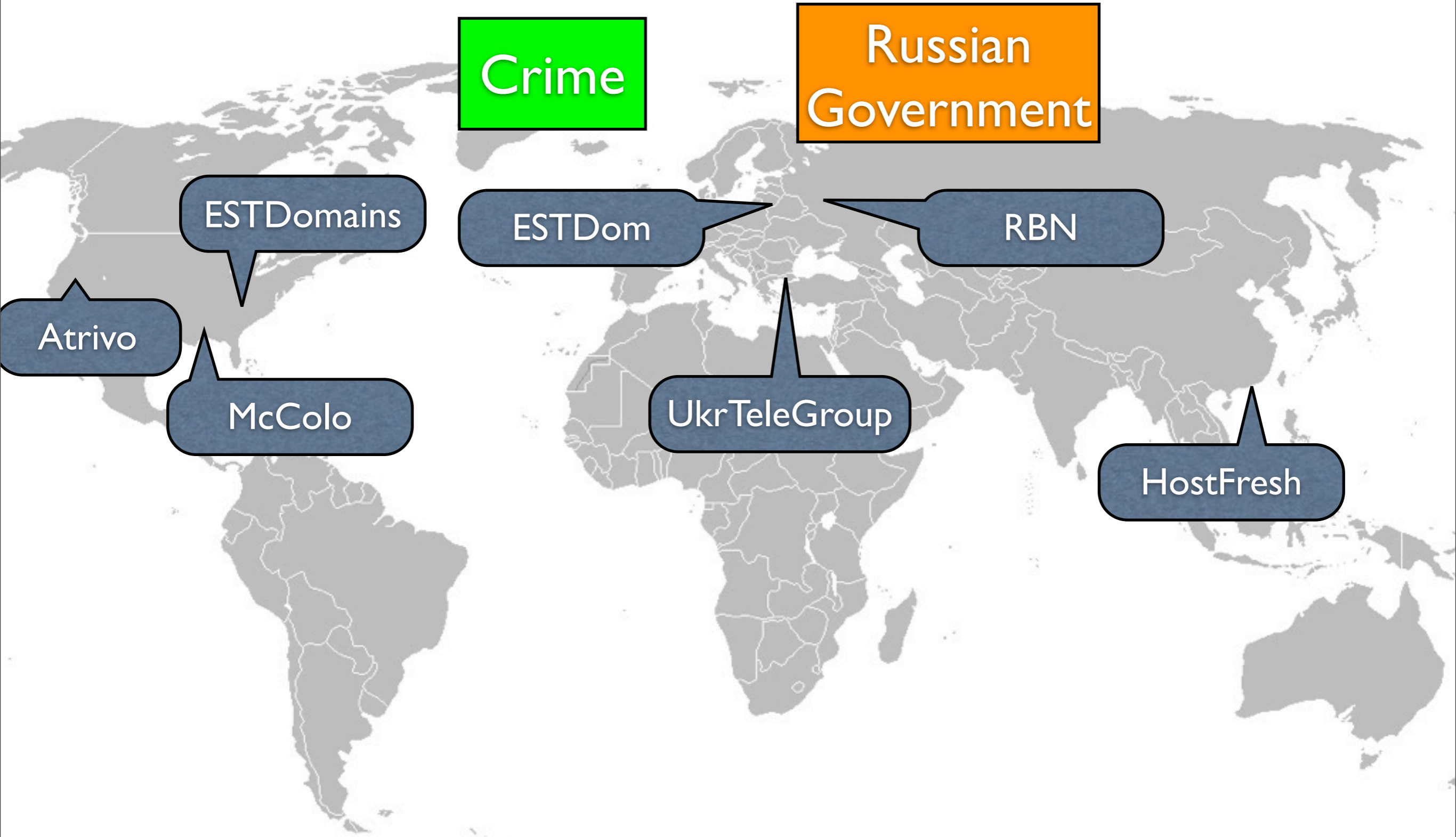
Launched from **civilian** networks



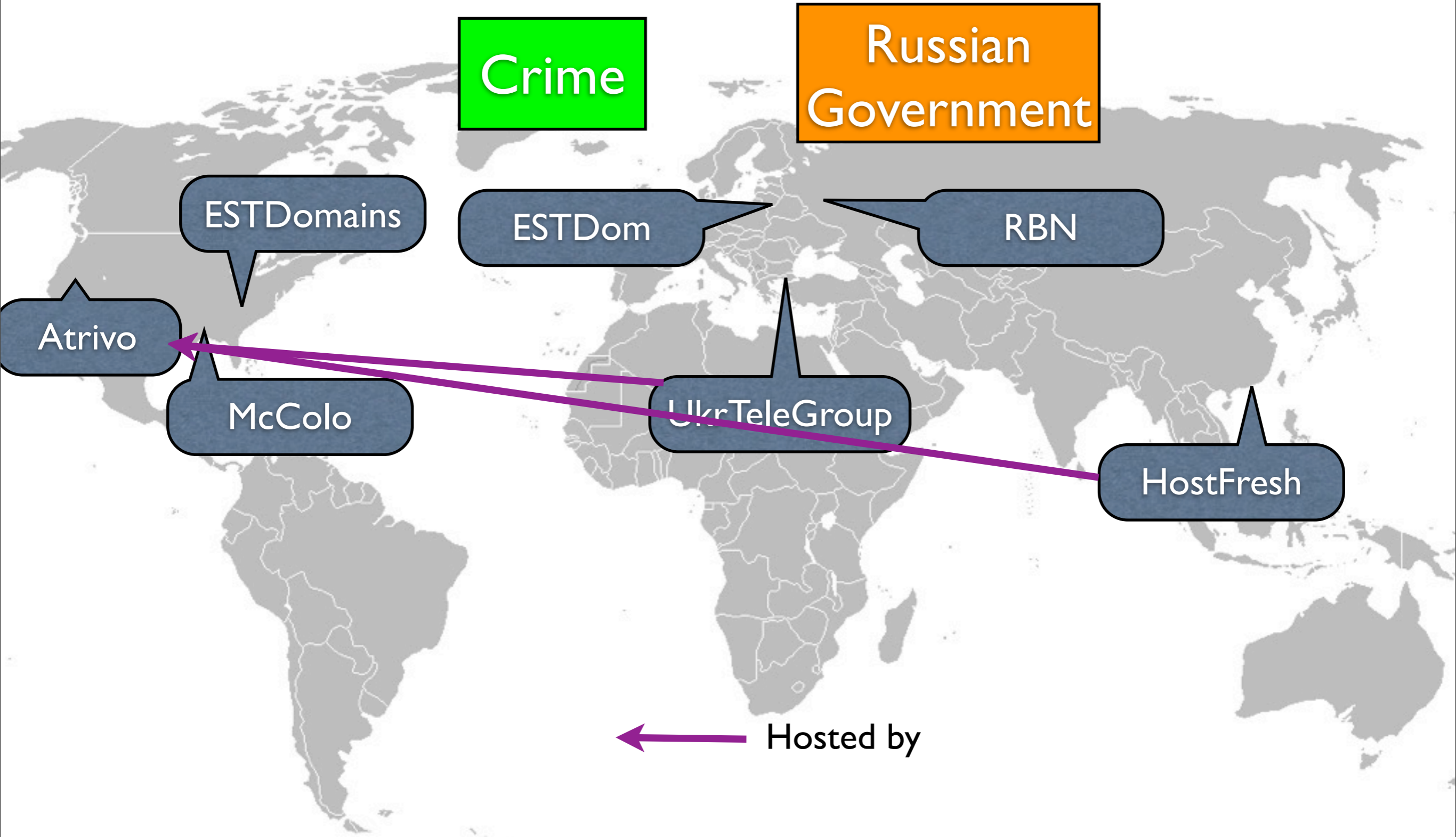
# Russian Crime/State Dilemma

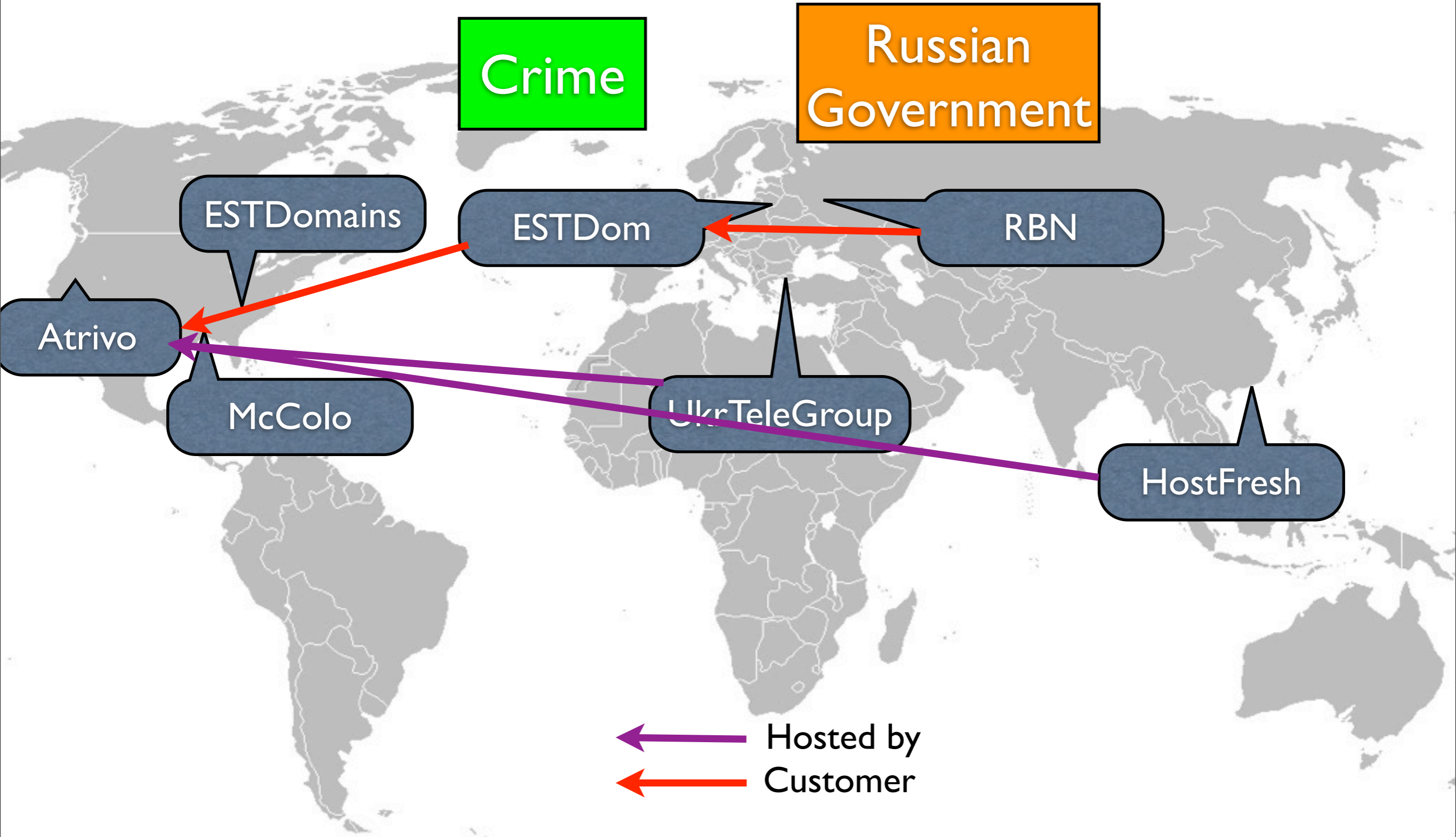
---

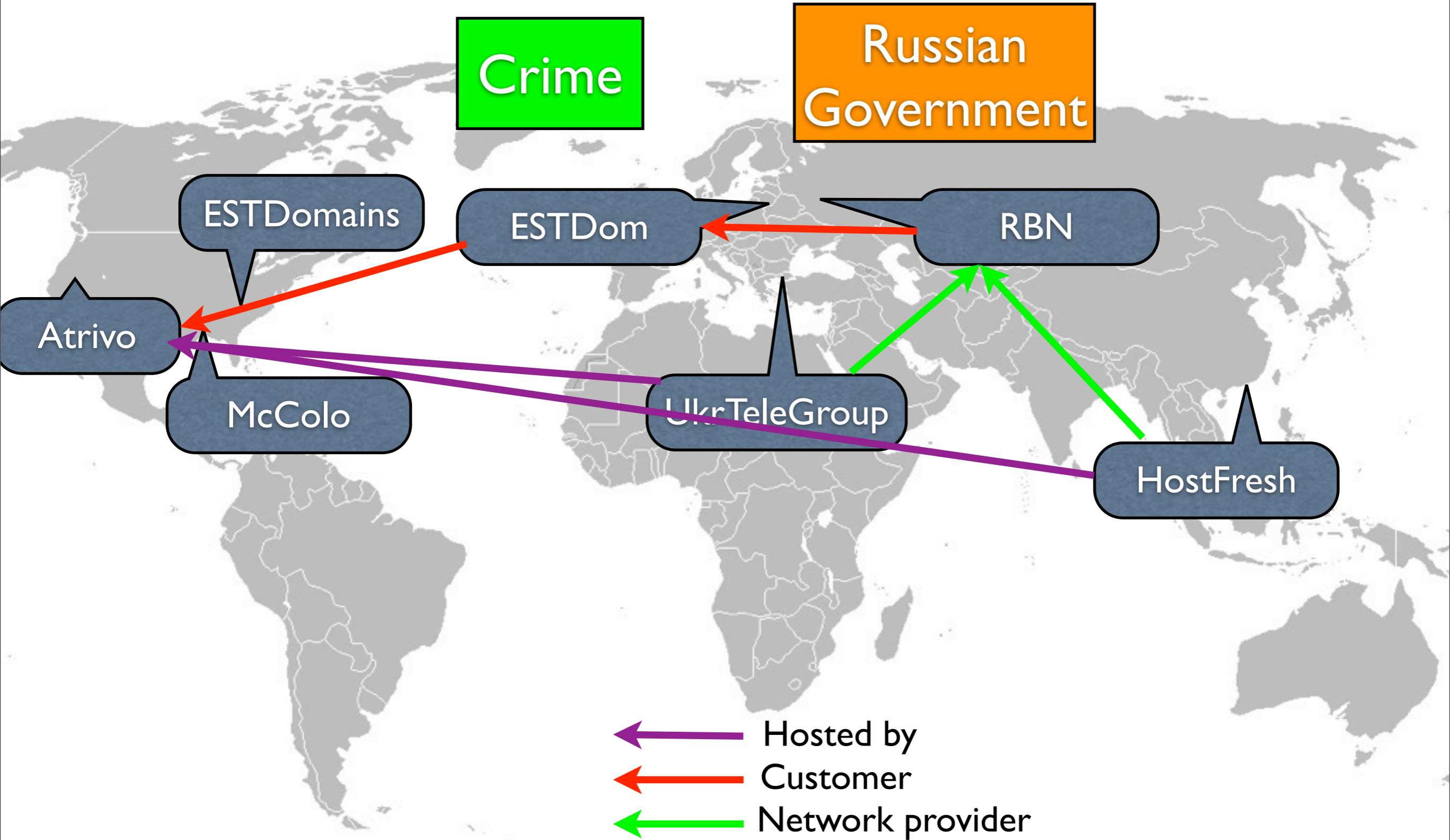




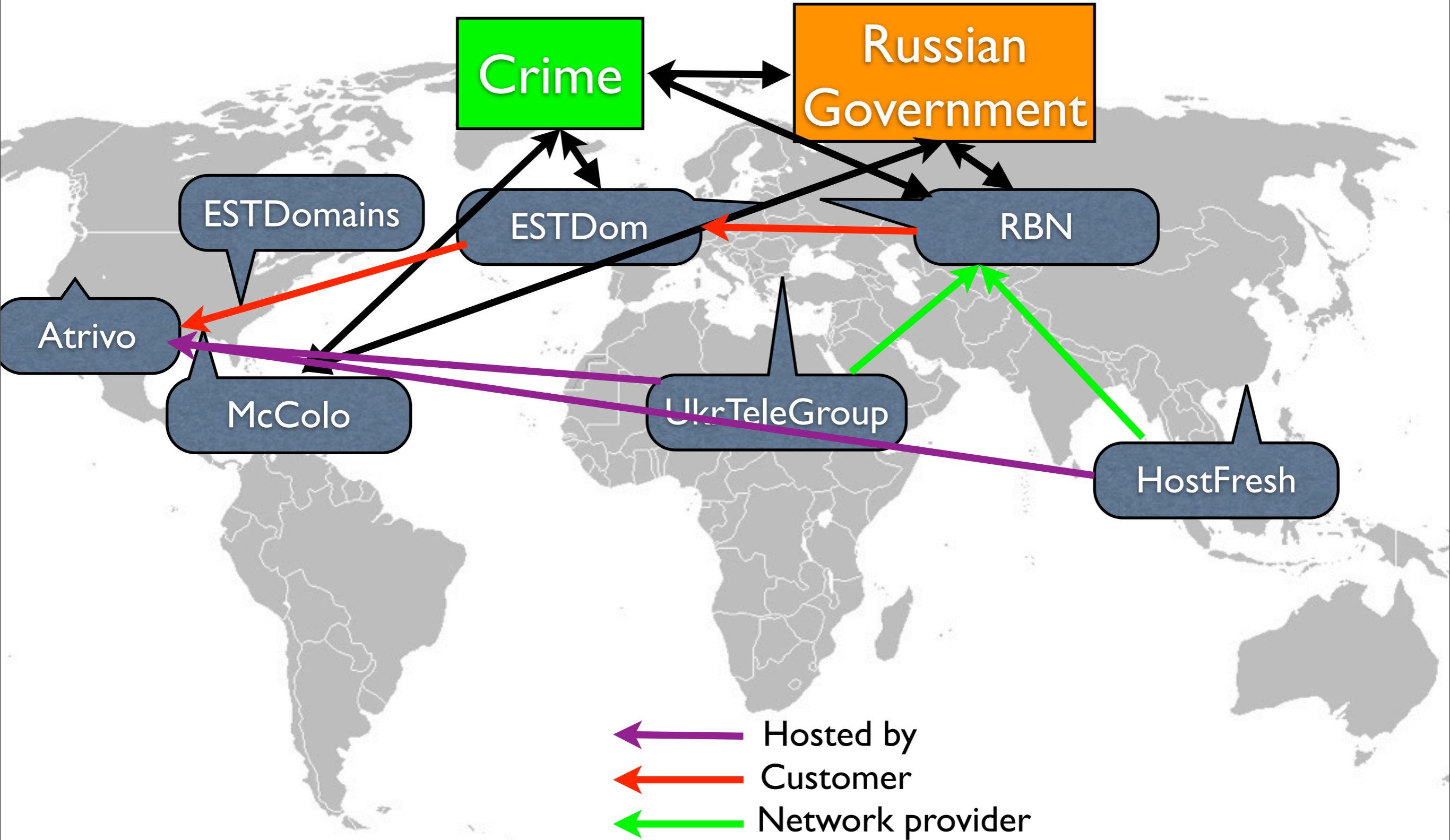












# Remember Georgia?

- 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.

---





# 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  
skandaly.ru



# 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  
skandaly.ru

- 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...



# 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  
skandaly.ru

- 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...





# 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  
skandaly.ru

- 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...

BTW - Guess who were the owners of all the Georgian ISPs?(Russia)



# Georgia - cont.

---



# Georgia - cont.

- Final nail in the coffin:





# Georgia - cont.

- Final nail in the coffin:
- The city of Gori



# Georgia - cont.

- Final nail in the coffin:
- The city of Gori
- DDoS hits all **municipal** sites August 7th 2008 at 22:00



# Georgia - cont.

- Final nail in the coffin:
- The city of Gori
- DDoS hits all **municipal** sites August 7th 2008 at 22:00
- Complete network disconnect of the **district** August 8th 06:00



# Georgia - cont.

- Final nail in the coffin:
- The city of Gori
- DDoS hits all **municipal** sites August 7th 2008 at 22:00
- Complete network disconnect of the **district** August 8th 06:00
- First **strike** on city August 8th 07:30





# Georgia - cont.

- Final nail in the coffin:
- The city of Gori
  - DDoS hits all **municipal** sites August 7th 2008 at 22:00
  - Complete network disconnect of the **district** August 8th 06:00
  - First **strike** on city August 8th 07:30



# History - Revisited...

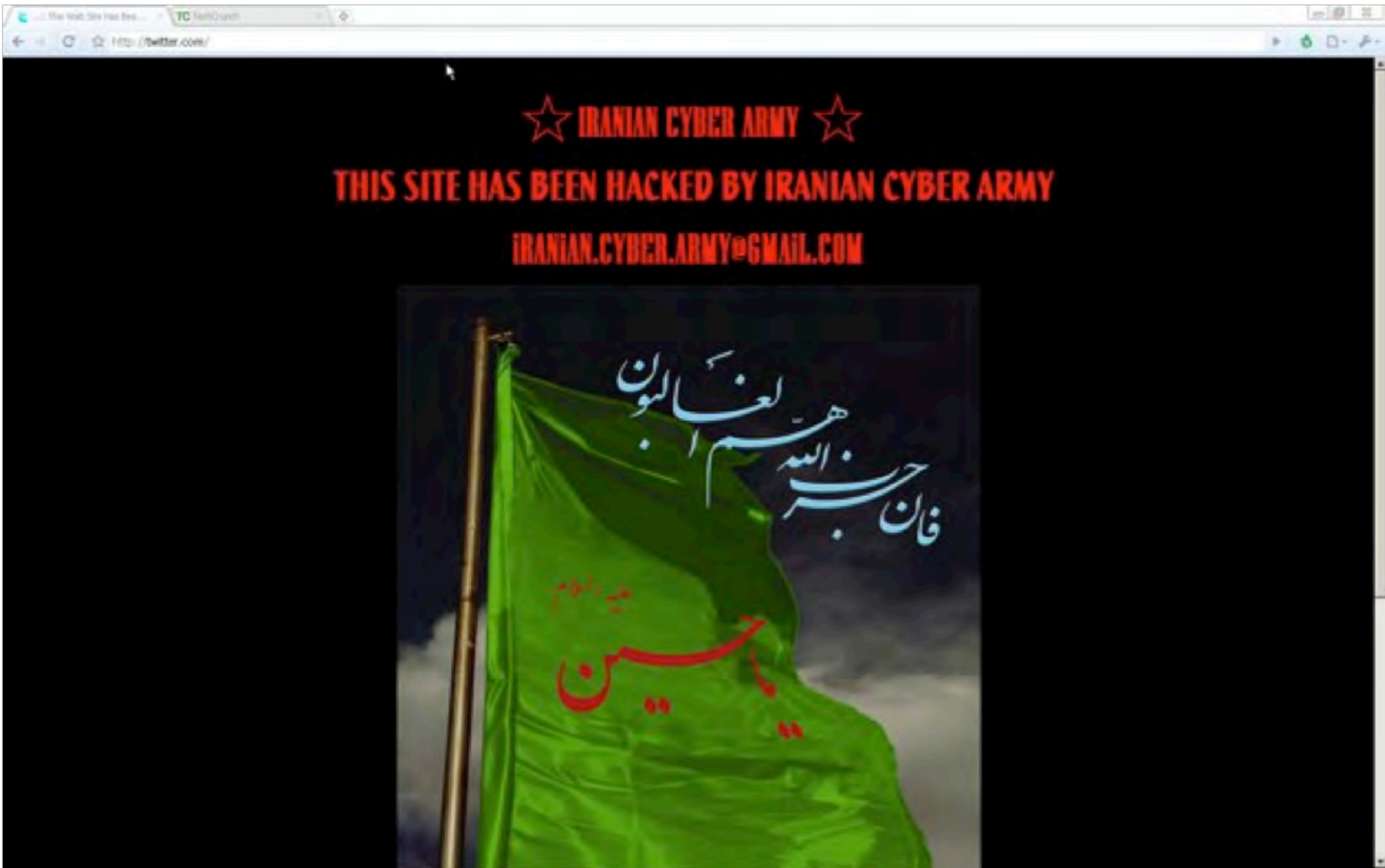
## Iran

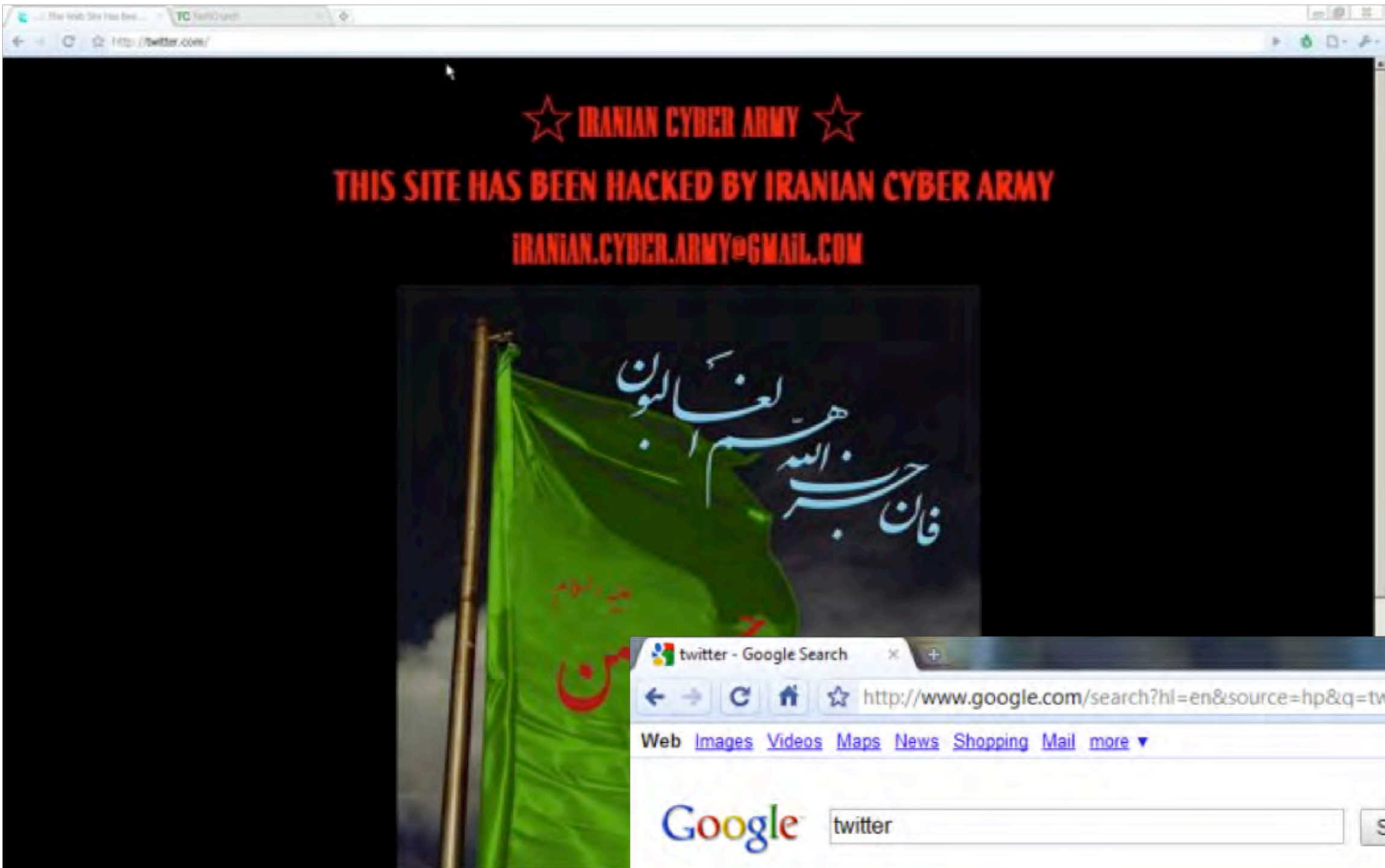
2009 **Twitter** DNS hack attributed to Iranian activity.

**Political** connections are too obvious to ignore (elections)

**Timing** was right on:

UN Council <b>Decisions</b>	<b>Protests</b> by leadership opposition in Tehran
--------------------------------	--





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 شیطان آمیز این سرویس دهنده به دستور مقامات آمریکایی در امور داخلی کشورم ( ... )

[twitter.com/](#) - [Cached](#) - [Similar](#)

[Search](#) [Status](#)  
[Blog](#) [API](#)  
[Help](#) [Contesting account suspension](#)  
[Advanced Search](#)

[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: 2009-12-18 11:55:48

Notified by: Ashiyane Digital Security Team      Domain: <http://www.natchitochesla.gov>      IP address: 69.20.16.77  
System: Win 2003      Web server: IIS/6.0      [Notifier stats](#)

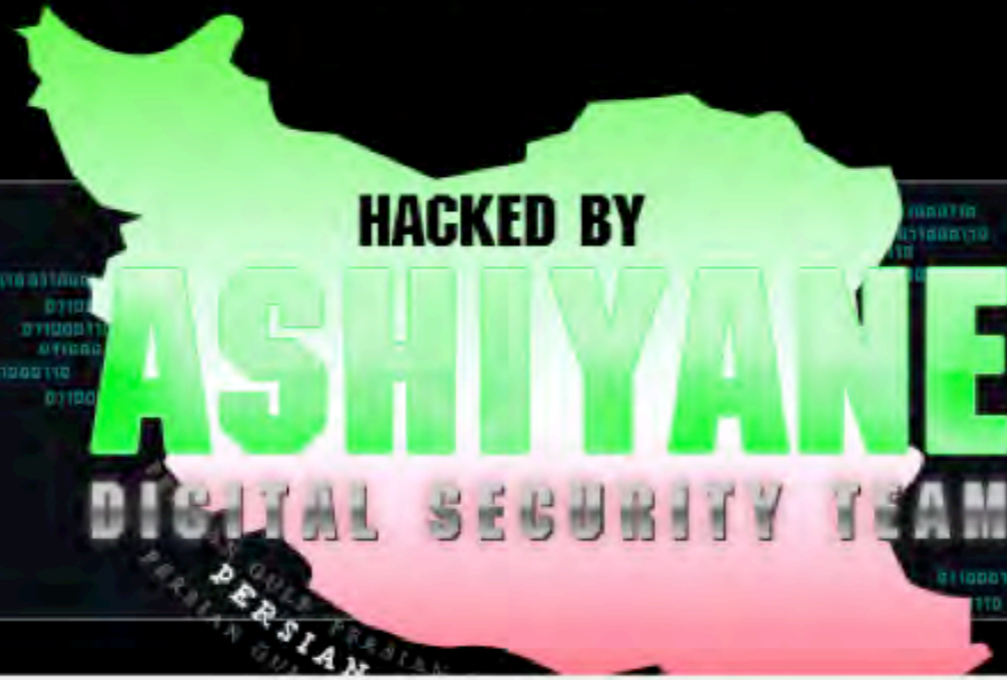
جنگ ما جنگ عقیده است و جغرافیا و مرز نمی شناسد. پس تا شرک و کفر هست مبارزه هست و تا مبارزه هست ما هستیم. ما می دانیم که جسارت توهین به امام خمینی جز از شما بر نمی آید. این فقط یک اخطار است به سایت های دولتی شما!

Our belligerence is religious and does not own any borders, thus we are here as long as atheism and blasphemy exist. We do know that 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



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](http://www.ashiyane.com/forum)

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





# On [Crime|War] training

Ashiyane forums  
**WarGames**



# On [Crime|War] training

## Ashiyane forums **WarGames**

Wargame

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

..... بینم کی می تونه نوشته تو جدول رو Edit کنه .....  
مدت 3 روز .....

**Sha2ow**  
Godfather

تاریخ عضویت: Mar 2005  
محل سکونت: Tehran  
پست: 1.188



# 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

ERroR  
کلانتر سایت

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

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 با 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 اشیانیه " Ashiyane Digital Security Team " دیفیس شده باشه .
- 3- لینک تایید + آدرس 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 اشیانیه 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- 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 )

پیشنهادات و انتقادات برای بهبود وضعیت سایت

بانک مقالات/آموزشی سایت اشیانیه

به مدت نیستم به دلیل خدمت سربازی (ماهشهر اهواز)





# Wargames 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

**LEARN ABOUT THE NEWEST GAS APPLIANCES FOR YOUR HOME**

**LET'S GO**

**WHY NATURAL GAS?**

**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.

**GETTING CONNECTED**

**LEARN MORE**



# Back to [Crime|War] Links:

---

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



# 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



# 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



# 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**





# 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**

**Later on** - Baidu takedown  
with the same MO (credentials)

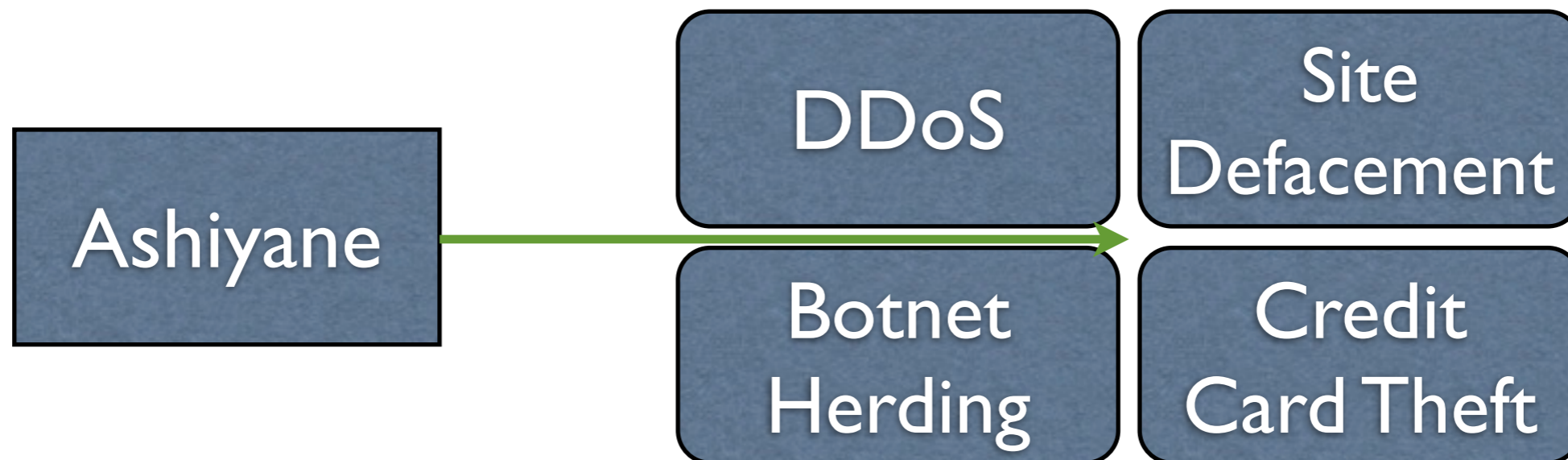


# Mapping Iran's [Crime|War].

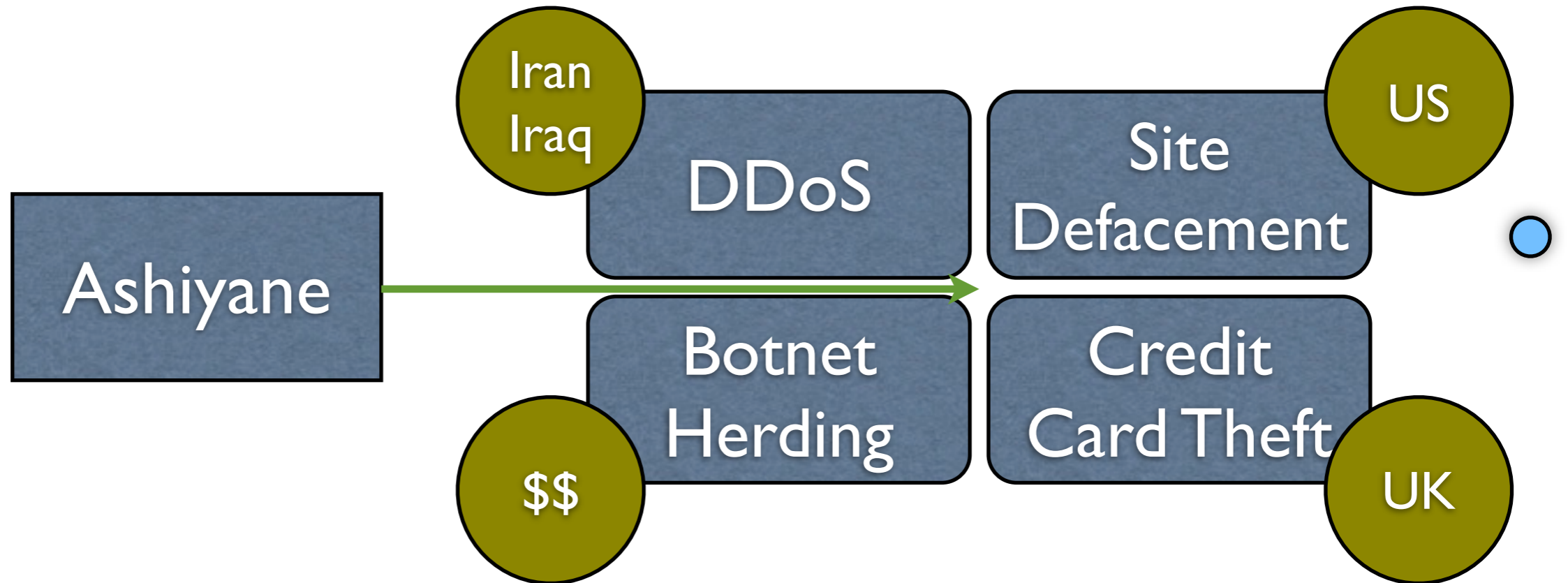
Ashiyane



# Mapping Iran's [Crime|War].

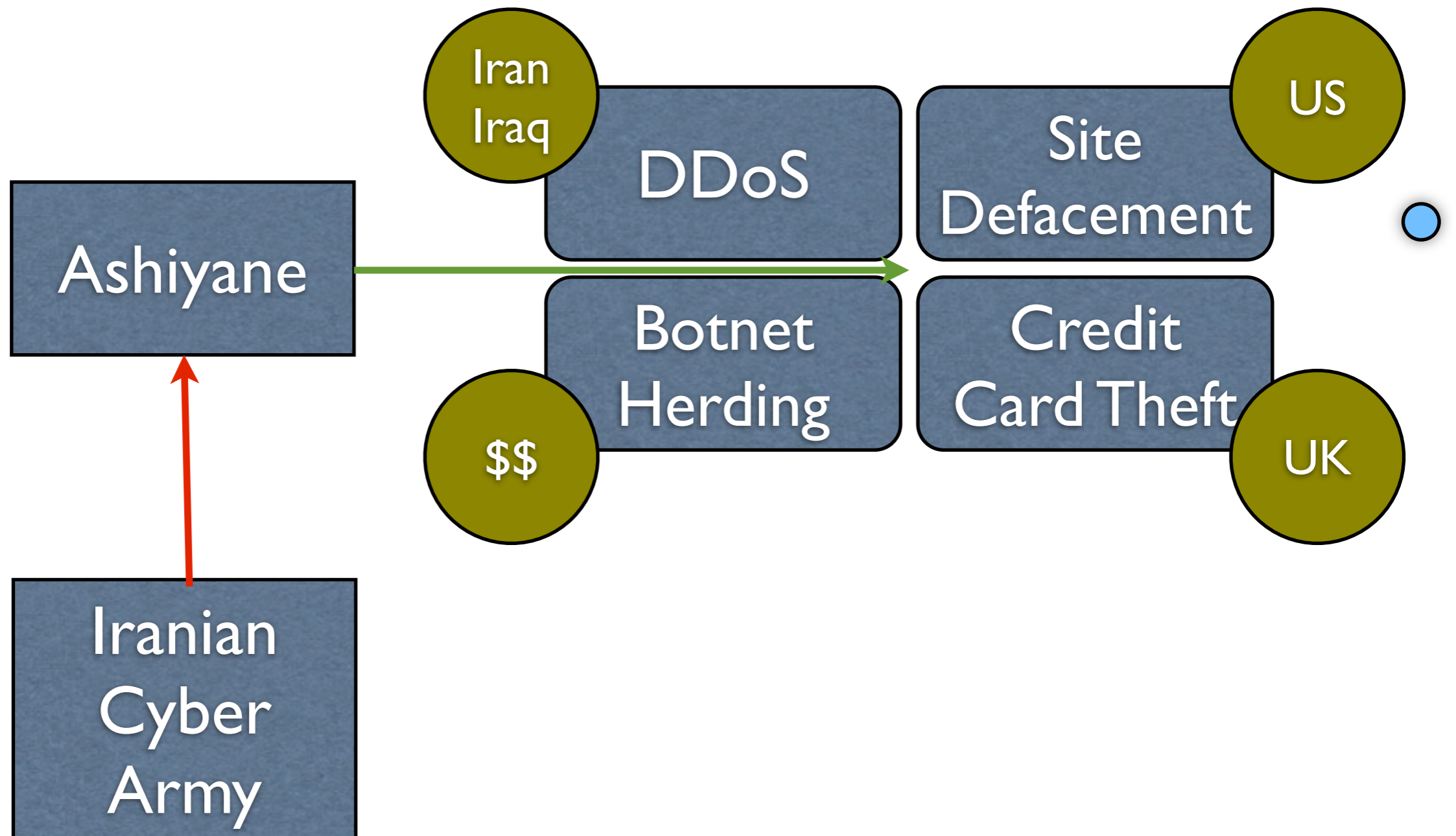


# Mapping Iran's [Crime|War]

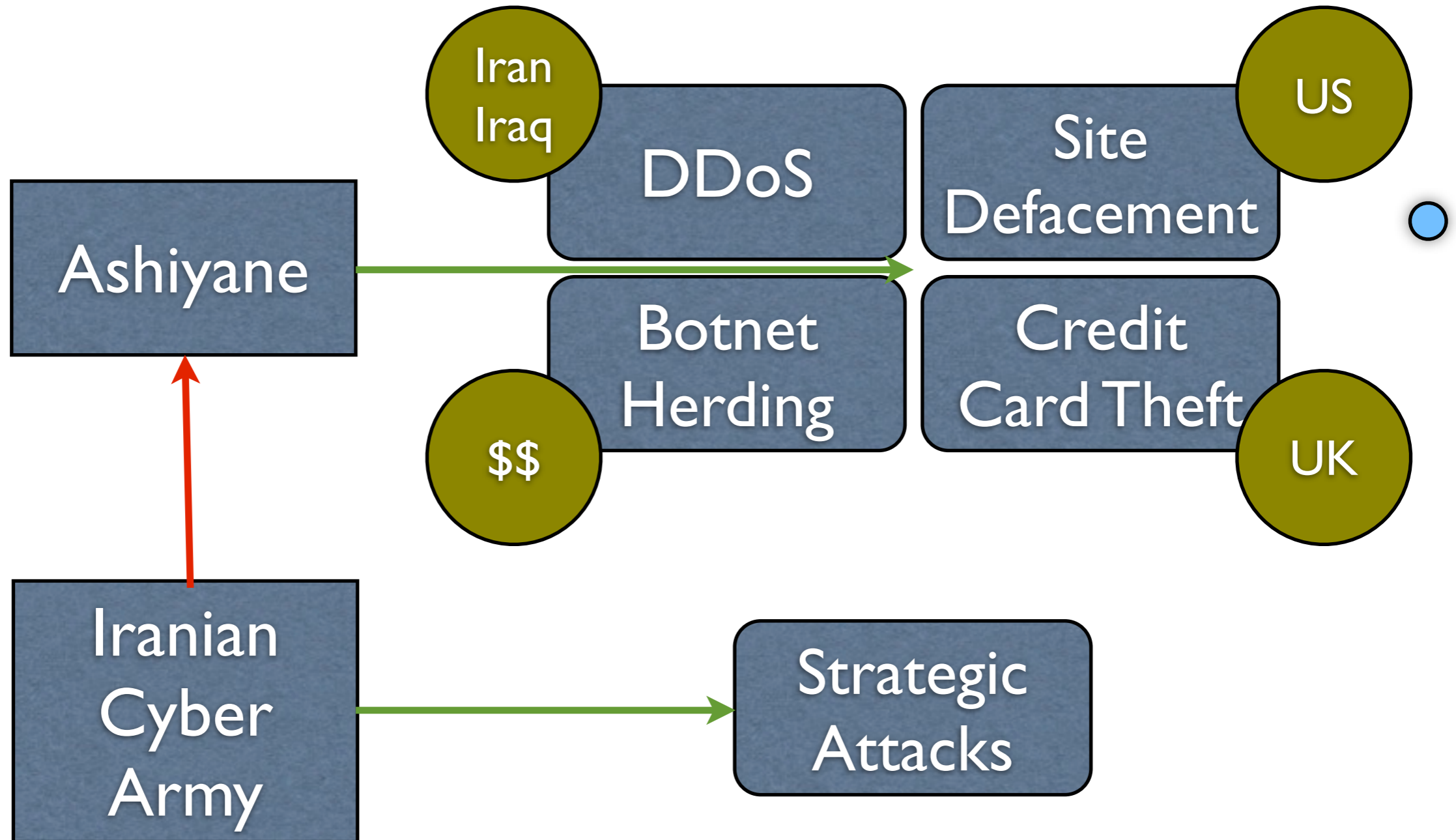




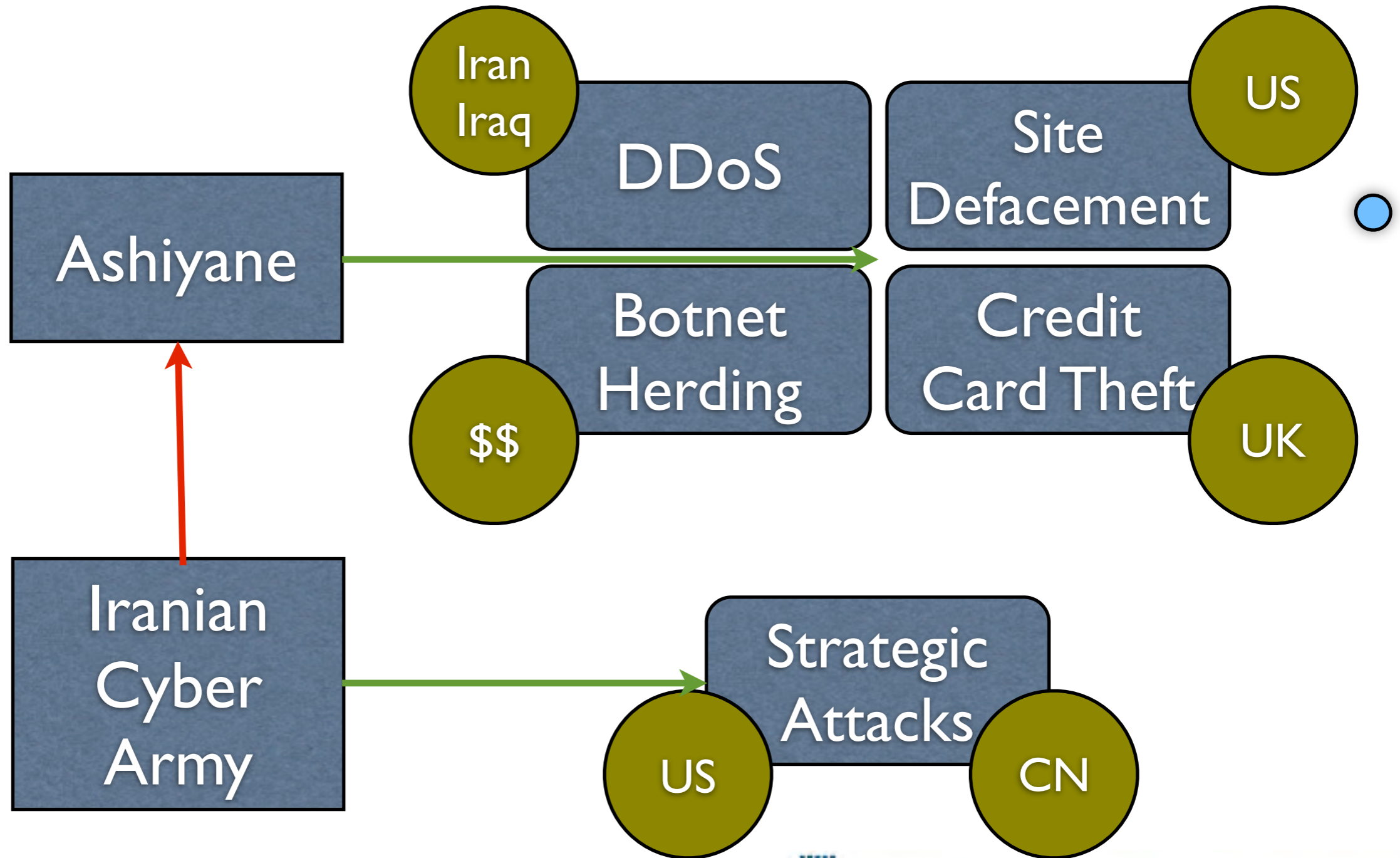
# Mapping Iran's [Crime|War]



# Mapping Iran's [Crime|War]

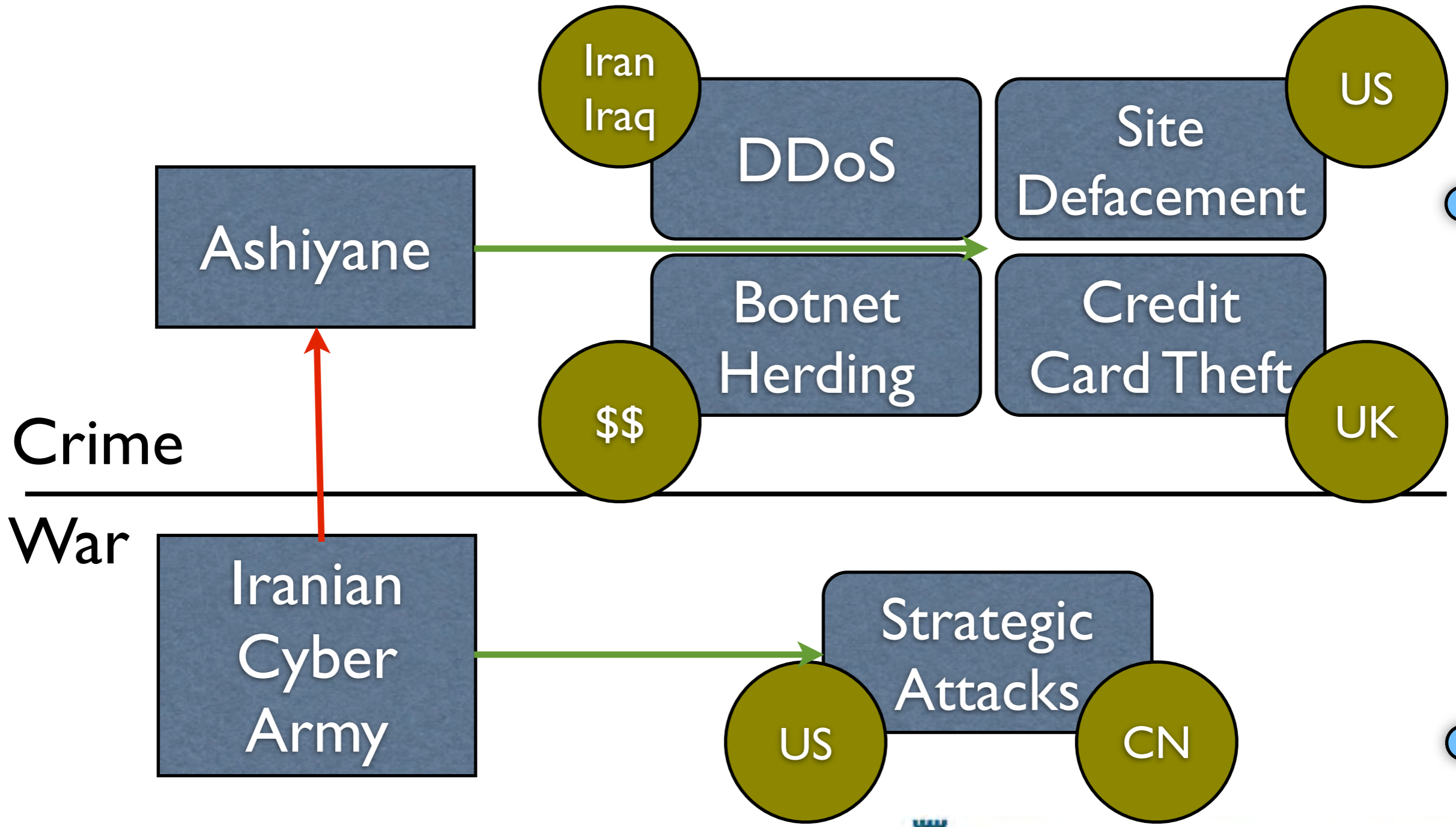


# Mapping Iran's [Crime|War]



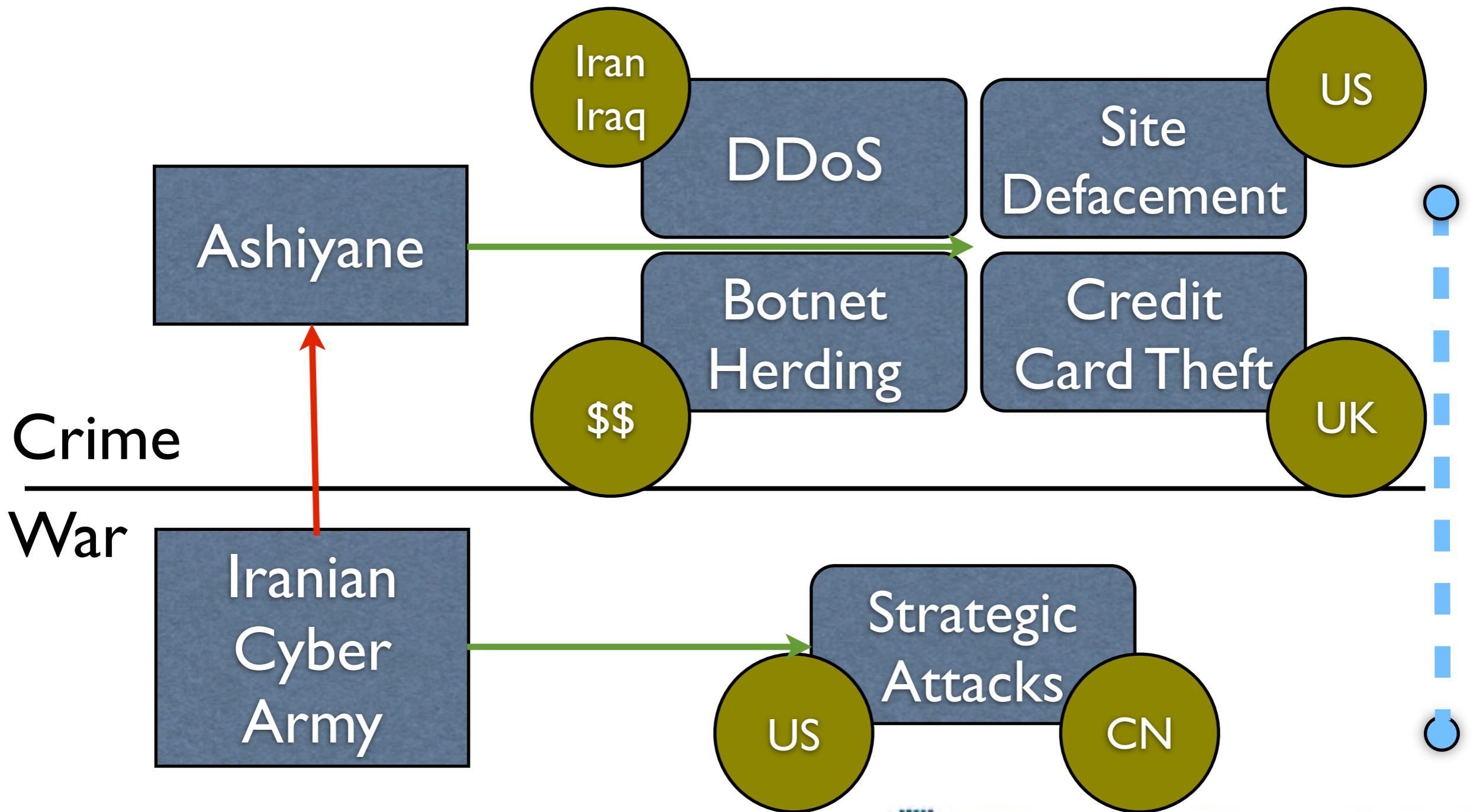


# Mapping Iran's [Crime|War]





# Mapping Iran's [Crime|War]



# Iran - the unspoken



# Iran - the unspoken

- Stuxnet



# Iran - the unspoken

- Stuxnet
- There, I've said it





# 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...

Problem: Attacks all carry the signs of Cybercrime...

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...



# China ...connecting the dots...

The China move:



# 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).



# China

Anecdote - a professor in one of the universities linked to the attack admitted that the school network is often used to anonymously relay attacks

## 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).





# China .....

Anecdote - a professor in one of the universities linked to the attack admitted that the school network is often used to anonymously relay attacks

## 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



# China

Anecdote - a professor in one of the universities linked to the attack admitted that the school network is often used to anonymously relay attacks

## 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

Anecdote - a professor in one of the universities linked to the attack admitted that the school network is often used to anonymously relay attacks

## 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 

# What about Anon/Lulz?

## Who are they?

- Started from 4chan in 2003
- Formed a more hacktivist setup early 2008
- Originally focused against civil liberty violations and the Church of Scientology
- Maintain “anonymity”
  - Which now means problems...





# What about Anon/Lulz?

---

Everyone is anonymous.

No way to know if they are truly from the  
“core” group.

Attack galore...



# What about Anon/Lulz?




# What about Anon/Lulz?



 **@anonymouSabu**  
The Real Sabu

RE: [#opFacebook](#) I've been saying this for months: I don't know who created that operation but I highly doubt it will be fruitful.

4 Nov via web  Favorite  Retweet  Reply  Buffer



# What about Anon/Lulz?

Example of how the “brand” is abused:

- An “OP” video uploaded on Nov 4th warning the Israeli government about an upcoming attack
- Gov. website DDoS’d on Nov 6th (minor traffic), caused rolling issues (HW+SW), sites unavailable for few hours.





# What about Anon/Lulz?



==



A hacker group known to be used by the Turkish government for launching “political” actions.

Daily activities focus on petty crime and defacements...



# What about Anon/Lulz?



!=



Far from the original Anonymous manifesto, yet highly effective as a tool for launching attacks with minimal attribution trail!

# THE FUTURE (Illustrated)



# THE FUTURE (Illustrated)





# THE FUTURE (Illustrated)



# THE FUTURE (Illustrated)



# THE FUTURE (Illustrated)





# THE FUTURE (Illustrated)





# THE FUTURE (Illustrated)



# THE FUTURE (Illustrated)



# Summary

## Good

Formal training on  
cybersecurity by  
nations

## Bad

Commercial  
development of  
malware still reigns



# 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. <- TRANSLATE TO POLITICS/LAW!!



# Thanks!

## Q & A

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

pro: [iamit@security-art.com](mailto:iamit@security-art.com)

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

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

