iDEFENSE

Actionable Threat Intelligence

Information Security's Third Wave

Eli Jellenc

International Intelligence Director

ejellenc@idefense.com

Overview

+ Cyber security will never be the same…

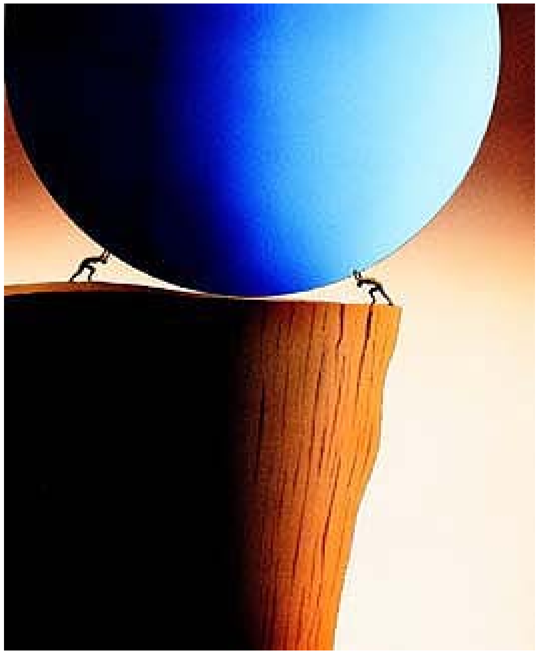
+ Theories of Cyber War and its Problems

+ Cyberwarfare in Practice: Russia, Estonia, and Georgia

+ Regional Trends

+ Conclusions

2008: Tipping Point



Malcom Gladwell's "Tipping Point"

"Little changes can have big effects; when small numbers of people start behaving differently, that behavior can ripple outward until a critical mass or 'tipping point' is reached, changing the world."

Source: Tipping Point Graphic

Mother Jones Cover Nov/Dec 2006

Strategic Hacking: A New Era

- Cyber security is now in the top 5 national security priorities of most great powers and many middle powers
- Defense is not enough; major players are developing the offense
- Private sector defense contractors are going on the offensive; underground elements are often employed as well
- Everyone is attacking everyone else, even allies vs. allies
- 2 likely scenarios: chaos or severe restriction

Everyone Attacks Everyone Else

- UK Army Intelligence Report (*Daily Telegraph*; February 8, 2009)
  - "Security sources have revealed that the list of foreign agencies operating within the UK includes **Iran, Syria, North Korea** and **Serbia**…"
  - "…and some members of the European Union, such as **France and Germany**"
- Germany: penetrated over 30 nations' government systems by 2009
  - Source: *Der Spiegel*, March, 2009
- Israel vs. Most of the Middle East
- Fatah vs. Hamas
- China
  - NOT just the official level
  - Chinese amateur crackers attack official systems and defense contractors
  - Foreign governments and private contractors fight back
- Russia attacks everyone…no surprise
- Myanmar (seriously, MYANMAR!!)
  - 2007 attacks against Irrawaddy.com
  - Using Russian criminal malware

Offense Becomes More Attractive

- All of the major US Defense Contractors are developing defensive and offensive “cyber solutions” offerings

- "One of the reasons we're looking at a Cyber Command is to unify all aspects of cyber defense, so that you don't separate out offense, defense, intelligence, so that all of the various aspects work together," (Dep. Secretary of Defense William Lynn, *VoA News*, June 15, 2009)

- The UK’s GCHQ is looking for “naughty boys” to conduct offensive (and defensive) operations (Lord West, in *The Register*, June 29, 2009)

Emerging Models of Cyber Conflict

- Centralized Model:
  - Authorized institutions
  - Working in secret
  - Big budgets
- Decentralized Model
  - Uses Underground
  - Working with “open secrets”
  - Lower budgets
- Internally Focused
  - Highly Defensive
  - Highly Restrictive
- In Reality: most are hybrids

Regional Trends - Russia

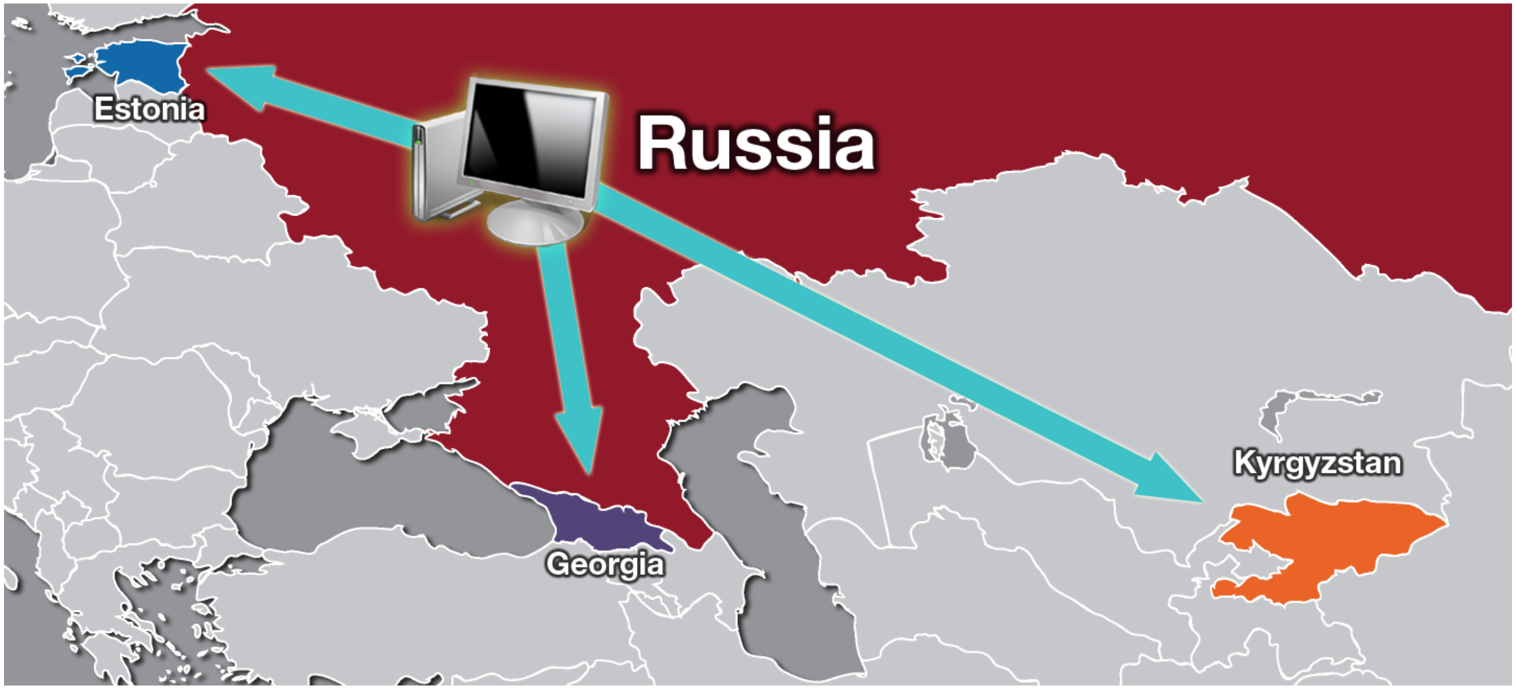
Justified Self Assertion

New Nationalism

Cyber War / Hactavism is a Reality

Cyber Crime

2008: Cyber War Becomes Reality



Increasing Nationalism

Cyber Criminals = Strategic Asset

The state wields cyber attack expertise for domestic and international advantage

Political Dispute with Russia? – Expect Cyber Harassment

Regional Trends - China

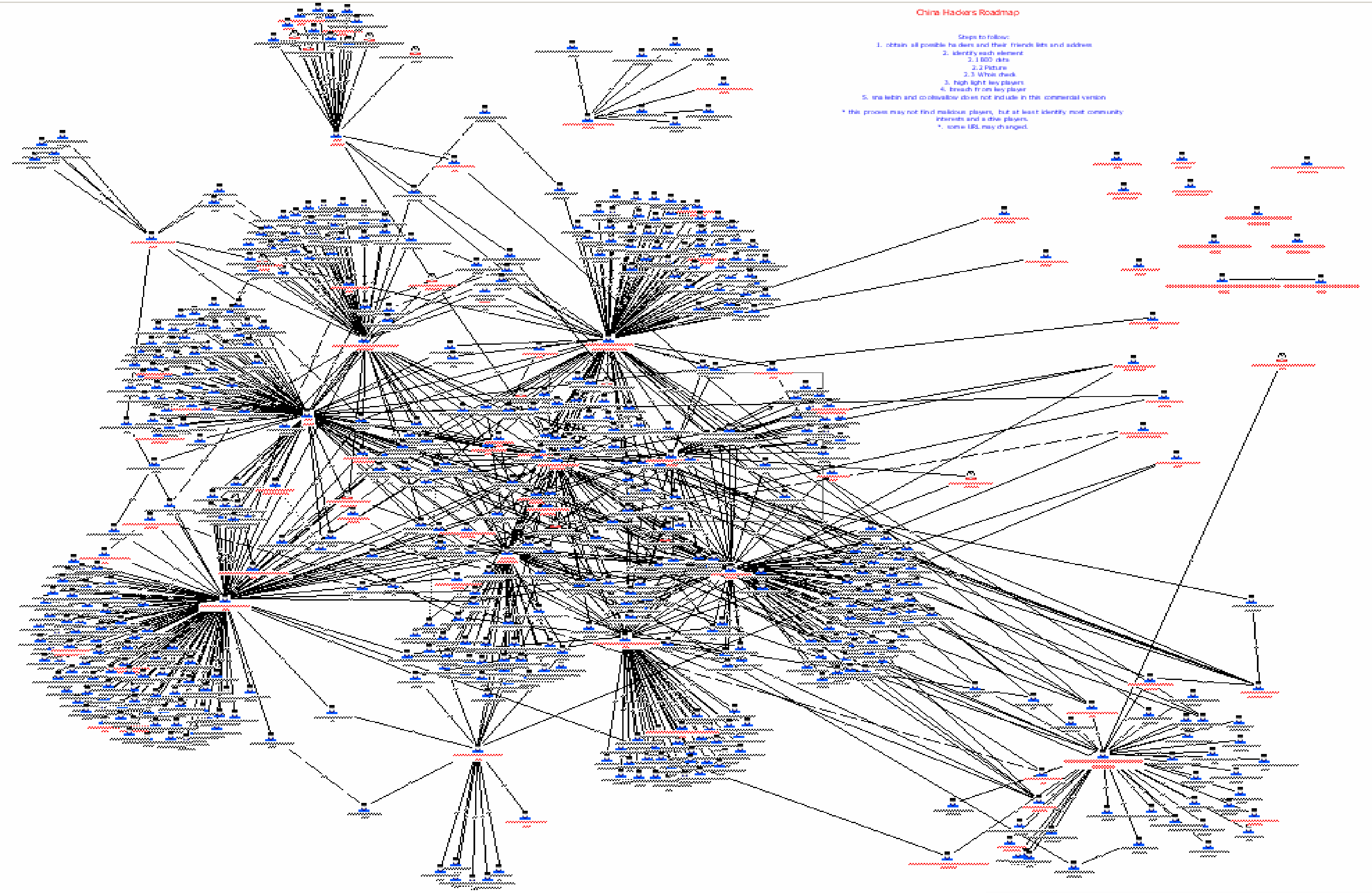
Cyber Espionage

Cyber Crime

Cyber Sabotage

Cyber Militias

Structure of Chinese Underground

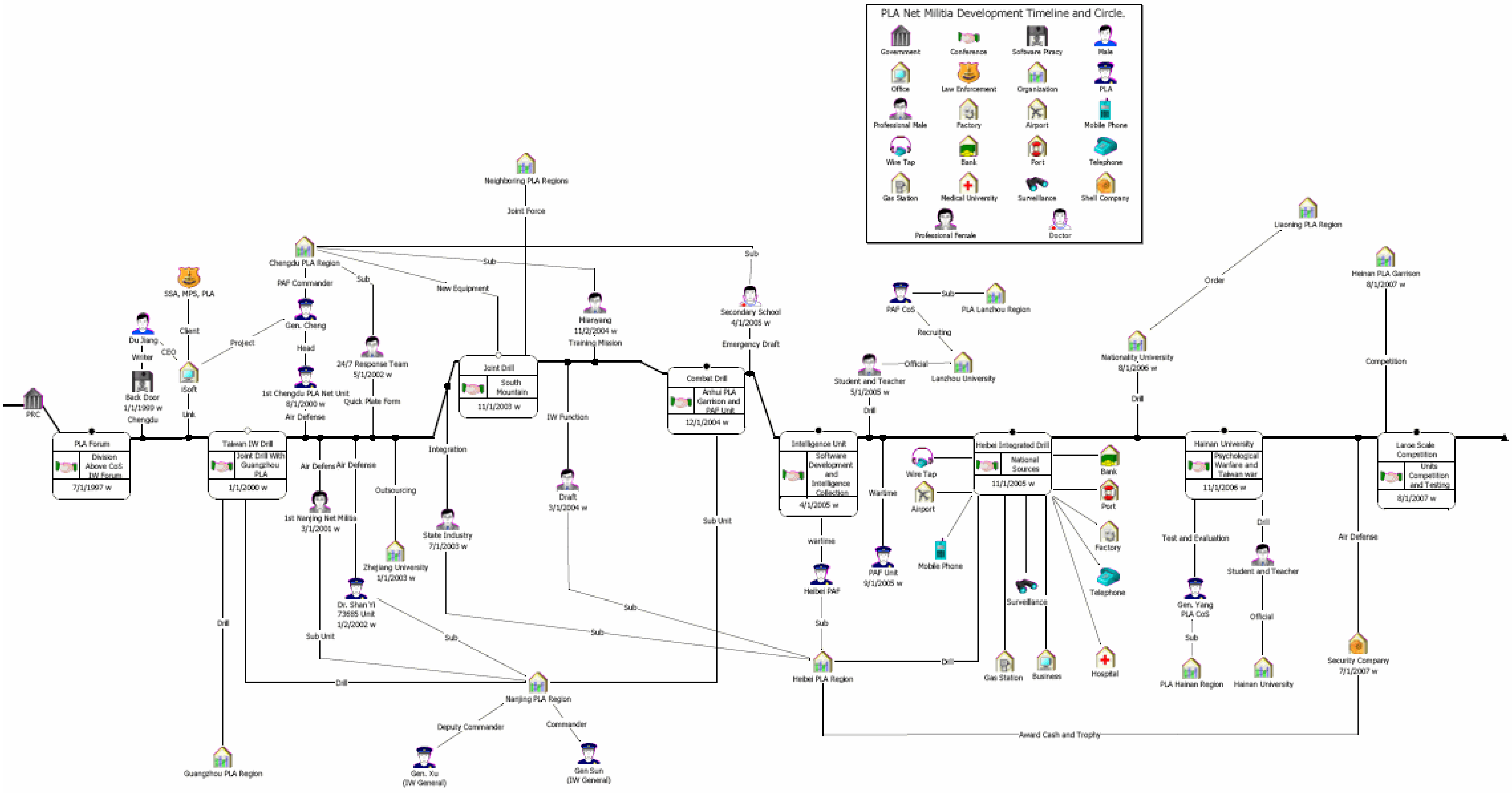


China Hackers Roadmap

Steps to follow:
1. obtain all possible hackers and their friends lists and address
2. identify each element
2.1 BBS data
2.2 Picture
2.3 Whois check
3. high light key players
4. breach from key player
5. snakebin and coolswallow does not include in this commercial version

* this process may not find malicious players, but at least identify most community interests and active players.
*. some URL may changed.

China: Net Militias



China’s Net Militias

长沙市岳麓区中南大学民兵网络攻防分队训练汇报演示
首战用我 全程用我 用我必胜

China’s Dirty Secrets

- They are just as vulnerable as everyone else…in some ways, more so.

- Chinese vs. Chinese attacks are rampant, almost as common as external attacks
  - Rival data centers
  - Rival departments within *the same company*

- Corruption makes many organizations more vulnerable…

- “The state” is not a monolith…there are rivalries within

Regional Trends – Greater Middle East

Secular Hacking

Ideological Hacking

Religiously Motivated Hacking

Fatwa Justification

Contracted Hacking

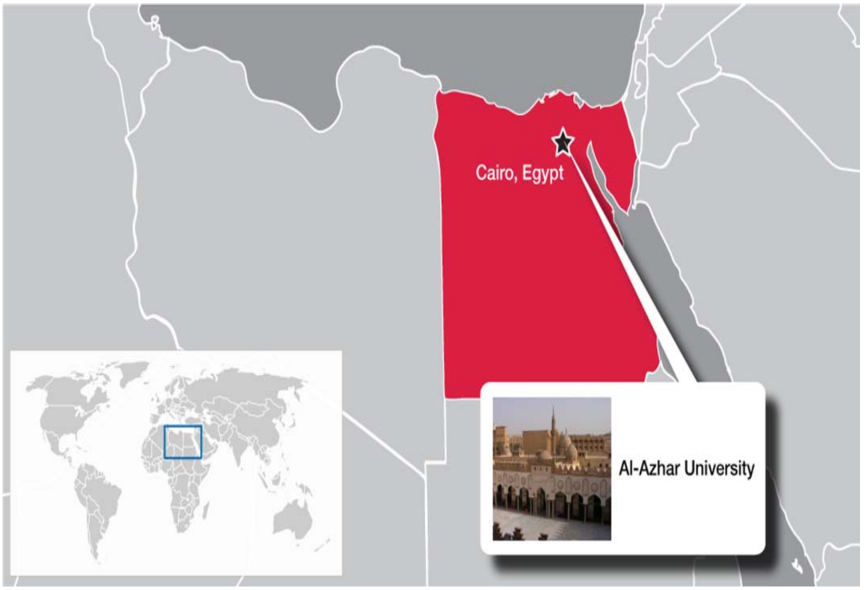
2008 Headlines: Middle East Fatwas Justify Cyber Fraud

Sheikh Al-Tantawi

Defend Islam against Internet based defamations

Cyber fraud is legitimate fund raising

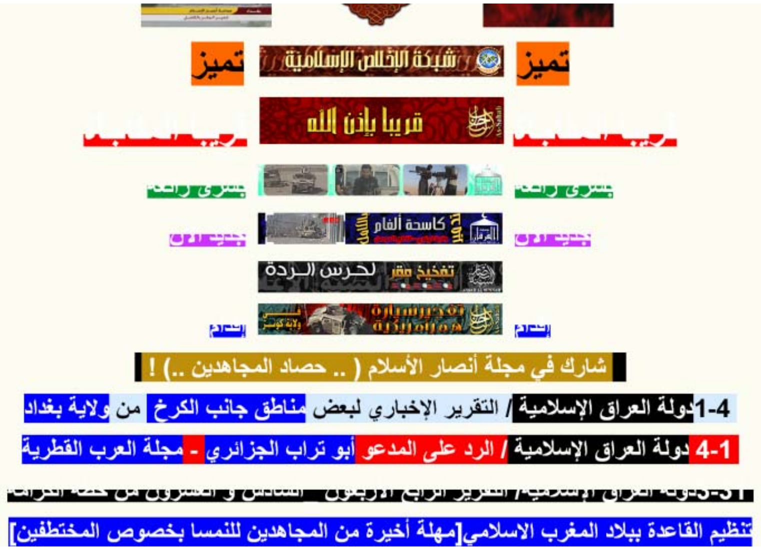
Prediction: Middle East - Threat Region - Cyber Fraud



Al-Azhar University

Fatwa Committee

Jihadists and Cyber Cartels: Moving Closer?

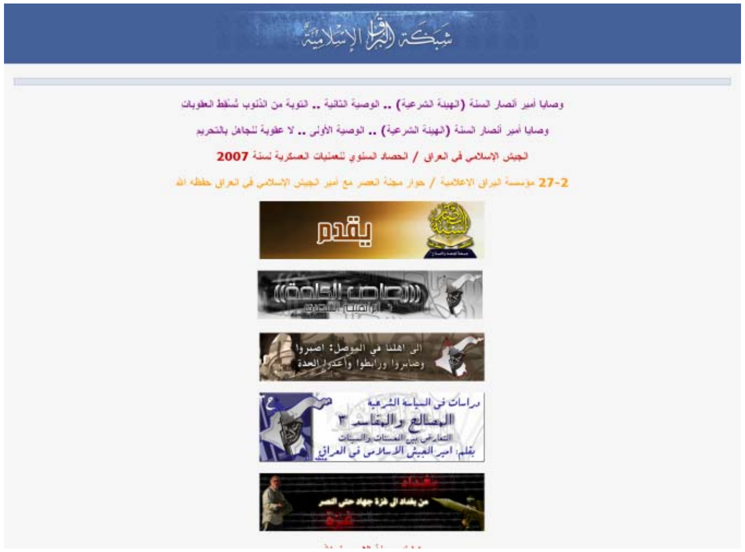


شارك في مجلة أنصار الأسلام (.. حصاد المجاهدين ..) !

1-4دولة العراق الإسلامية/ التقرير الإخباري لبعض مناطق جانب الكرخ من ولاية بغداد

4-1 دولة العراق الإسلامية / الرد على المدعو أبو تراب الجزائري - مجلة العرب القطرية

تنظيم القاعدة ببلاد المغرب الاسلامي[مهلة أخيرة من المجاهدين للنمسا بخصوص المختطفين]

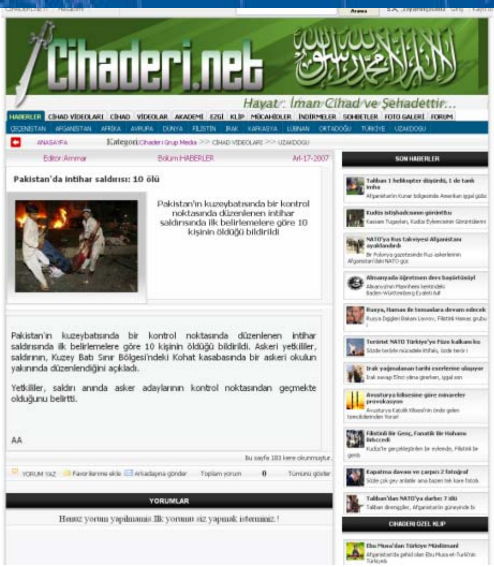

شبكة البراق الإسلامية
يقدم
((رصاص الكاتمة))
الى اهلنا في الموصل: اصبروا وصابروا ورابطوا واعدوا العدة
دراسات في السياسة الشرعية
المصالح والمفاسد ٣
التعارض بين الحسنات والسيئات
بقلم: امير الجيش الاسلامي في العراق
من بغداد الى غزة جهاد حتى النصر

وصايا أمير أنصار السنة (الهيئة الشرعية) .. الوصية الثانية .. التوبة من الذنوب تسقط العقوبات

وصايا أمير أنصار السنة (الهيئة الشرعية) .. الوصية الأولى .. لا عقوبة للجاهل بالتحريم

الجيش الإسلامي في العراق / الحصاد السنوي للعمليات العسكرية لسنة 2007

27-2 مؤسسة البراق الاعلامية / حوار مجلة العصر مع أمير الجيش الاسلامي في العراق حفظه الله



Kategori:Cihaderi Grup Medya >> CİHAD VİDEOLARI >> UZAKDOĞU

Editör:Ammar Bölüm:HABERLER Arl-17-2007

Pakistan'da intihar saldırısı: 10 ölü

Pakistan'ın kuzeybatısında bir kontrol noktasında düzenlenen intihar saldırısında ilk belirlemelere göre 10 kişinin öldüğü bildirildi

Pakistan'ın kuzeybatısında bir kontrol noktasında düzenlenen intihar saldırısında ilk belirlemelere göre 10 kişinin öldüğü bildirildi. Askeri yetkililer, saldırının, Kuzey Batı Sınır Bölgesi'ndeki Kohat kasabasında bir askeri okulun yakınında düzenlendiğini açıkladı.

Yetkililer, saldırı anında asker adaylarının kontrol noktasından geçmekte olduğunu belirtti.

AA

Bu sayfa 183 kere okunmuştur.

Toplam yorum 0

YORUMLAR

Henüz yorum yapilmamis.Ilk yorumu siz yapmak istermisiniz.!

SON HABERLER

Taliban 1 helikopter düşürdü, 1 de tank imha
Afganistan'ın Kunar bölgesinde Amerikan işgal güç

Kudüs istişhadcısının görüntüsü
Kassam Tugayları, Kudüs Eylemcisinin Görüntülerini

NATO'ya Rus takviyesi Afganistanı ayaklandırdı
Bir Polonya gazetesinde Rus askerlerinin Afganistan'daki NATO güç

Almanya'da öğretmen ders başörtüsüyl
Almanya'nın Mannheim kentindeki Baden-Württemberg Eyaleti Adl

Rusya, Hamas ile temaslara devam edecek
Rusya Dışişleri Bakanı Lavrov, Filistinli Hamas grubu

Terörist NATO Türkiye'ye Füze kalkanı ku
Sözde terörle mücadele ittifakı, özde terör i

Irak yağmalanan tarihi eserlerine ulaşıyor
Irak savaşı 5inci yılına girerken, işgal son

Avusturya kilisesine göre minareler provokasyon
Avusturya Katolik Kilisesi'nin önde gelen temsilcilerinden [illegible]

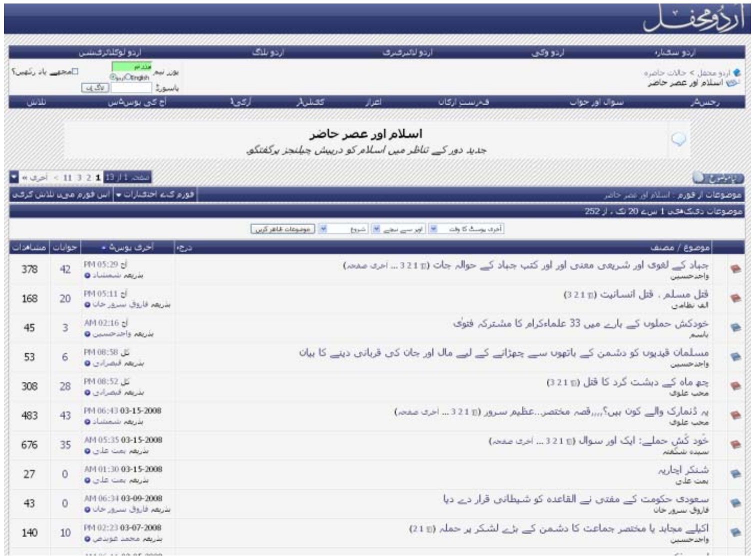
Filistinli Bir Genç, Fanatik Bir Hahamı Bıçakladı
Kudüs'te gerçekleştirilen bir eylemde, Filistinli bir genç

Kapatma davası ve çarpıcı 2 fotoğraf
Sözde çok şey anlatır ama bazen tek kare fotoğ

Taliban'dan NATO'ya darbe: 7 ölü
Taliban direnişçiler, Afganistan'ın güneyinde bi

CIHADERI ÖZEL KLİP

Ebu Musa'dan Türkiye Müslümanl
Afganistan'da şehid olan Ebu Musa et-Turki'nin Türkiyeli



اردو محفل > حالات حاضرہ
اسلام اور عصر حاضر

اسلام اور عصر حاضر
جدید دور کے تناظر میں اسلام کو درپیش چیلنجز پرگفتگو

صفحہ 1 از 13 1 2 3 11 > آخری »

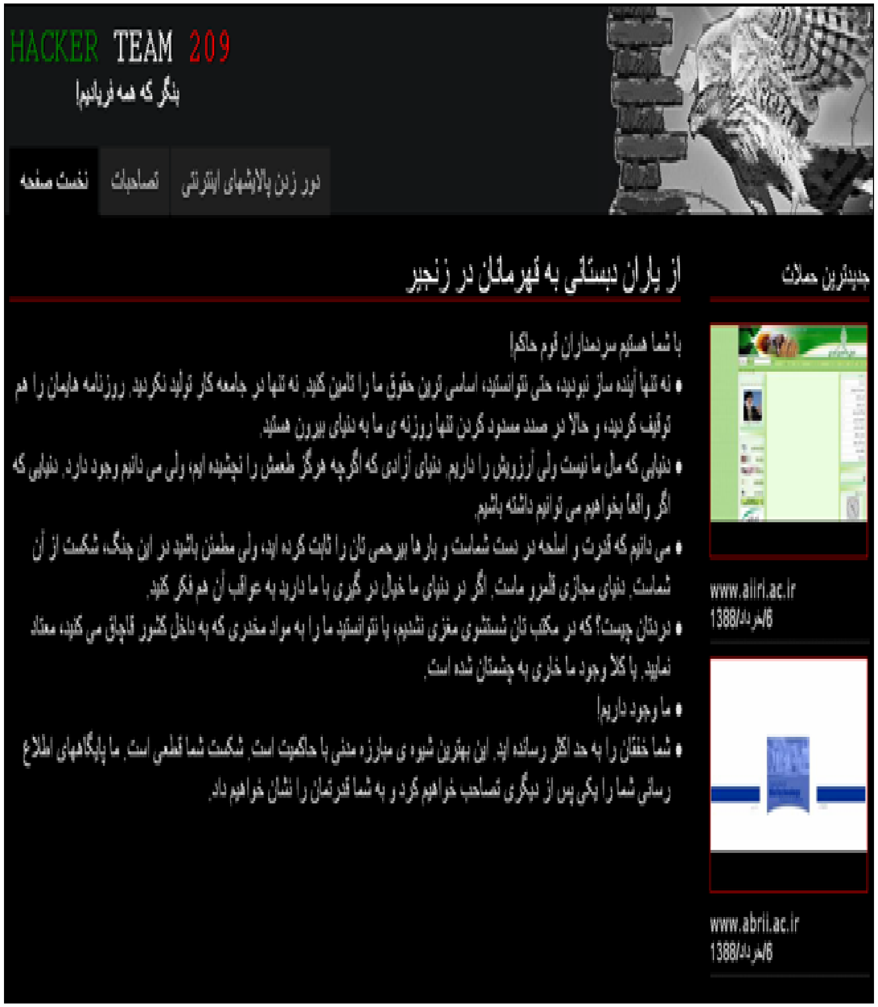
موضوعات از فورم : اسلام اور عصر حاضر

موضوعات دکھائی 1 سے 20 تک ، از 252

موضوع / مصنف	درجہ	آخری پوسٹ	جوابات	مشاہدات
جہاد کے لغوی اور شریعی معنی اور اور کتب جہاد کے حوالہ جات (1 2 3 ... آخری صفحہ) واجدحسین		آج PM 05:29 بذریعہ شمشاد	42	378
قتل مسلم . قتل انسانیت (1 2 3) الف نظامی		آج PM 05:11 بذریعہ فاروق سرور خان	20	168
خودکش حملوں کے بارے میں 33 علماءکرام کا مشترکہ فتوٰی باسم		آج AM 02:16 بذریعہ واجدحسین	3	45
مسلمان قیدیوں کو دشمن کے ہاتھوں سے چھڑانے کے لیے مال اور جان کی قربانی دینے کا بیان واجدحسین		کل PM 08:58 بذریعہ قیصرانی	6	53
چھ ماہ کے دہشت گرد کا قتل (1 2 3) محب علوی		کل PM 08:52 بذریعہ قیصرانی	28	308
یہ ڈنمارک والے کون ہیں؟,,,,قصہ مختصر..عظیم سرور (1 2 3 ... آخری صفحہ) محب علوی		03-15-2008 PM 06:43 بذریعہ شمشاد	43	483
خُود کُش حملے: ایک اور سوال (1 2 3 ... آخری صفحہ) سیدہ شگفتہ		03-15-2008 AM 05:35 بذریعہ بمت علی	35	676
شنکر اچاریہ بمت علی		03-15-2008 AM 01:30 بذریعہ بمت علی	0	27
سعودی حکومت کے مفتی نے القاعدہ کو شیطانی قرار دے دیا فاروق سرور خان		03-09-2008 AM 06:34 بذریعہ فاروق سرور خان	0	43
اکیلے مجاہد یا مختصر جماعت کا دشمن کے بڑے لشکر پر حملہ (1 2) واجدحسین		03-07-2008 PM 02:23 بذریعہ محمد شوئیض	10	140

Cyber Revolution in Iran: Ongoing

- Government uses service deactivation and monitoring to disrupt opposition communications
- Opposition uses DDoS attacks and twitter to spread dissident messages
- *Pro-opposition Hacker Group “209,” Organizing and Coordinating its Hacking Campaigns through Twitter (Right)*



از یاران دبستانی به قهرمانان در زنجیر

با شما هستیم سردمداران قوم حاکم!

- نه تنها آینده ساز نبودید، حتی نتوانستید، اساسی ترین حقوق ما را تامین کنید. نه تنها در جامعه کار تولید نکردید، روزنامه هایمان را هم توقیف کردید، و حالا در صدد مسدود کردن تنها روزنه ی ما به دنیای بیرون هستید.
- دنیایی که مال ما نیست ولی آرزویش را داریم. دنیای آزادی که اگرچه هرگز طعمش را نچشیده ایم، ولی می دانیم وجود دارد. دنیایی که اگر واقعا بخواهیم می توانیم داشته باشیم.
- می دانیم که قدرت و اسلحه در دست شماست و بارها بیرحمی تان را ثابت کرده اید، ولی مطمئن باشید در این جنگ، شکست از آن شماست. دنیای مجازی قلمرو ماست. اگر در دنیای ما خیال درگیری با ما دارید به عواقب آن هم فکر کنید.
- دردتان چیست؟! که در مکتب تان شستشوی مغزی نشدیم، یا نتوانستید ما را به مواد مخدری که به داخل کشور قاچاق می کنید، معتاد نمایید. یا کلا وجود ما خاری به چشمتان شده است.
- ما وجود داریم!
- شما خفقان را به حد اکثر رسانده اید. این بهترین شیوه ی مبارزه مدنی با حاکمیت است. شکست شما قطعی است. ما پایگاههای اطلاع رسانی شما را یکی پس از دیگری تصاحب خواهیم کرد و به شما قدرتمان را نشان خواهیم داد.

Regional Trends – Brazil

2008 Proof of Concept: Hacks Change Data of Brazilian Ministry of Natural Resources Management

Result: millions of Reais in illegal logging

Permissive Environment

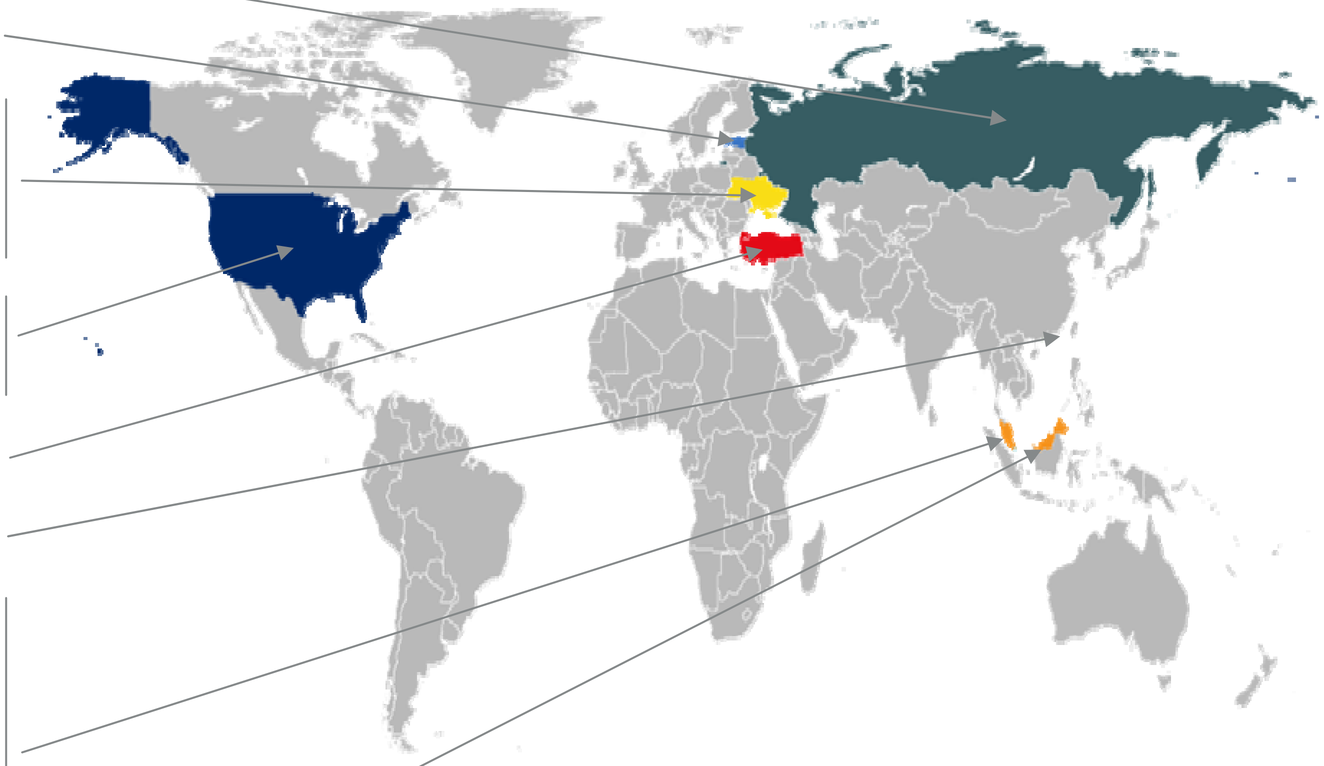
Financially Motivated

Innovative Attack Vectors

Catalyst: Bullet Proof Hosting

Provider Name	Origin
Madet Ltd.	Russia
STARLINE_EE	Estonia
UATELECOM	Ukraine
UrkTeleGroup	Ukraine
Colocall Ltd.	Ukraine
HopOne	USA
Net Access	USA
ABDAllah	Turkey
Hostfresh	Hong Kong
TIMETELECOM	Malaysia
TMNET-BORNEO	Malaysia
MALAYSIA BERHAD	Malaysia
PRIADIUS NET	Malaysia
Applied Info Mgt	Malaysia
Starhub Internet	Singapore

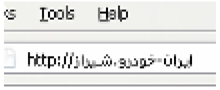
Published in 2002



Press Exposure Kills: RBN, McColo, Intercage

Disruptor/Catalyst: Splintered Internet

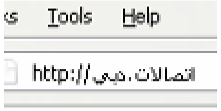
Farsi



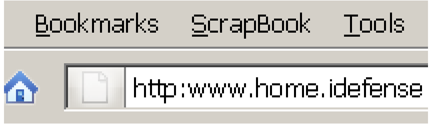
http://ایران-خودرو.شیراز

Top Level Domains

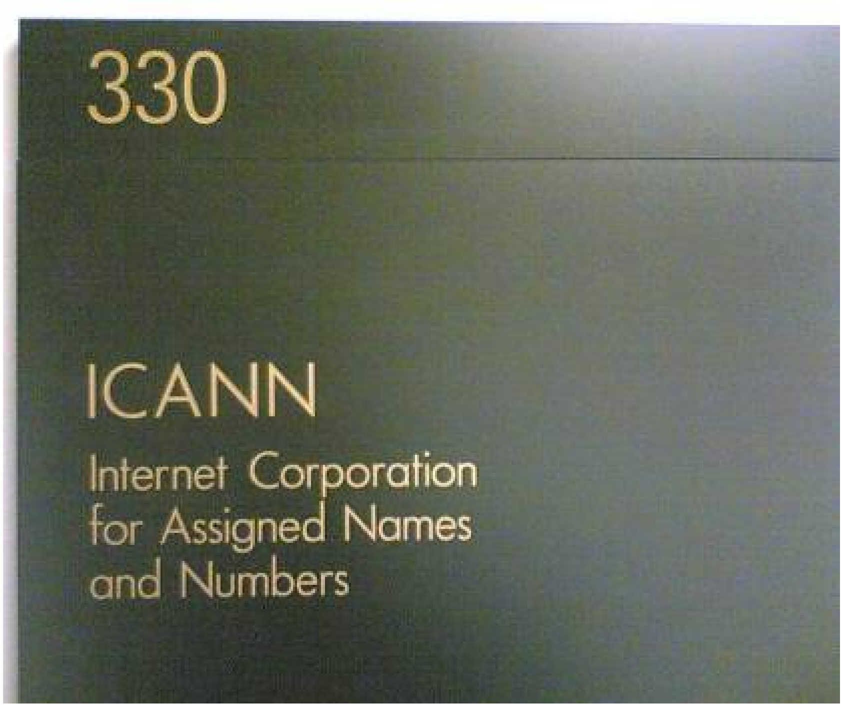
Arabic

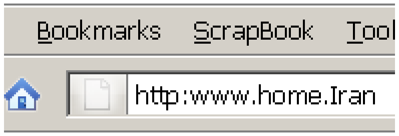


http://اتصالات.دبي



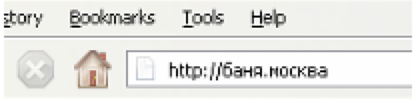
http:www.home.idefense





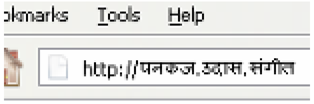
http:www.home.Iran

Russian



http://баня.москва

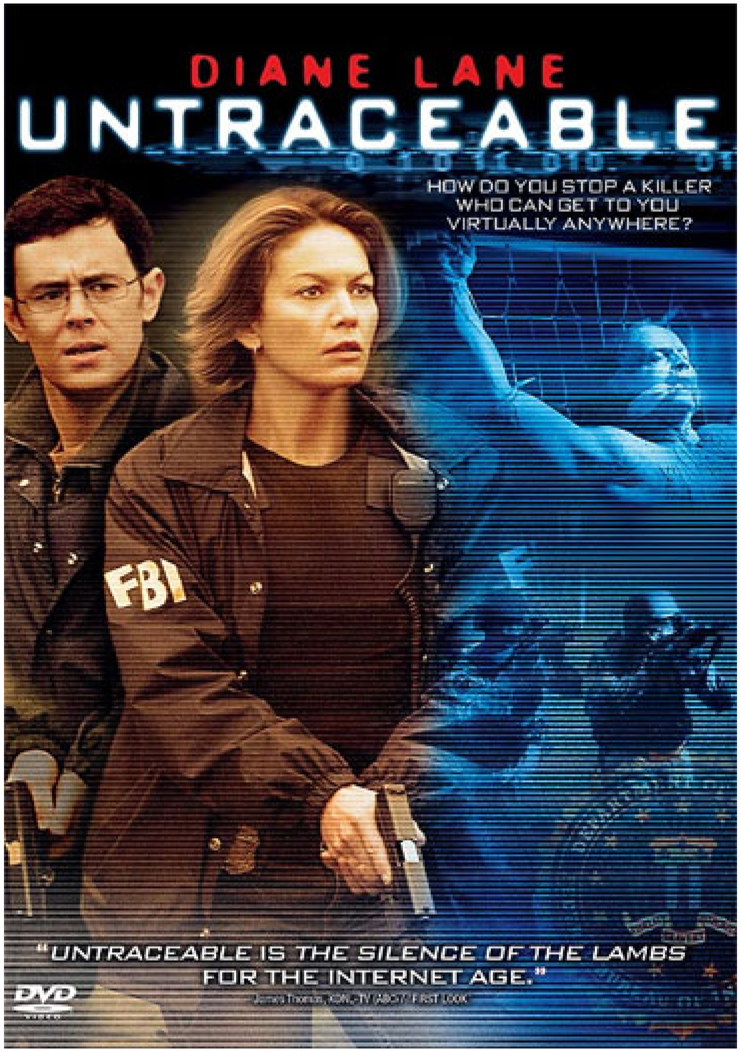
Hindi



http://पनकज.उदास.संगीत

International Domains

Catalyst: Evolving FastFlux, DoubleFlux, MetaFlux


DIANE LANE
UNTRACEABLE
HOW DO YOU STOP A KILLER WHO CAN GET TO YOU VIRTUALLY ANYWHERE?
FBI
"UNTRACEABLE IS THE SILENCE OF THE LAMBS FOR THE INTERNET AGE."
DVD

Manipulates DNS

Distributed Botnets

Practically Untraceable

Permanent Malicious Infrastructure

Better than Bullet Proof Hosting

Asprox – OlateSuite - Storm

Why is Progress Elusive?

- Conflicting Interests…turf wars…

- Lack of conceptual clarity…almost no consensus among the expert communities

- Foundational Theories are absent or poorly formed

Theories of Cyber Warfare

- Until 2007, there was no empirical evidence of cyber conflict…only secretive examples of cyber espionage

- Now, we have examples, and everything is much different than most theorists supposed

- 2 biggest conceptual (and empirical) problems:
  - Deterrence
  - The Security Dilemma

Theories of Cyber Warfare: Deterrence

- Basic premise: if you can’t defend, threaten to attack in response
- Model of nuclear deterrence in the Cold War

- Many theorists think that this concept is useful for cyber warfare:

- IT IS NOT!

Theories of Cyber Warfare: Deterrence

- Deterrence requires:
  - Capacity to impose pain on adversary
  - Credible threat to be able to impose pain
  - Ability to absorb first attack and respond
  - Ability to respond in variable way
  - Ability to identify attacker
- With cyber attacks, many of these are not present
  - Difficult to identify attacker
  - Others can pose as attacker
  - Damage assessment is unclear
  - No guarantee that attack will not also hurt others

Theories of Cyber Warfare: The Security Dilemma

- Basic premise: Efforts to increase your own security makes other insecure

- With Cyber Warfare:
  - Everyone can attack easier than they can defend
  - Sometimes, defense and attack are difficult to distinguish
  - Most countries are talking more about offense
  - Private sector and underground are doing offense

- Results:
  - Spiral of Mistrust
  - Incentives to go on the offense

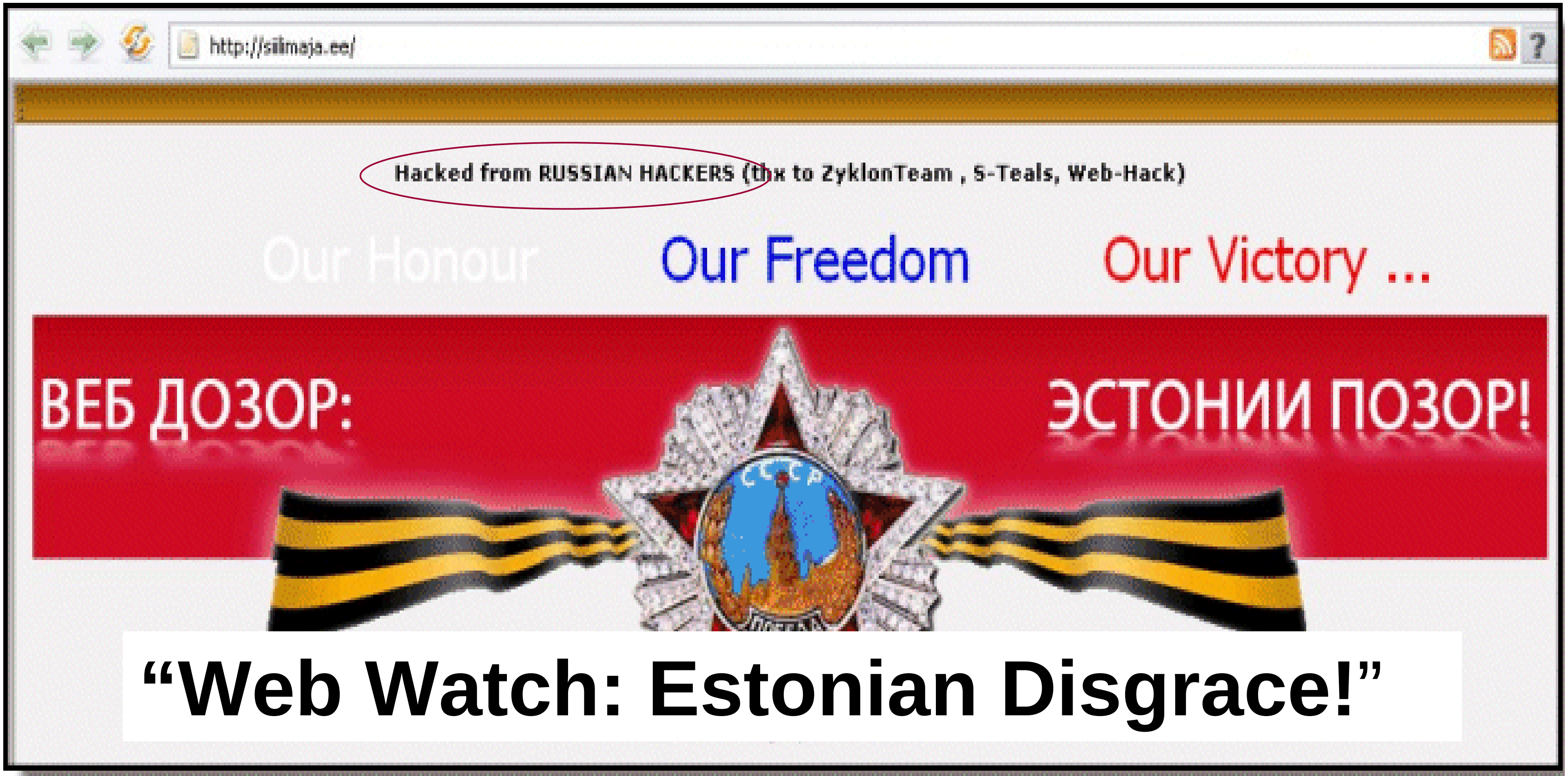
The Security Dilemma: Game Theory Foundation

		Player 2	
		Hold	Attack
Player 1	Hold	(1) Low Threat ; (2) Low Threat	(1) Exploited ; (2) Dominant
	Attack	(1) Dominant ; (2) Exploited	(1) Arms Race ; (2) Arms Race

The Realities of Cyber Conflict

- Nothing like the theorists though it would be
- Messy…not entirely controlable
- No understanding of ultimate consequences…interconnected networks yield extensive feedback
- Symbolic effects are often as important as direct effects

Russian Attacks Against Estonia: May 2007



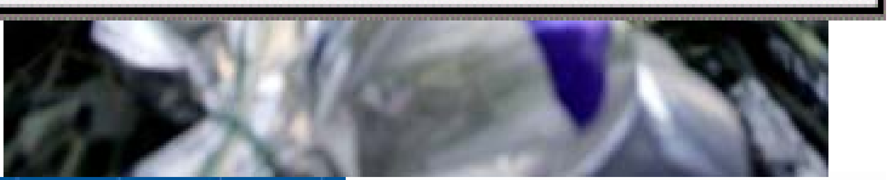
http://silimaja.ee/

Hacked from RUSSIAN HACKERS (thx to ZyklonTeam , 5-Teals, Web-Hack)

Our Honour Our Freedom Our Victory ...

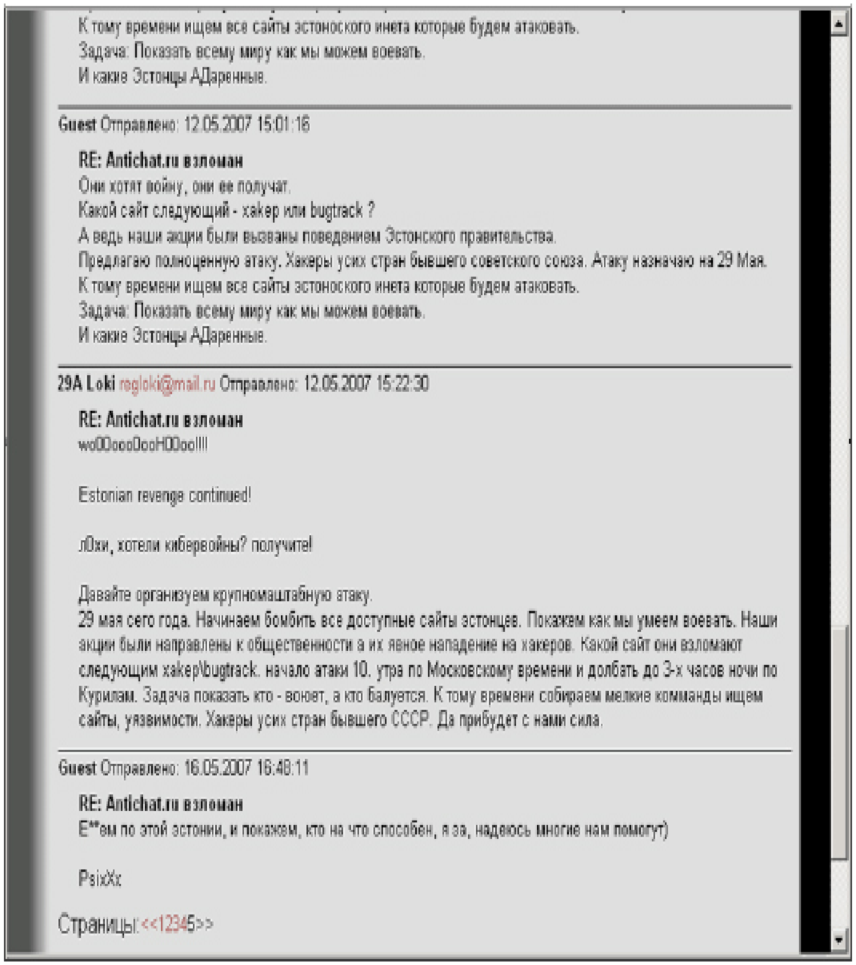
ВЕБ ДОЗОР: ЭСТОНИИ ПОЗОР!

“Web Watch: Estonian Disgrace!”



Russian DDoS Coordination

- Organized on Blogs (e.g. antichat.ru, Livejournal)
- New Attack lists circulated among hundreds of blogs in minutes
- Highly coordinated
- Hundreds of attackers
- Many identified as ordinary people



К тому времени ищем все сайты эстоноского инета которые будем атаковать.
Задача: Показать всему миру как мы можем воевать.
И какие Эстонцы АДаренные.

Guest Отправлено: 12.05.2007 15:01:16

RE: Antichat.ru взломан
Они хотят войну, они ее получат.
Какой сайт следующий - хакер или bugtrack ?
А ведь наши акции были вызваны поведением Эстонского правительства.
Предлагаю полноценную атаку. Хакеры усих стран бывшего советского союза. Атаку назначаю на 29 Мая.
К тому времени ищем все сайты эстоноского инета которые будем атаковать.
Задача: Показать всему миру как мы можем воевать.
И какие Эстонцы АДаренные.

29A Loki regloki@mail.ru Отправлено: 12.05.2007 15:22:30

RE: Antichat.ru взломан
woOOoooOooHOOoo!!!!

Estonian revenge continued!

л0хи, хотели кибервойны? получите!

Давайте организуем крупномаштабную атаку.
29 мая сего года. Начинаем бомбить все доступные сайты эстонцев. Покажем как мы умеем воевать. Наши акции были направлены к общественности а их явное нападение на хакеров. Какой сайт они взломают следующим хакер\bugtrack. начало атаки 10. утра по Московскому времени и долбать до 3-х часов ночи по Курилам. Задача показать кто - воюет, а кто балуется. К тому времени собираем мелкие комманды ищем сайты, уязвимости. Хакеры усих стран бывшего СССР. Да прибудет с нами сила.

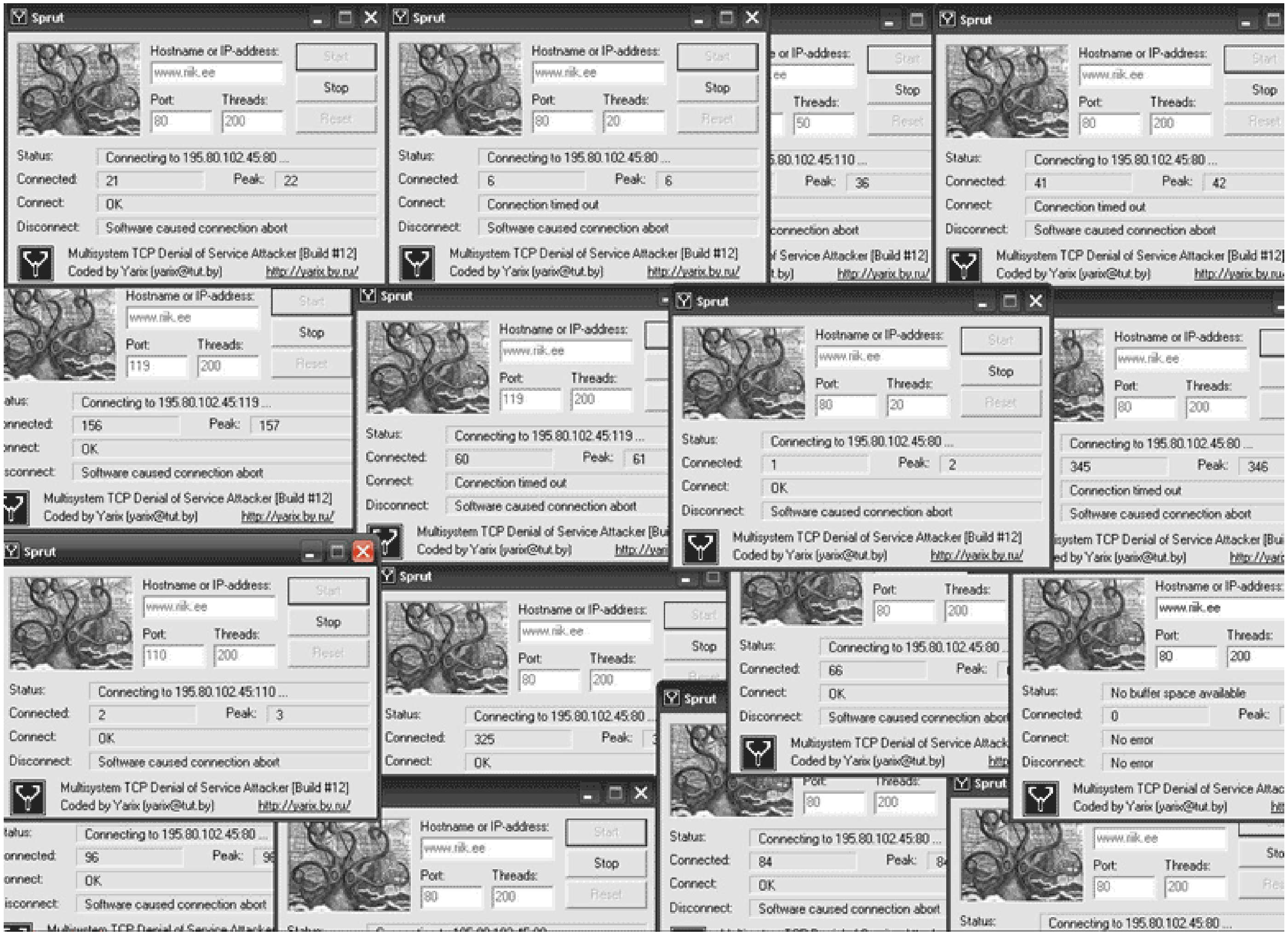
Guest Отправлено: 16.05.2007 16:48:11

RE: Antichat.ru взломан
E**ем по этой эстонии, и покажем, кто на что способен, я за, надеюсь многие нам помогут)

PsixXx

Страницы: <<12345>>

Russian DDoS Attack Tool: Sprut



Sprut
Hostname or IP-address: www.riik.ee
Port: 80 Threads: 200
Status: Connecting to 195.80.102.45:80 ...
Connected: 21 Peak: 22
Connect: OK
Disconnect: Software caused connection abort
Multisystem TCP Denial of Service Attacker [Build #12]
Coded by Yarix (yarix@tut.by) http://yarix.by.ru/

Sprut
Hostname or IP-address: www.riik.ee
Port: 80 Threads: 20
Status: Connecting to 195.80.102.45:80 ...
Connected: 6 Peak: 6
Connect: Connection timed out
Disconnect: Software caused connection abort
Multisystem TCP Denial of Service Attacker [Build #12]
Coded by Yarix (yarix@tut.by) http://yarix.by.ru/

e or IP-address:
ee
Threads: 50
.80.102.45:110 ...
Peak: 36
connection abort
f Service Attacker [Build #12]
t.by) http://yarix.by.ru/

Sprut
Hostname or IP-address: www.riik.ee
Port: 80 Threads: 200
Status: Connecting to 195.80.102.45:80 ...
Connected: 41 Peak: 42
Connect: Connection timed out
Disconnect: Software caused connection abort
Multisystem TCP Denial of Service Attacker [Build #12]
Coded by Yarix (yarix@tut.by) http://yarix.by.ru

Hostname or IP-address: www.riik.ee
Port: 119 Threads: 200
atus: Connecting to 195.80.102.45:119 ...
nnected: 156 Peak: 157
nnect: OK
sconnect: Software caused connection abort
Multisystem TCP Denial of Service Attacker [Build #12]
Coded by Yarix (yarix@tut.by) http://yarix.by.ru/

Sprut
Hostname or IP-address: www.riik.ee
Port: 119 Threads: 200
Status: Connecting to 195.80.102.45:119 ...
Connected: 60 Peak: 61
Connect: Connection timed out
Disconnect: Software caused connection abort
Multisystem TCP Denial of Service Attacker [Bu
Coded by Yarix (yarix@tut.by) http://yari

Sprut
Hostname or IP-address: www.riik.ee
Port: 80 Threads: 20
Status: Connecting to 195.80.102.45:80 ...
Connected: 1 Peak: 2
Connect: OK
Disconnect: Software caused connection abort
Multisystem TCP Denial of Service Attacker [Build #12]
Coded by Yarix (yarix@tut.by) http://yarix.by.ru/

Hostname or IP-address: www.riik.ee
Port: 80 Threads: 200
Connecting to 195.80.102.45:80 ...
345 Peak: 346
Connection timed out
Software caused connection abort
ystem TCP Denial of Service Attacker [Bu
ed by Yarix (yarix@tut.by) http://yari

Sprut
Hostname or IP-address: www.riik.ee
Port: 110 Threads: 200
Status: Connecting to 195.80.102.45:110 ...
Connected: 2 Peak: 3
Connect: OK
Disconnect: Software caused connection abort
Multisystem TCP Denial of Service Attacker [Build #12]
Coded by Yarix (yarix@tut.by) http://yarix.by.ru/

Sprut
Hostname or IP-address: www.riik.ee
Port: 80 Threads: 200
Status: Connecting to 195.80.102.45:80 ...
Connected: 325 Peak: 3
Connect: OK

Port: 80 Threads: 200
Status: Connecting to 195.80.102.45:80 ...
Connected: 66 Peak:
Connect: OK
Disconnect: Software caused connection abor
Multisystem TCP Denial of Service Attack
Coded by Yarix (yarix@tut.by) http

Hostname or IP-address: www.riik.ee
Port: 80 Threads: 200
Status: No buffer space available
Connected: 0 Peak:
Connect: No error
Disconnect: No error
Multisystem TCP Denial of Service Attac
Coded by Yarix (yarix@tut.by) htt

tatus: Connecting to 195.80.102.45:80 ...
onnected: 96 Peak: 96
onnect: OK
isconnect: Software caused connection abort
Multisystem TCP Denial of Service Attacke

Hostname or IP-address: www.riik.ee
Port: 80 Threads: 200

Sprut
Port: 80 Threads: 200
Status: Connecting to 195.80.102.45:80 ...
Connected: 84 Peak: 84
Connect: OK
Disconnect: Software caused connection abort

Sprut
www.riik.ee
Port: 80 Threads: 200
Status: Connecting to 195.80.102.45:80 ...

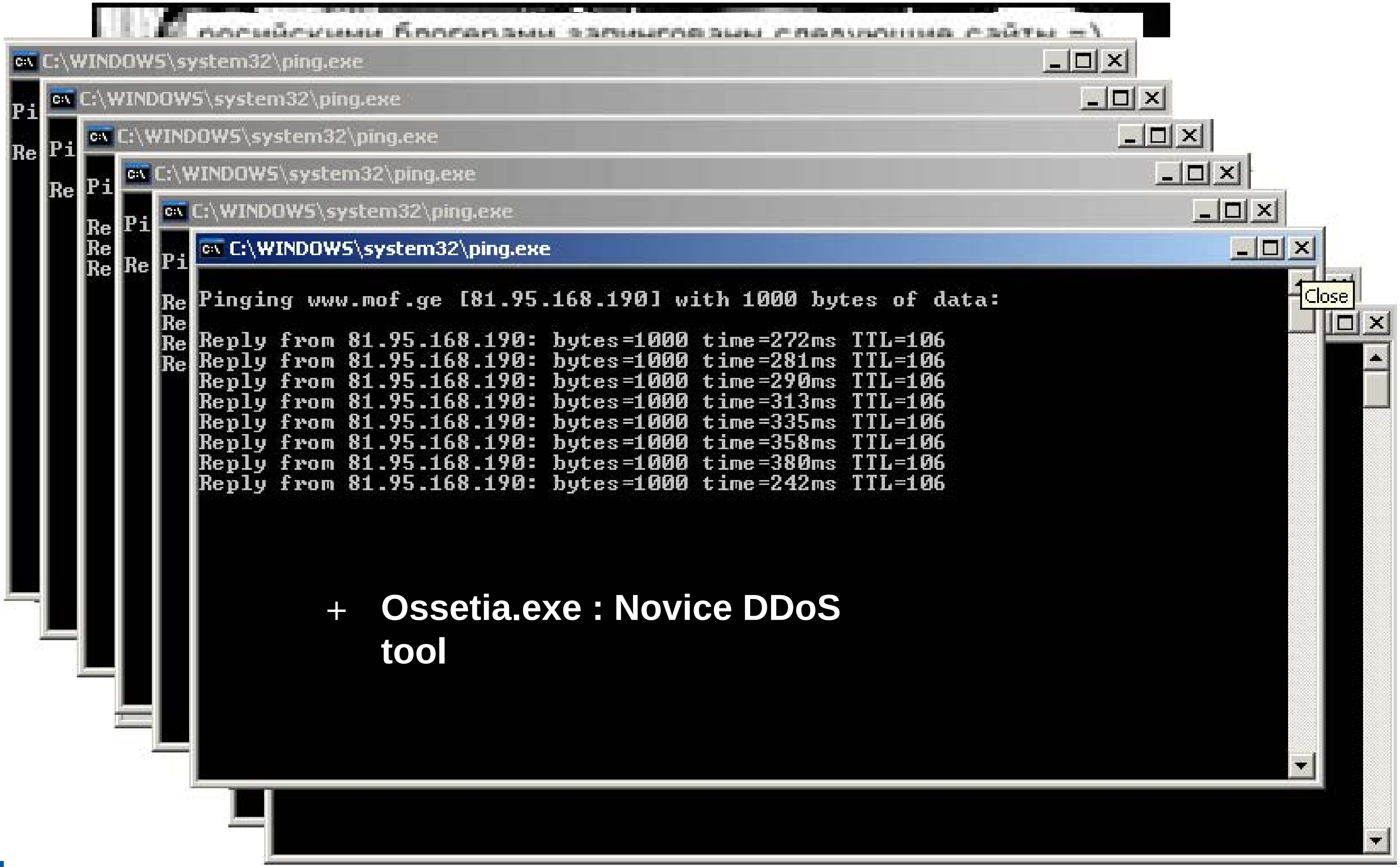
Effects on Estonia

- Major disruption to government websites and e-government services
- Varying disruption to financial institutions
  - Some banks shut down for 1 day or more
  - Most banks have problems for several hours
  - ATMs disrupted
- No real response plan in Estonia, but with NATO assistance, they handled it well
- Problem: nothing could have prevented the attacks completely

Russia vs. Georgia: August, 2008

- Presaged by more robust equipment installation in Georgia
- Unlike Estonia, Georgia fought back
- Both sides attack the other’s media sites
- Russia completely shuts off Georgian government’s web space
- Georgia began hosting some sites on Blogger.com pages:
  - Why?
  - Because Russia can take down a country, but it can’t stop Google.

Russia Takes Down Georgian Government Sites



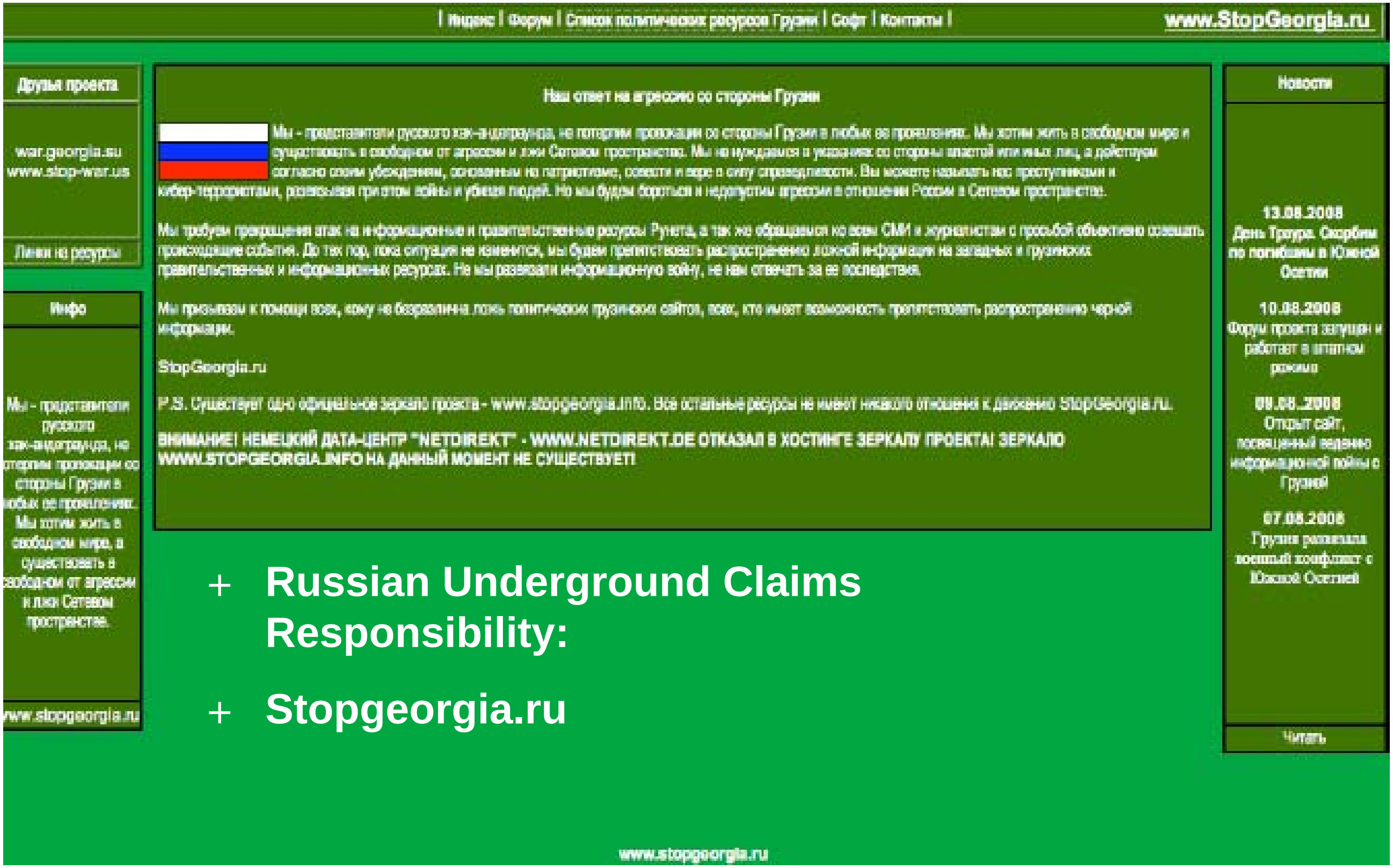
российскими блогерами [illegible] следующие сайты =)

```
Pinging www.mof.ge [81.95.168.190] with 1000 bytes of data:

Reply from 81.95.168.190: bytes=1000 time=272ms TTL=106
Reply from 81.95.168.190: bytes=1000 time=281ms TTL=106
Reply from 81.95.168.190: bytes=1000 time=290ms TTL=106
Reply from 81.95.168.190: bytes=1000 time=313ms TTL=106
Reply from 81.95.168.190: bytes=1000 time=335ms TTL=106
Reply from 81.95.168.190: bytes=1000 time=358ms TTL=106
Reply from 81.95.168.190: bytes=1000 time=380ms TTL=106
Reply from 81.95.168.190: bytes=1000 time=242ms TTL=106
```

- **Ossetia.exe : Novice DDoS tool**

Pro-South Ossetian Spam



| Индекс | Форум | Список политических ресурсов Грузии | Софт | Контакты |

www.StopGeorgia.ru

Друзья проекта

war.georgia.su
www.stop-war.us

Линки на ресурсы

Инфо

Мы - представители русского хак-андерграунда, не потерпим провокации со стороны Грузии в любых ее проявлениях. Мы хотим жить в свободном мире, а существовать в свободном от агрессии и лжи Сетевом пространстве.

www.stopgeorgia.ru

Наш ответ на агрессию со стороны Грузии

Мы - представители русского хак-андерграунда, не потерпим провокации со стороны Грузии в любых ее проявлениях. Мы хотим жить в свободном мире и существовать в свободном от агрессии и лжи Сетевом пространстве. Мы не нуждаемся в указаниях со стороны властей или иных лиц, а действуем согласно своим убеждениям, основанным на патриотизме, совести и вере в силу справедливости. Вы можете называть нас преступниками и кибер-террористами, развязывая при этом войны и убивая людей. Но мы будем бороться и недопустим агрессии в отношении России в Сетевом пространстве.

Мы требуем прекращения атак на информационные и правительственные ресурсы Рунета, а так же обращаемся ко всем СМИ и журналистам с просьбой объективно освещать происходящие события. До тех пор, пока ситуация не изменится, мы будем препятствовать распространению ложной информации на западных и грузинских правительственных и информационных ресурсах. Не мы развязали информационную войну, не нам отвечать за ее последствия.

Мы призываем к помощи всех, кому не безразлична ложь политических грузинских сайтов, всех, кто имеет возможность препятствовать распространению черной информации.

StopGeorgia.ru

P.S. Существует одно официальное зеркало проекта - www.stopgeorgia.info. Все остальные ресурсы не имеют никакого отношения к движению StopGeorgia.ru.

ВНИМАНИЕ! НЕМЕЦКИЙ ДАТА-ЦЕНТР "NETDIREKT" - WWW.NETDIREKT.DE ОТКАЗАЛ В ХОСТИНГЕ ЗЕРКАЛУ ПРОЕКТА! ЗЕРКАЛО WWW.STOPGEORGIA.INFO НА ДАННЫЙ МОМЕНТ НЕ СУЩЕСТВУЕТ!

Новости

13.08.2008
День Траура. Скорбим по погибшим в Южной Осетии

10.08.2008
Форум проекта запущен и работает в штатном режиме

09.08.2008
Открыт сайт, посвященный ведению информационной войны с Грузией

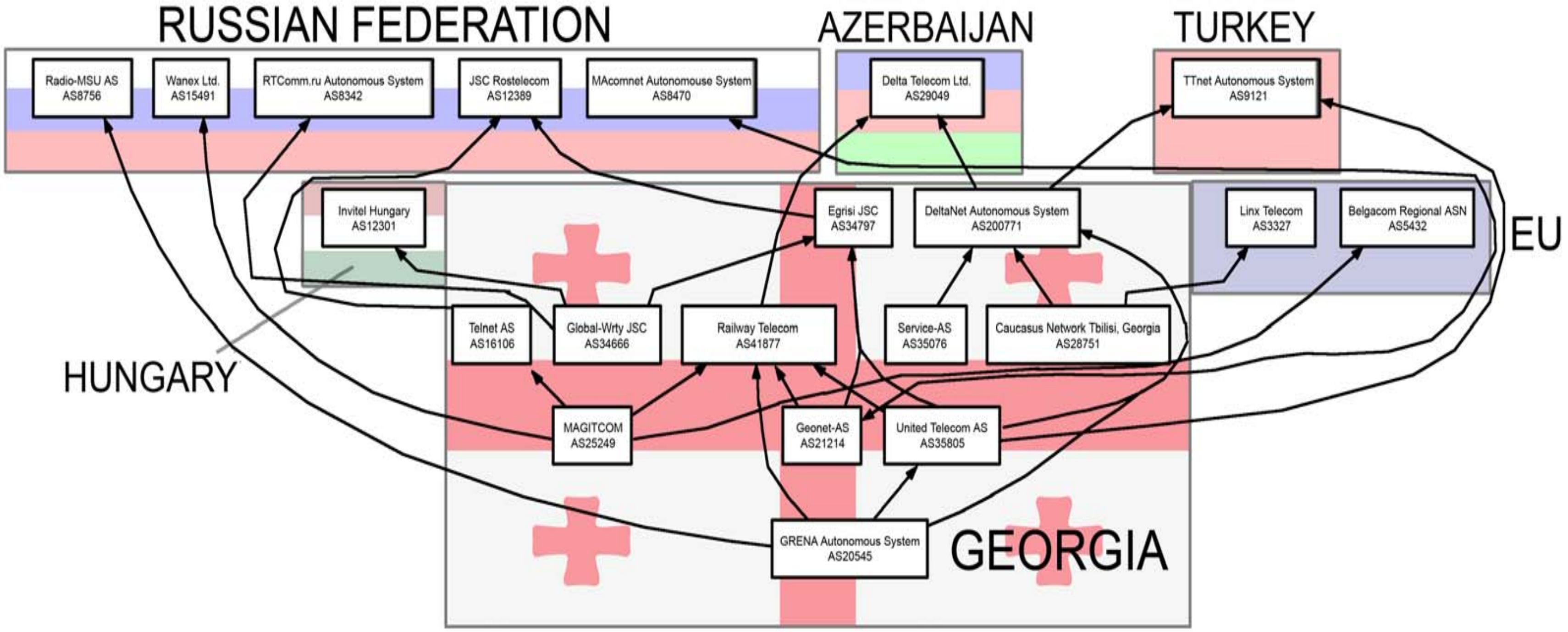
07.08.2008
Грузия развязала военный конфликт с Южной Осетией

Читать

www.stopgeorgia.ru

- **Russian Underground Claims Responsibility:**
- **Stopgeorgia.ru**

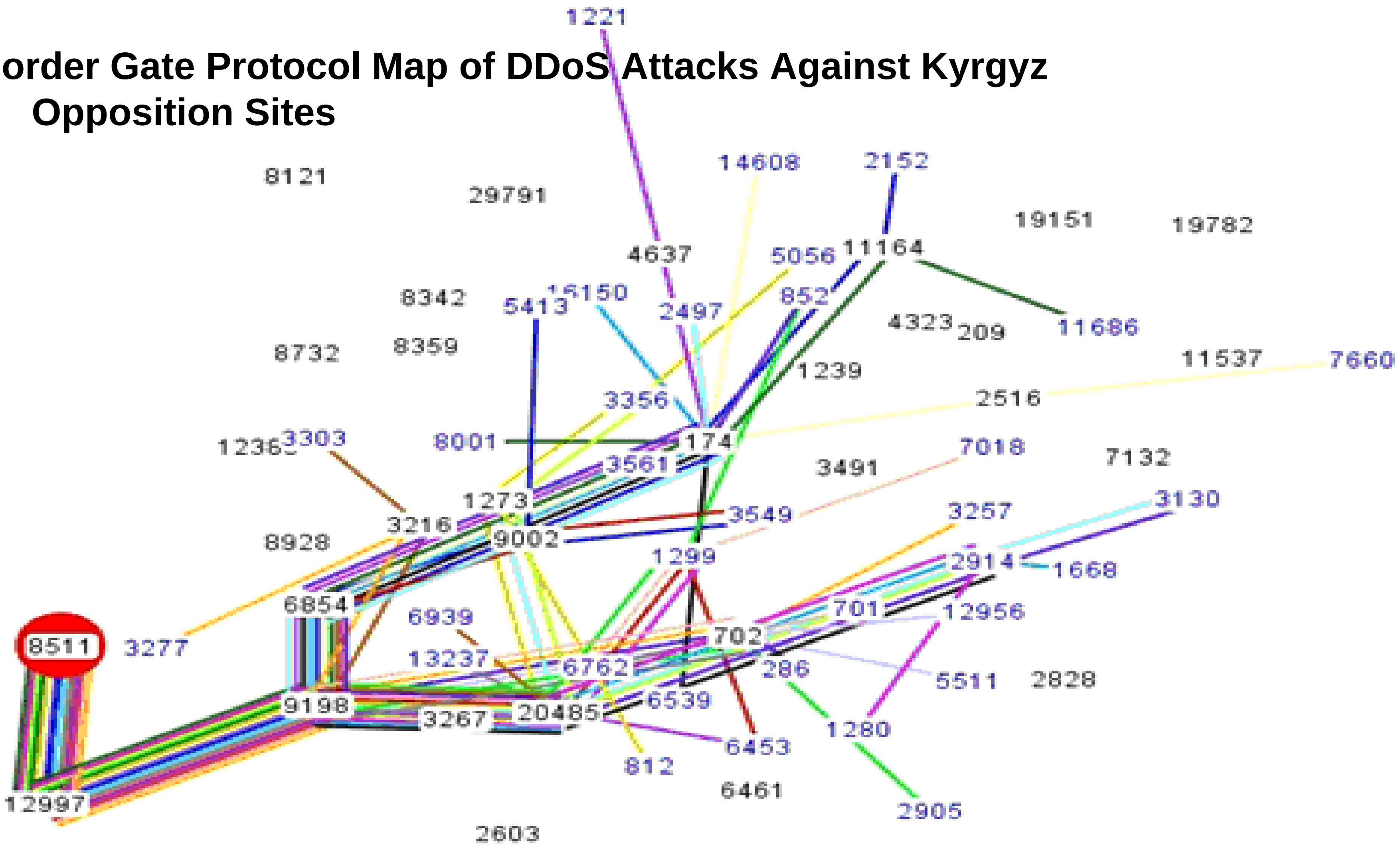
Russia Also Deactivated Cables


RUSSIAN FEDERATION
AZERBAIJAN
TURKEY
Radio-MSU AS AS8756
Wanex Ltd. AS15491
RTComm.ru Autonomous System AS8342
JSC Rostelecom AS12389
MAcomnet Autonomouse System AS8470
Delta Telecom Ltd. AS29049
TTnet Autonomous System AS9121
Invitel Hungary AS12301
Egrisi JSC AS34797
DeltaNet Autonomous System AS200771
Linx Telecom AS3327
Belgacom Regional ASN AS5432
EU
Telnet AS AS16106
Global-Wrty JSC AS34666
Railway Telecom AS41877
Service-AS AS35076
Caucasus Network Tbilisi, Georgia AS28751
HUNGARY
MAGITCOM AS25249
Geonet-AS AS21214
United Telecom AS AS35805
GRENA Autonomous System AS20545
GEORGIA

Courtesy of Arbor Networks

Kyrgyzstan: January, 2009

Border Gate Protocol Map of DDoS Attacks Against Kyrgyz Opposition Sites



Cyber Security Becomes a Public Affair

+ More offense:
  - Hints of a more offense-heavy strategy in new Administration’s proto-policy
+ Law Enforcement, Contractors and Consultants already doing so or are planning to
  - Definitely pragmatic, but offense is a dangerous default
+ What deterrence?
  - Attacker Origin?
  - Second-order effects?
  - Damage Assessment?
+ Increased Budgets = Dramatic Shift in Industry Priorities

What does this mean for Policy?

+ Is a cyberczar a good idea?
  - In the US?
  - The EU?

+ What is “the cyber infrastructure”?
  - Is it even realistic to think we can secure it all?
  - What international legal problems does this raise?
  - Do the obligations it imposes outweigh the benefits?

+ Is more offense a good idea?
  - Alternative— trapped defense
  - Alternative— collective defense

+ Do we even know how to spend $6 billion? Who will do it?

+ Where are the diplomats and the treaties?

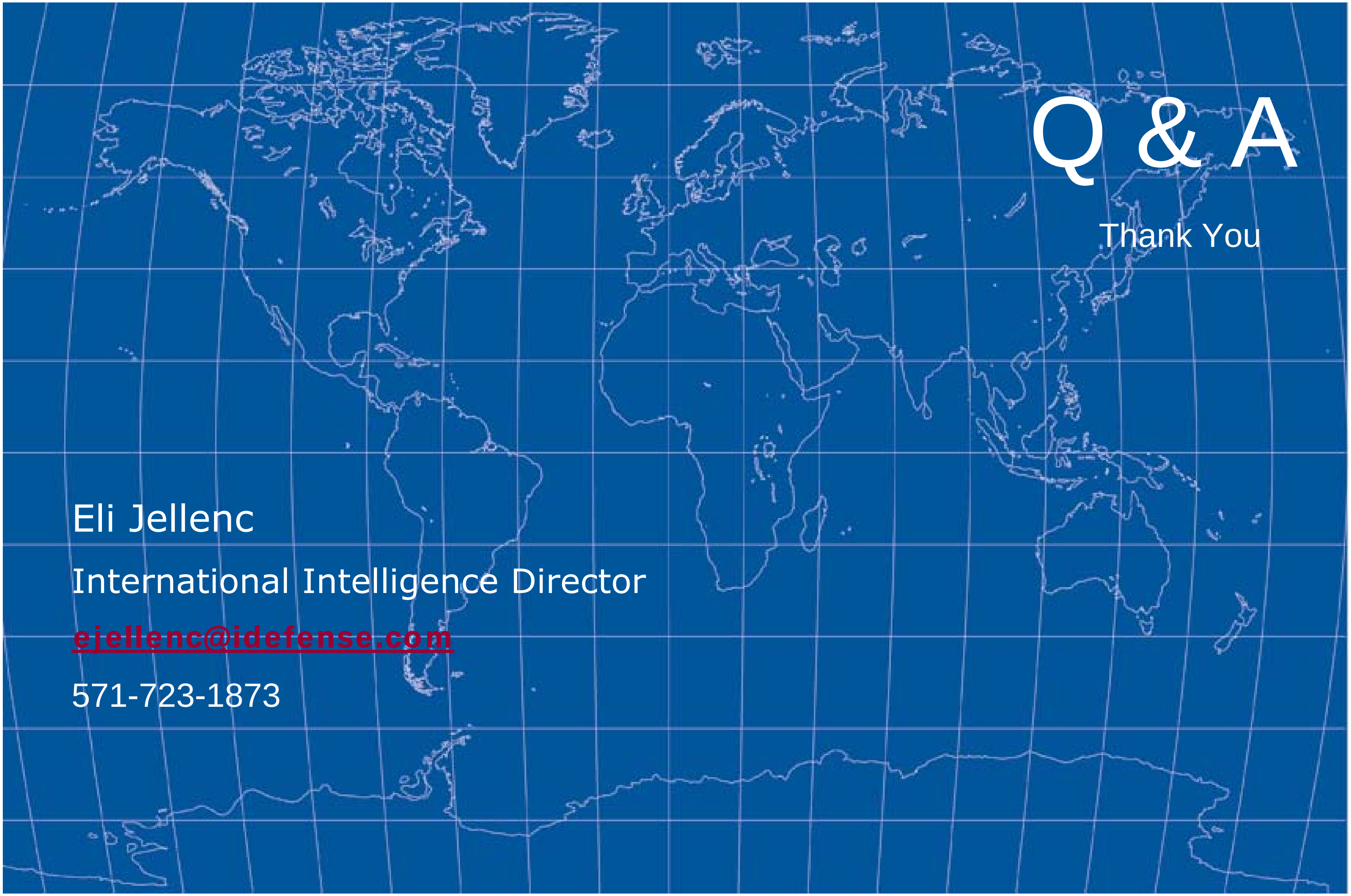
What does this all mean?

- The late 1980s and early 1990s: the age of the pure hacker
- Late 1990s and early 2000s: the age of the cyber criminal
- Now…
- The age of political and strategic information operations…up to and including war

What does this all mean?

- If you thought the worms of the 1990s were bad…
- If you thought RBN and Rockphish and Conficker were bad…
- Just wait…
- Wait until you see what political and strategic organizations with billions of dollars, and incentives for offensive strategies, will do…

iDEFENSE
Actionable Threat Intelligence



Q & A

Thank You

Eli Jellenc

International Intelligence Director

ejellenc@idefense.com

571-723-1873