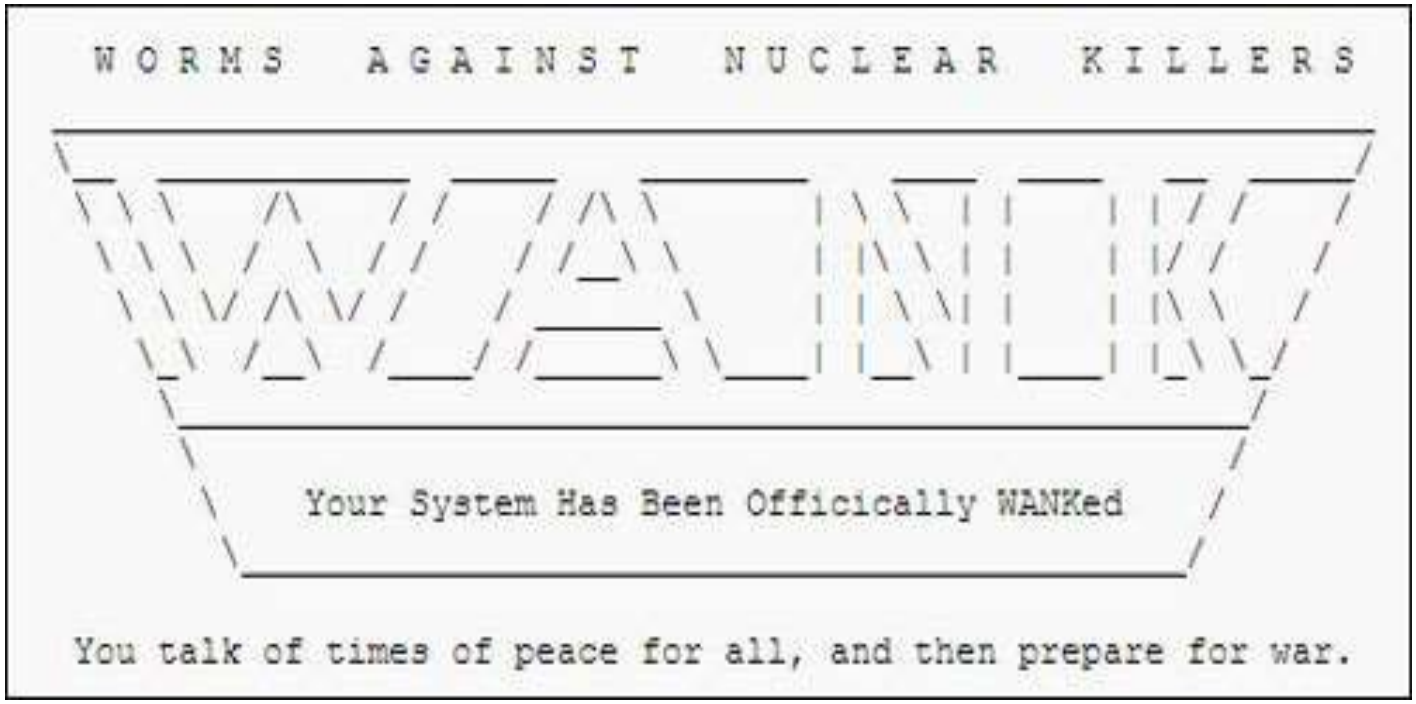
# Cybersecurity
# Cybercrime
# Cyberwarfare

Dr. Alana Maurushat

# What is this?

# Worms Against Nuclear Killers



# OPERATION: TITSTORM

## A PART OF OPERATION INTERNET FREEDOM

3 hours till launch

### THE ATTACK!

1. On February 10th 8:00 AM Australian time we will begin a DDoS of government servers

2. This will be quickly followed by a shitstorm of porn email, fax spam, black faxes, and prank phone calls to government offices (emails/faxes *should* focus on small-breasted porn, cartoon porn, and female ejaculation, the 3 types banned so far)

DDoS Tools & Instructions:
http://www.mediafire.com/?qj0tnwjqhmd
EVERYTHING YOU NEED IS
THERE!! FOLLOW THE INSTRUC-
TIONS!
HAVE FUN!!

### WHAT? WHEN?

PARTICIPATE FELLOW ANONYMOUS!

The Campaign begins...
8:00 AM , **AUSTRALIAN TIME (GMT +10:00)**
February 10th.

**(FEBRUARY 9TH FOR U.S.A. AND CANADA.)**
(5:00 EST | 4:00 CST | etc. )

**TO FULLY PARTICIPATE IN THE ATTACK:**

Use an IRC Client and connect to...

irc.anonnet.org
#titstorm

"We are Anonymous. We are legion."

# What is this?

# EXIF Data

cat.jpg

*(click for original)*

**Camera**
Canon Canon EOS 400D DIGITAL

**GPS Position**
59.924755 degrees N, 10.695598 degrees E

**Date of Creation**
2008:08:05 20:59:32

**Artist**
unknown

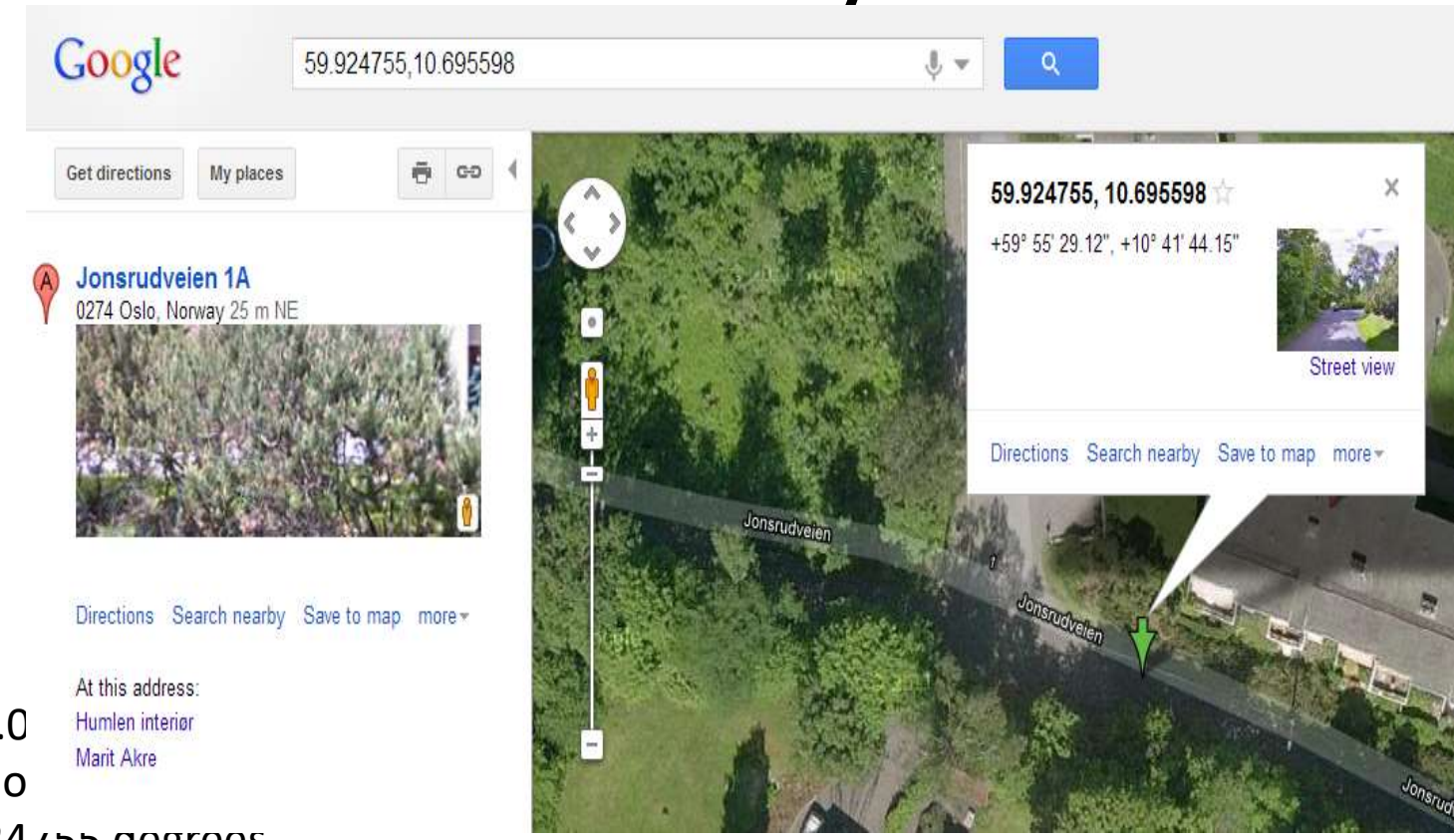
**Resolution**
1280x853

| | |
|---|---|
| **Make** | Canon |
| **Model** | Canon EOS 400D DIGITAL |
| **Exposure** | +0.33 |
| **Aperture** | 2.2 |
| **Exposure Time** | 1/100 (0.01 sec) |
| **Focal Length** | 50.0 mm |
| **Flash** | Off, Did not fire |
| **File Size** | 436 kB |
| **File Type** | JPEG |
| **MIME Type** | image/jpeg |
| **Image Width** | 1280 |
| **Image Height** | 853 |
| **Encoding Process** | Baseline DCT, Huffman coding |
| **Bits Per Sample** | 8 |
| **Color Components** | 3 |
| **X Resolution** | 300 |
| **Y Resolution** | 300 |
| **YCbCr Sub Sampling** | YCbCr4:4:4 (1 1) |
| **Exposure Program** | Program AE |
| **Date and Time (Original)** | 2008:08:05 20:59:32 |
| **Date and Time (Digitized)** | 2008:08:05 20:59:32+02:00 |
| **Max Aperture Value** | 1.4 |
| **Metering Mode** | Average |
| **Custom Rendered** | Normal |
| **Exposure Mode** | Auto |
| **White Balance** | As Shot |
| **Scene Capture Type** | Standard |
| **Contrast** | +25 |
| **Saturation** | N/A |
| **Sharpness** | 25 |
| **F Number** | 2.2 |
| **Exposure** | N/A |

59.924655 N, 10.695598 E

Powered by
Google™
Maps

# The EXIF Data and Analysis




- **GPS Version ID** 2.2.0
- **GPS Latitude Ref** No
- **GPS Latitude** 59.924755 degrees
- **GPS Longitude Ref** East
- **GPS Longitude** 10.695598 degrees
- **GPS Altitude Ref** Above Sea Level
- **GPS Altitude** 81 m

59.924755N,10.695598E

# Geotags

sed Cell Phone Geotags to Dest...

03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq/

Latest Headlines | Customize Links | Free Hotmail | Windows Marketplace | Windows Media | Windows

ADVERTISEMENT

With Kelley Direct's flexible MBA program, you're the one who decides how to get where you want to go. Learn more at a Virtual Open House.

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

**Tip Us Off**

Tip for Defense Tech?

**SEND IT!**

It's Confidential!

**Follow Us!**

**About Defense Tech**

Defense Tech examines the intersection of technology and defense from every angle and provides analysis on what's ahead.



## Insurgents Used Cell Phone Geotags to Destroy AH-64s in Iraq

*By* JOHN REED *on* MARCH 15, 2012

Like 1,258 people like this.

**Milit**

Army to Screen Leaders

British Soldier E

Policy Change Y

Pentagon Wants Prison

Man Sentenced Theft

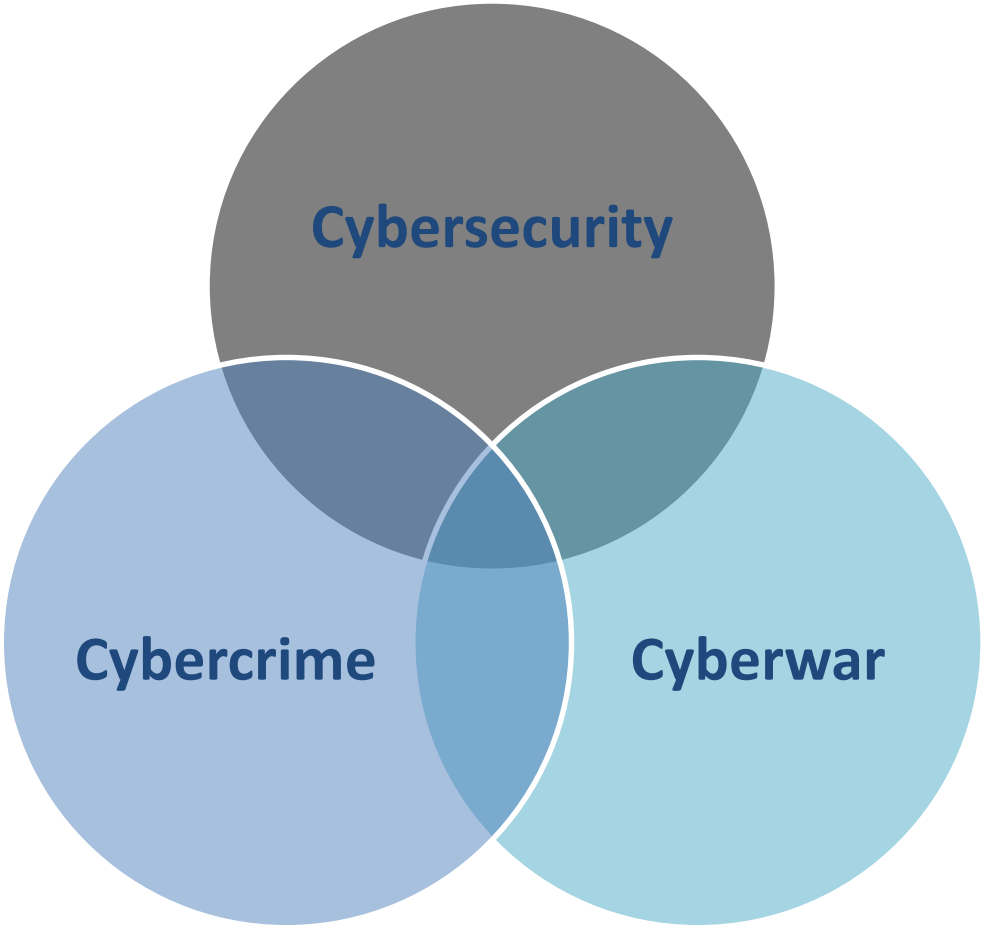
FBI: Man Fatally

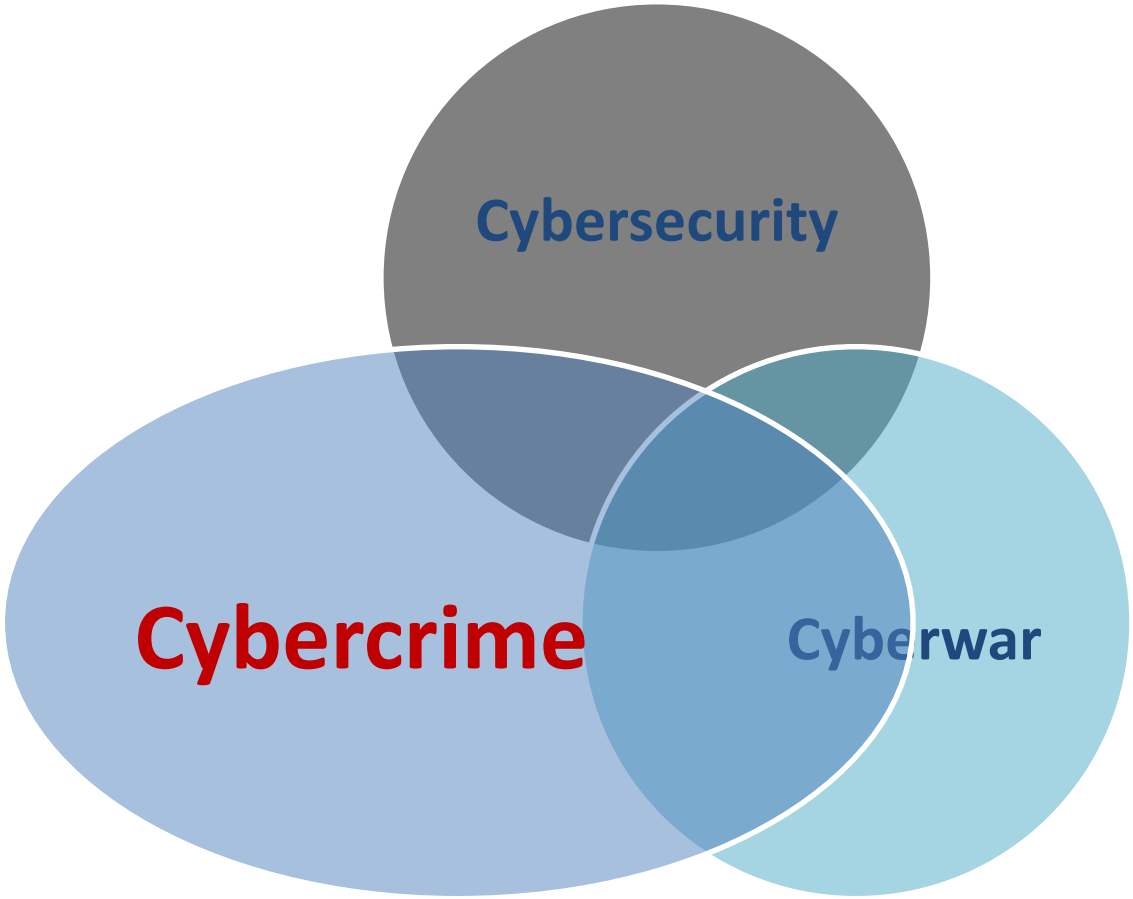
Kerry: US, Allies

With Ke

program

# Terms used loosely, interchangeably and ***dangerously***




Cybersecurity
Cybercrime
Cyberwar

# Cybercrime

## Old Wine, New Bottles?

- Traditional crimes that are committed or enhanced with the use of technology

(Eg. Fraud, stalking)

- New crimes that have

Emerged as a result of a technology

(Eg. "Hacking"/Unauthorised Use)

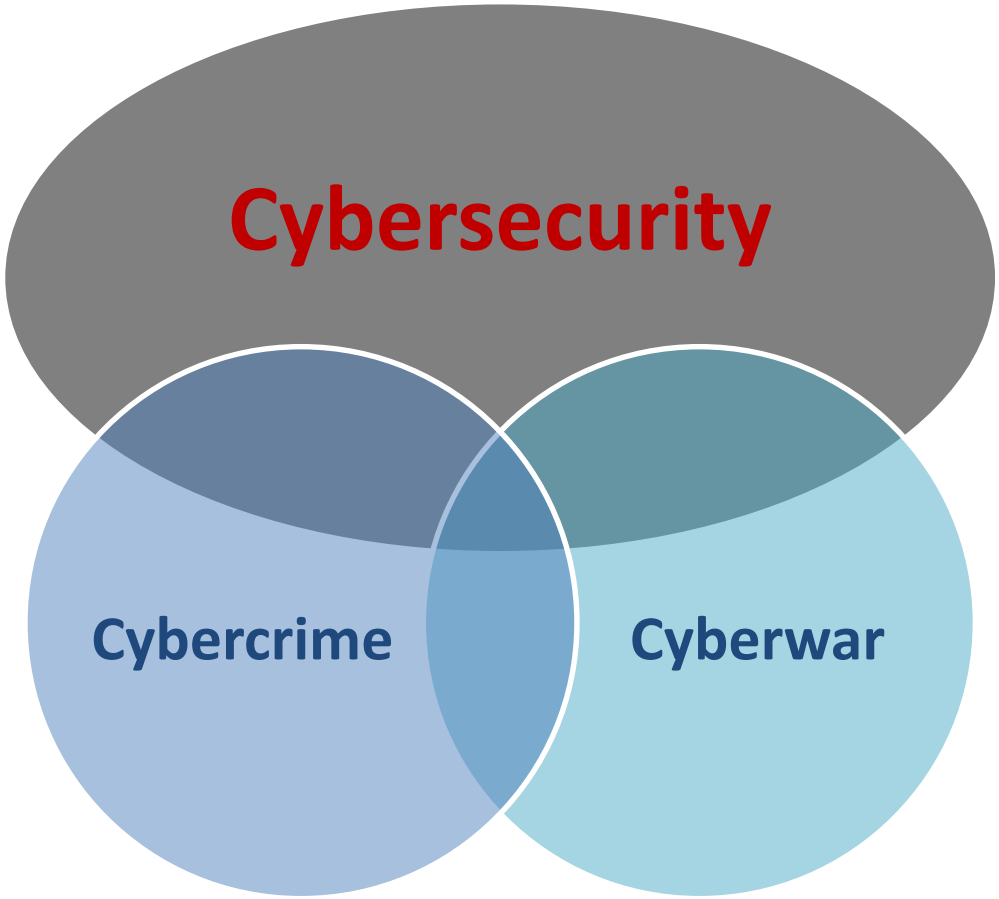
# Convention on Cybercrime

Fraud/Forgery

Copyright Infringement

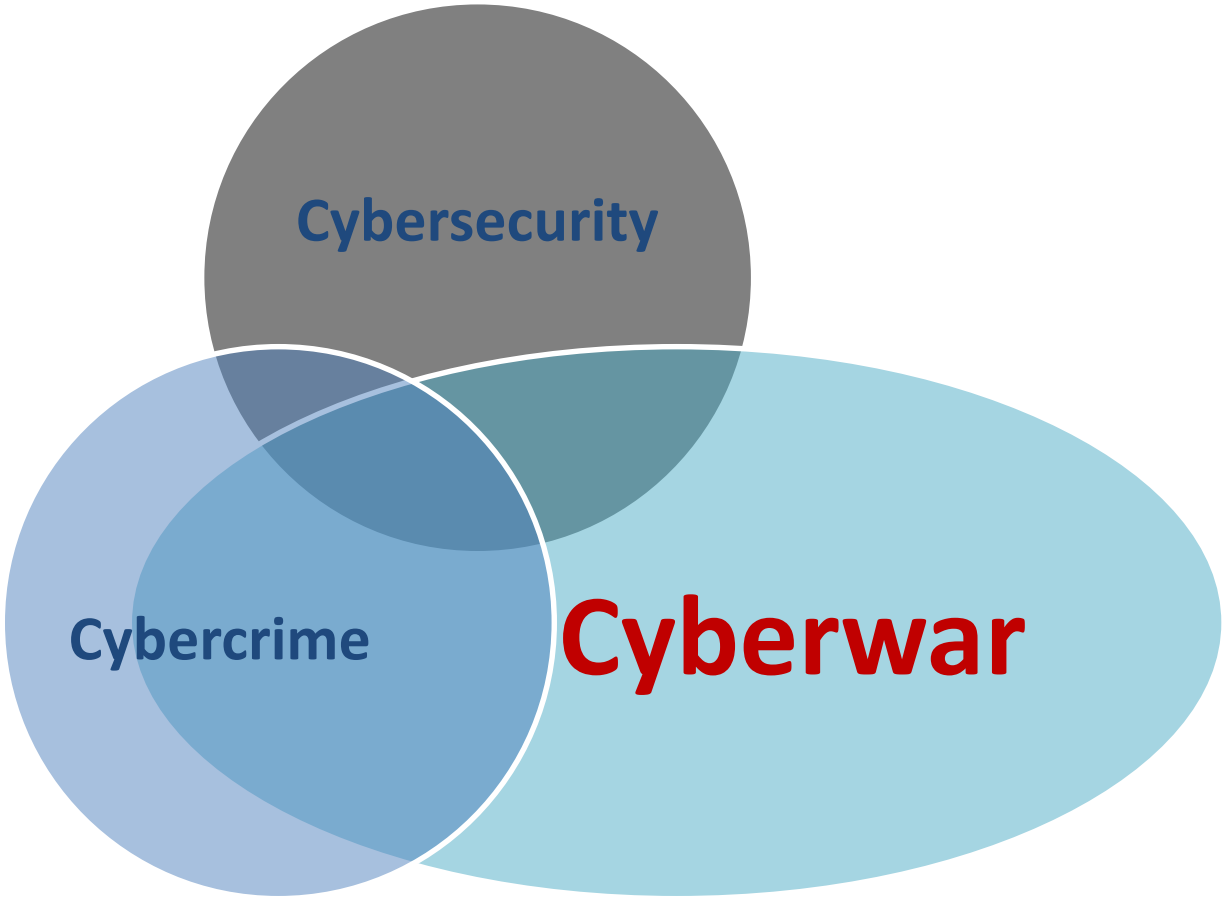
Child Pornography

**Unauthorised Access, Modification, Impairment or Interference with Data, a Data System, or a Computer**


Cybersecurity
Cybercrime
Cyberwar

# Cybersecurity

- Cybersecurity is the protection of data, data systems and computers from unauthorised access, modification, impairment or interference.

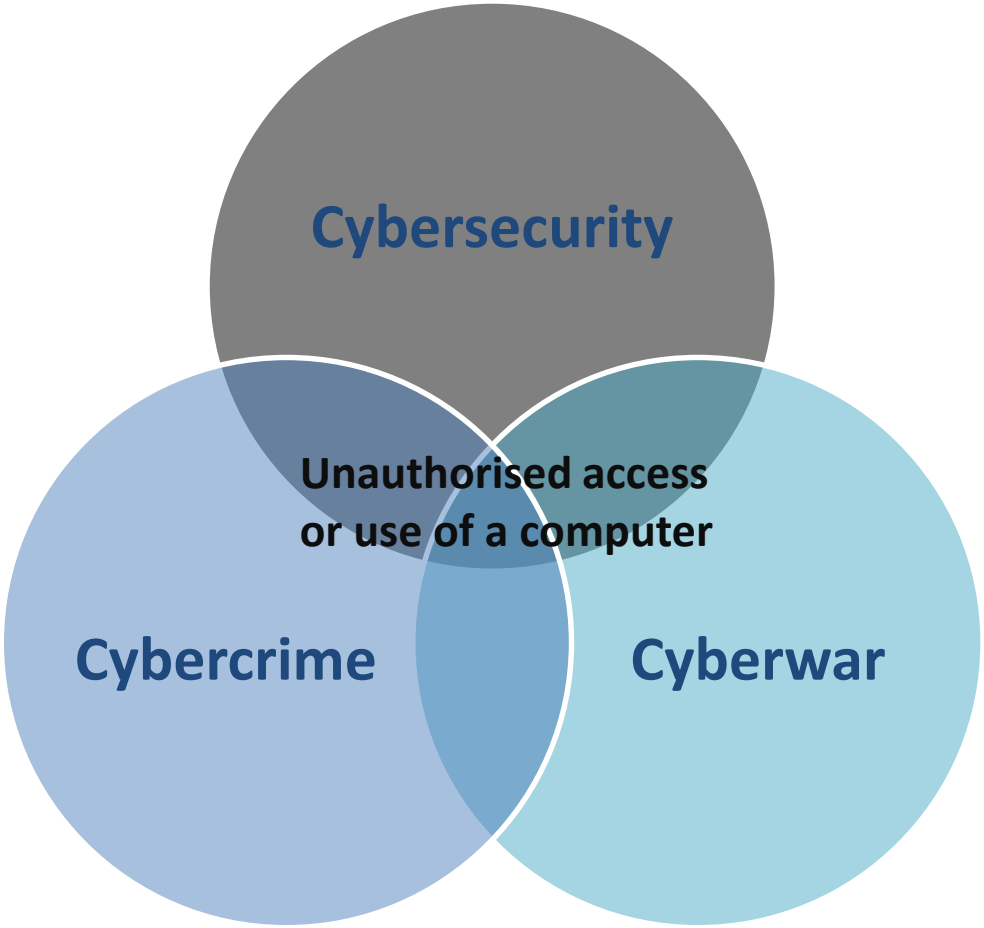

Cybersecurity
Cybercrime
Cyberwar

# Cyberwarfare

- Cyberwarfare involves actions taken to affect an adversary's information and information systems while defending one's own information, information systems and critical infrastructure.

- Cyberwarfare differs from cybersecurity in that the cyber-attacks are initiated through government infrastructure (by the state) or are state sponsored.

- The cyber-attacks must either be used in armed conflict or where there have been acts of use of force, or in the lead up to armed conflict and use of force.


Cybersecurity
Unauthorised access
or use of a computer
Cybercrime
Cyberwar

# Trends &Threats

- No single Australian department, organisation, corporation, university, or military division has the skill and resources available to combat many of the current threats that we will see today, and not the capability to counter future threats.

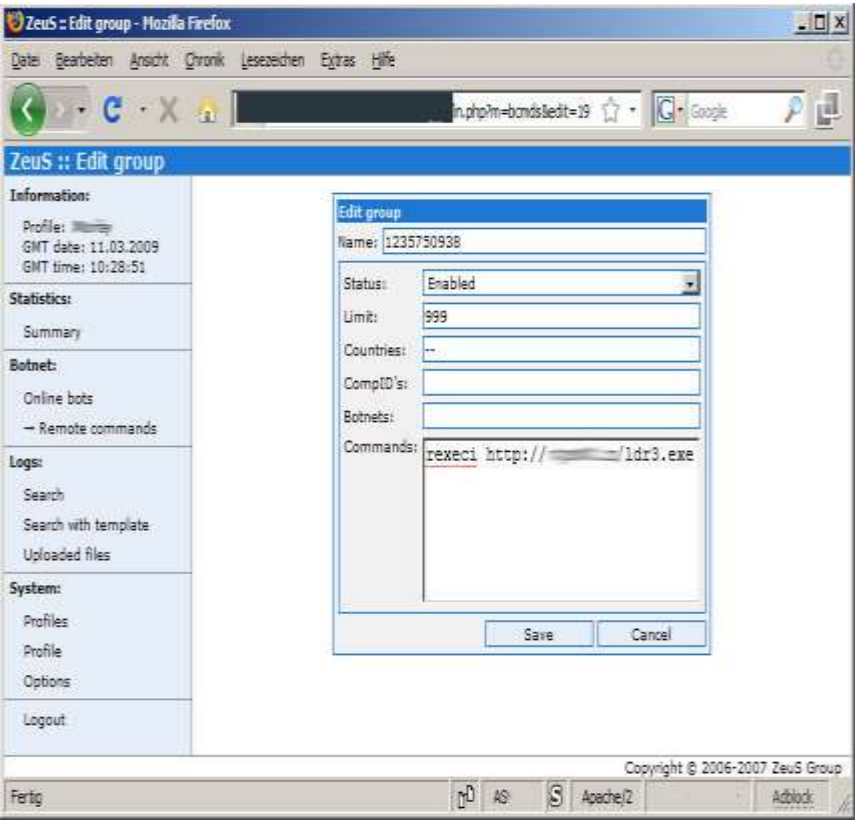
No network or technology is immune from attack.

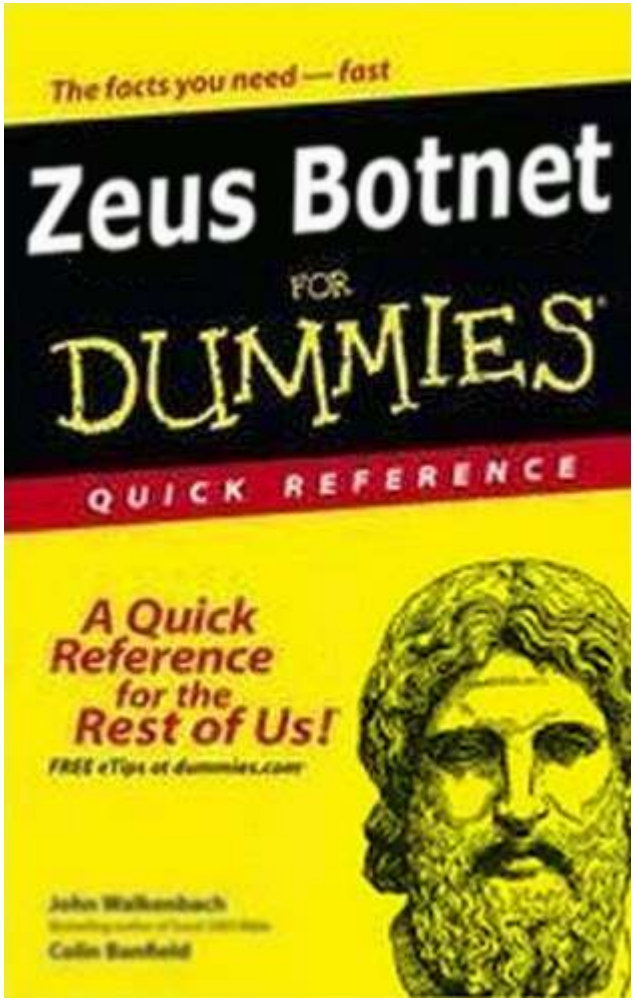
- Cyber-security reports around the globe have alleged high-scale state-sponsored espionage of government and corporate information.

# Even Luddites Can Participate

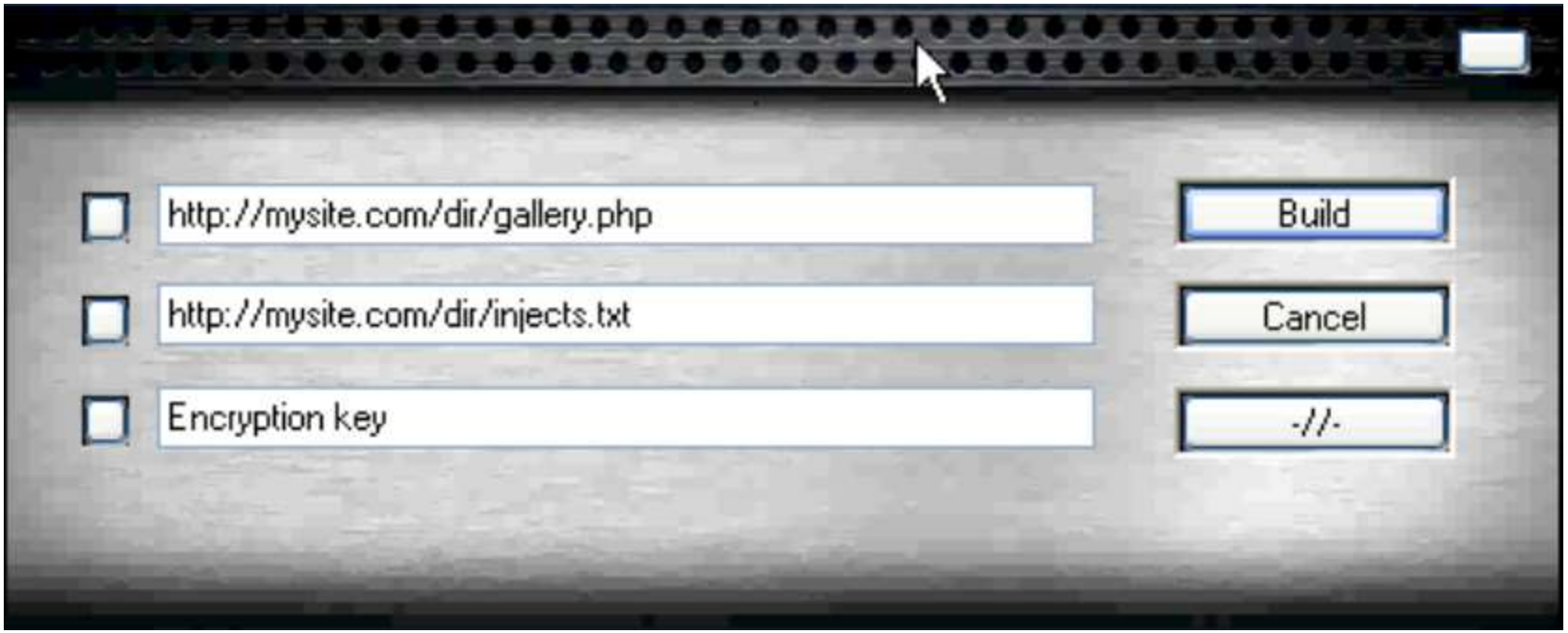
- Many forms of cyber-attack do not require sophisticated computer skills or high levels of start-up money.

# Zeus Crimeware Kit



# Weyland Utani for Macs



# Malware as a Service

**Try-before-you-buy offers for malware**

Трафик на сплоиты.

Для пробы всем Бесплатно 100 посетителей!!!

Цена

4 $ за 1000 посетителей - При заказе от 1000 до 5.000

3.8 $ за 1000 посетителей - При заказе от 5.000 до 10.000

3.5 $ за 1000 посетителей - При заказе от 10.000

Traffic for sploits

Free trial, 100 visitors!!!

Price

$4 per 1000 if buying 1000 – 5000

$3.80 per 1000 if buying 5000 – 10,000

$3.50 per 1000 if buying over 10,000

Courtesy of Peter Gutmann

# Botnets For Hire Directory

# Silk Road

*anonymous marketplace*

Welcome [redacted]

messages(0) | orders(0) | account($0.00) | settings | log out

search | (0)

Shop by category:

- Drugs(1819)
  - Benzos(176)
  - Cannabis(417)
  - Dissociatives(49)
  - Ecstasy(187)
  - Opioids(162)
  - Other(242)
  - Psychedelics(232)
  - Stimulants(216)
- Apparel(5)
- Books(188)
- Collectibles(2)
- Computer equipment(3)
- Digital goods(147)
- Drug paraphernalia(62)
- Electronics(9)
- Fireworks(2)
- Food(11)
- Forgeries(51)
- Home & Garden(1)
- Jewelry(1)
- Lab Supplies(9)
- Medical(13)
- Money(122)
- Packaging(1)
- Services(49)
- XXX(52)

Ibogaine HCL 2 grams

**$146.45**

Barcode Manipulation scam keeping...

**$0.59**

Metal Chamber Pipe

**$1.78**

HEROIN (AFGHAN) PURE STRAIGHT...

**$18.08**

_Grape Wreck_ *Premium*

**$3.04**

250mg 2C-E (4-ethyl-2,5-dimethoxyphenethyla

**$13.83**

Ephedrine Hcl 48mg - 100 Tablets

**$17.72**

--=== Party Time ===-- 2x 110mg...

**$3.14**

One Kilogram Crystal Methylone

**$435.22**

News:

- Who's your **favorite?**
- Acknowledging **Heroes**
- A new annonymous market **The Armory!**
- **State of the Road Address**

| | | | |
|---|---|---|---|
| **dave00** | **re: subject**<br><br>I would recommend ak47 or m4 , for sidearm mp5 or handguns like glock or beretta 92<br>The body armor will be NIJ IV level, it can stop also an ak47 rounds<br>This kind of material is easily to obtain especially for body armor | 5 days | read<br>**delete** |
| **triadische2** | **re: subject**<br><br>What would you recommend for a group of 20? I'd like sidearms, automatic rifles, and body armor if possible. Need something suitable for both jungle and urban combat. Would it be possible to see photos of the equipment you have available? | 7 days | read<br>**delete** |
| **dave00** | **re: subject**<br><br>yes for sure | 7 days | read<br>**delete** |
| **triadische2** | **re: subject**<br><br>Understood.<br><br>Do you think your wares would be capable of taking on a 3rd world government organization? Probably using out of date Soviet weaponry and older munitions. | 8 days | read<br>**delete** |
| **dave00** | **re: subject**<br><br>I don't want to talk about my sourcings<br>I have many but i won't speak about | 8 days | read<br>**delete** |

GIZMODO

# Darkweb

## Commercial Services

Buying and selling stuff, auction houses, sales forums, gaming.

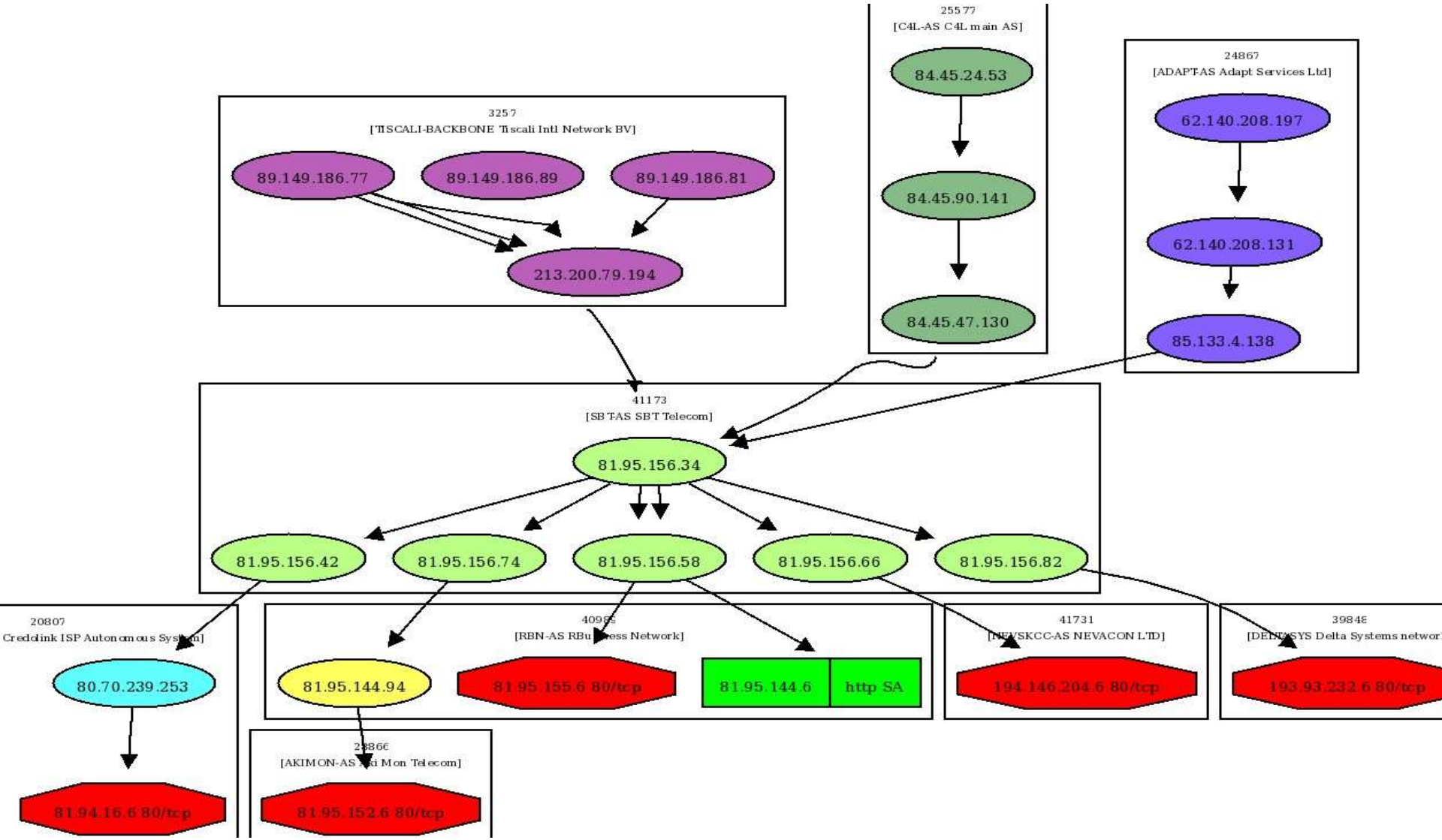
*See also: The separate Drugs and Erotica sections for those specific services.*

- Contract Killer - Kill your problem (snitch, paparazzo, rich husband, cop, judge, competition, etc). (Host: FH)
- BitPoker v1.93 - Poker (Bitcoin). (Host: FH)
- Buttery Bootlegging - Get any expensive item from major stores for a fraction of the price! (Host: FH)
- Stat ID's - Selling fake ID's.
- Bidcoin - Like Ebay. We increase the gross national product. (Host: FH)
- Video Poker - A casino that features "jacks or better" video poker. - DOWN 2011-08-07
- Cheap SWATTING Service - Calls in raids as pranks. (Host: FH)
- Data-Bay - Buy and sell files using digital currency.
- The Last Box - Assassination Market (Bitcoin). - DOWN 2011-08-07
- Pirax Web DDoS - Take out your enemies in seconds. (Host: FH)
- Hacking Services - Hacks IM and Social Nets, does DDoS, sells bank/credit/paypal accounts. Se Habla Espanol. (Host:
- Email Hacker - Hacks emails (Bitcoin). (Host: FH)
- CC4ALL - Selling valid Credit-Cards. Most from Germany. (Host: FH)
- Slash'EM online - Super Lots'A Stuff Hack-Extended Magic tournament server (Bitcoin).
- Rent-a-Hacker - Pay a professional hacker to solve your problem, destroy your enemys. (Host: FH)
- BitPoker v2.0 - New version of poker (Bitcoin). (Host: FH)
- BacKopy - Sells game, software and movie discs (Bitcoin). (Neglected status note) - Broken 2011-08-07
- The Pirates Cove - Classifieds. (Host: FH)
- BitLotto - A lottery using Bitcoin. (Host: FH)
- Brimstone Entertainment - Escort Ads, Strippers, Adult Entertainers. (Host: FH)
- Red Dog Gaming - Play black jack, red dog poker and more (Bitcoin).
- CouponaTOR - A service for getting retail coupons created (Bitcoin). (Host: FH)
- Virtual Thingies - Buy virtual goodies like premium accounts, usenet access or domains (Bitcoin). (Host: FH)

- Organised criminal networks and terrorist networks are involved in cybercrime, cybersecurity AND cyberwarfare.

# Internet Service Provider Headquartered St. Petersburg (Pre-2004)

# RBN – Bullet Proof Hosting up to 2004

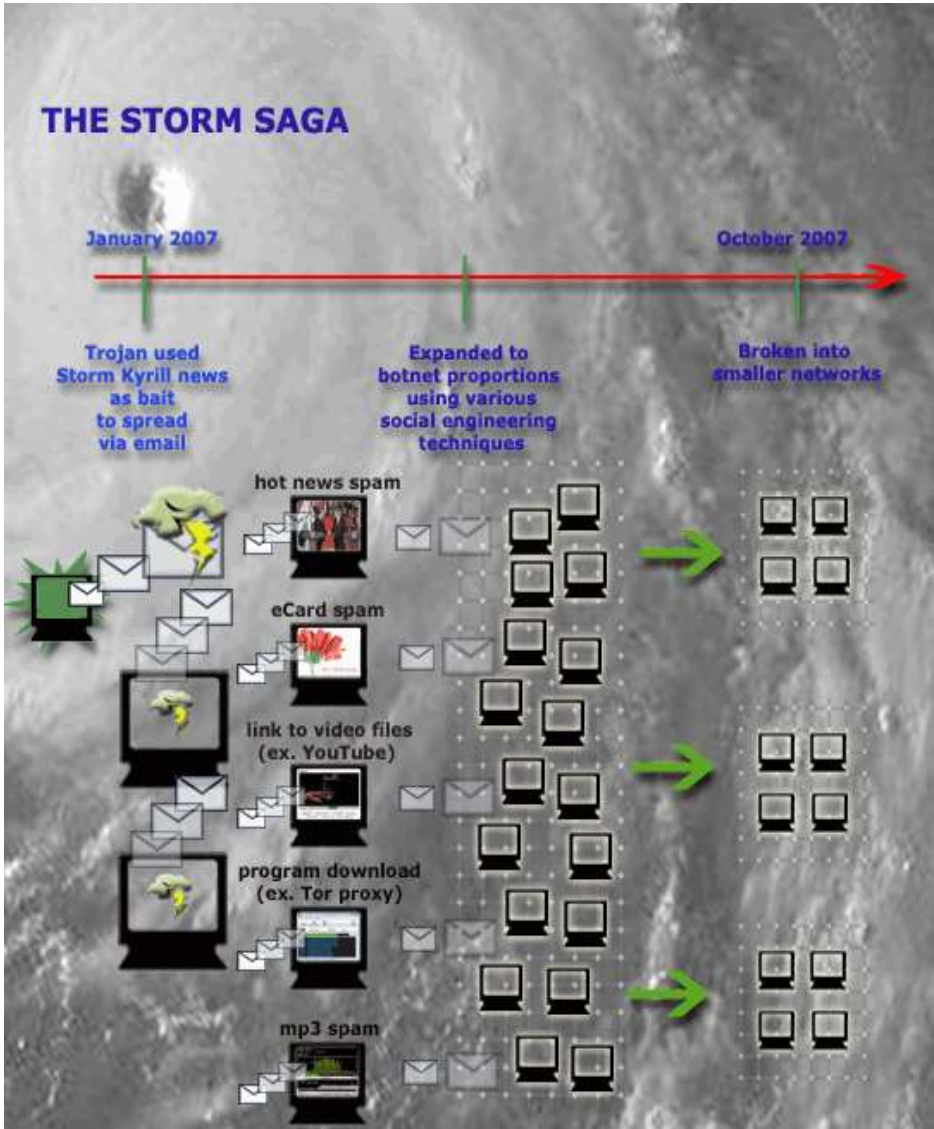


# Innovation Begins

- Purchase large block of IP addresses in multiple countries
- China, Panama, the UK, Bahamas, Taiwan, Turkey, Malaysia, Latvia, Estonia, Singapore, Japan, Korea and NOW in Iran

# Technical Innovation

- ☐ Fast-flux Botnet
- ☐ Onioning (deniable encryption)
- ☐ double fast-flux botnet (Command and Control in Peer to Peer Channel)
- ☐ Use of Dynamic DNS for IP addresses
- ☐ Denial of Service anyone who gets in your way

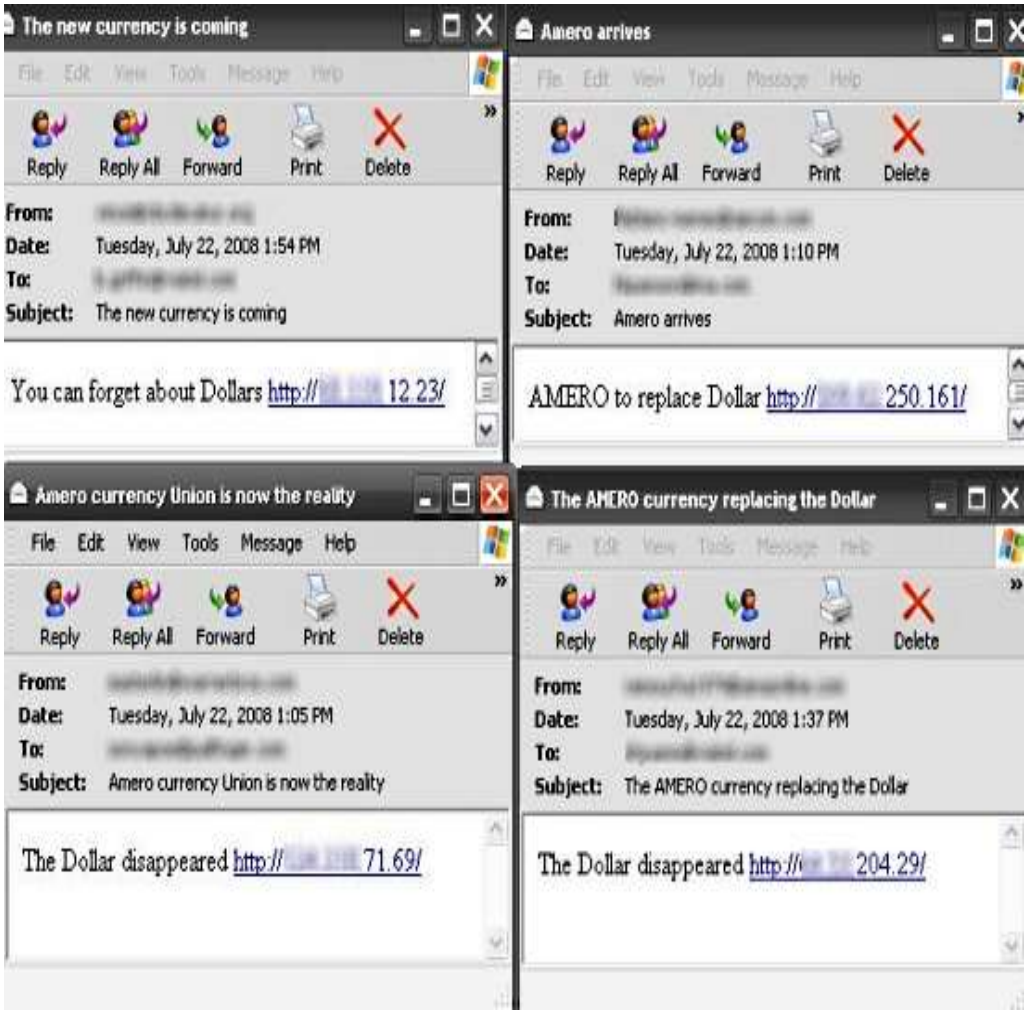


# Iframe Cash, Stepan Kuchernko and Russian Business Network

## ROCK PHISH

**(2006, 36 banks, $200 million lost in 3 days)**

## STORM WORM



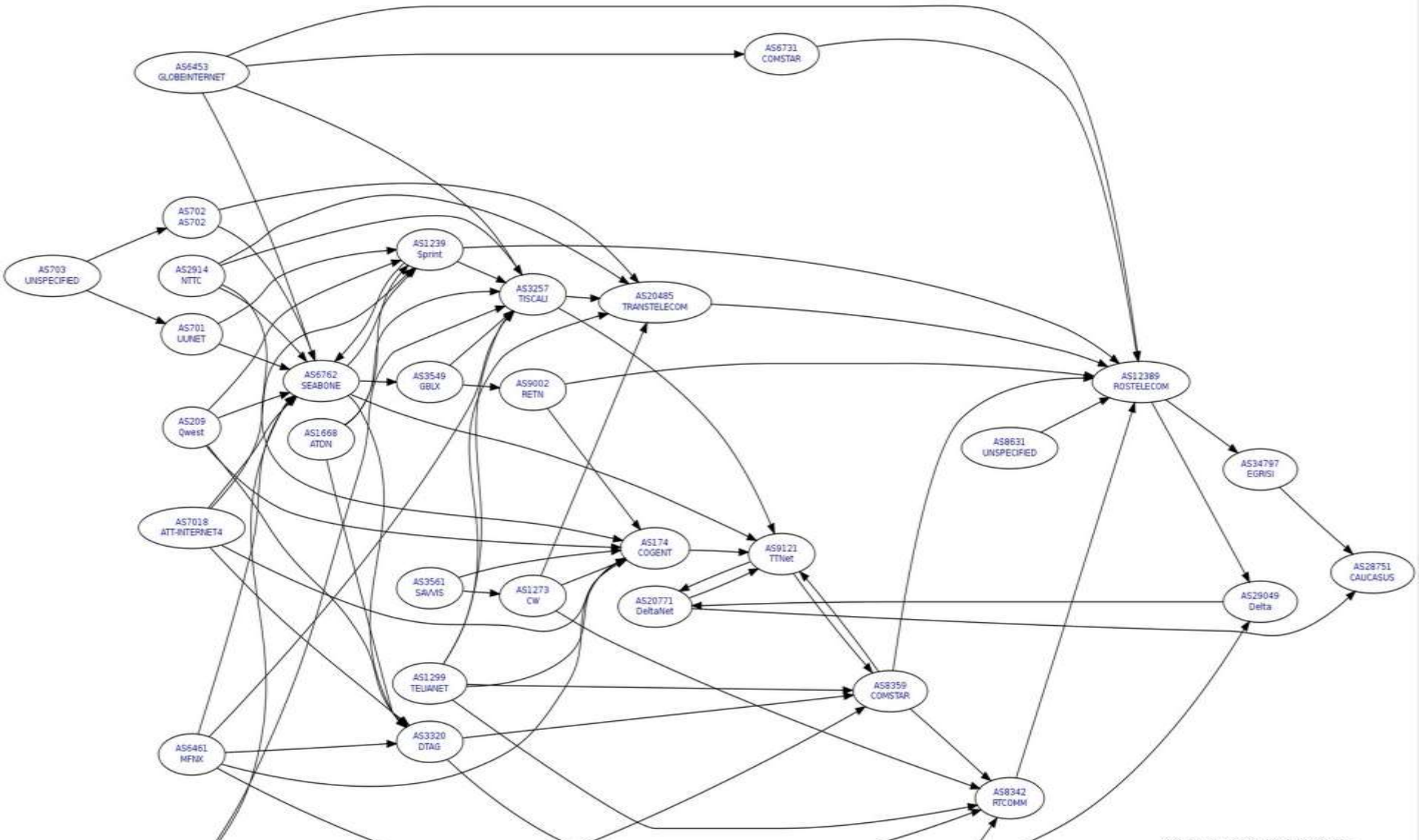
# STORM Botnet

- Encrypted Executable Code
- Undetected by anti-virus products
- Embedded in a Rootkit
- Distributed by a Double FastFlux Botnet = P2P system
- Botnet Herder linked to Eastern European Organized Crime

# Georgian Attacks

August 7, 2008 messages released to wider Russian hacker community

# Cyber Warfare on Georgia



**Äðóçüÿ ïðîåêòà**

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

**Ëèíêè íà ðåñóðñû**

**Èíôî**

Ìû - ïðåäñòàâèòåëè ðóññêîãî ðàé-àíäàðòàóíàà, íà ïîðòàëå ïîñâÿùåííîì ñîáûòèÿì â ñâÿçè ñ ñòîëêíîâåíèåì â Þæíîé Îñåòèè. Ìû õîòèì æèòü â ñâîáîäíîì ìèðå è ñòóäåíòàìè â ñâîáîäíîì îò àãðåññèè ëæè Ñàêàøâèëè ïðîñòðàíñòâå. Ìû íå óâåäîìëÿì â óêàçàíèÿõ íî ñòîðîíû äëåñòå èëè èíûõ ëèö, à äåéñòâóåì ñîãëàñíî ñâîèì óáåæäåíèÿì, ïîñòàíîâèâ íà ïàóçó ïîâñåäíåâíûå äåëà è âàøè â ñèëó ñïîâåäëèâîñòè. Âû ïîæåòå íàçâàòü íàñ ïðîñòóïíûìè è êèáåð-òåððîðèñòàìè, ðàçâÿçûâàÿ ïðè ýòîì âîéíó è óáèâàÿ ëþäåé. Íî ìû áóäåì áîðîòüñÿ è íàäîñòüì àãðåññèè â ïîïûòêè Ðîññèè â Ñàêàøâèëè ïðîòèâîñòîÿ.

Ìû òðåáóåì ïðåêðàùåíèÿ àòàê íà èíôðàñòðóêòóðó è ïðàâèòåëüñòâåííûå ðåñóðñû Ðóñòàâè, à òàê æå îáåùàåì ñâîþ ñîçíàòåëüíóþ ïîääåðæêó ïî ïðîòèâîäåéñòâèþ ïîëèòèêå ïîäêóïîâ è ïðîâîêàöèé ñïåöñëóæá. Äî òåõ ïîð, ïîêà ñèòóàöèÿ íå èçìåíèòñÿ, ìû áóäåì ïðåïÿòñòâîâàòü ðàñïðîñòðàíåíèþ ëîæíîé èíôîðìàöèè íà çàïàäíûõ è ãðóçèíñêèõ èíòåðíåò-ñàéòàõ. Íà ìû ðàçâÿçàëè èíôîðìàöèîííóþ âîéíó, íà íàì ïðåä÷èòü çà âñ ïîñëåäñòâèÿ.

Ìû ïðèçûâàåì ê ïîëíîé âñåð, êîíó íà áåçóâçëè÷íà ëîæü ïîëèò÷åñêèõ ñàéòîâ, âñåð, êòî èìåò âîçìîæíîñòü ïðåïÿòñòâîâàòü ðàñïðîñòðàíåíèþ +âðîé èíôîðìàöèè.

StopGeorgia.ru

**ÂÍÈÌÀÍÈÅ! ÍÀÌÀÒÅÉÉ ÄÀÒÀ-ÖÅÍÒÐ "NETDIREKT" - WWW.NETDIREKT.DE ÏÒÊÀÇÀË Â ÓÏÑÒÈÍÀÀ ÇÀÐÅÀËÓ ÏÐÎÅÊÒÀ! ÇÀÐÅÀÉÑÜ WWW.STOPGEORGIA.INFO ÍÀ ÄÀÍÍÛÉ ÌÎÌÅÍÒ ÍÀ ÑÓÙÅÑÒÂÓÞ!**

**Â ÏÒ×Ü ÍÀ 14 ÀÂÃÓÑÒÀ ÍÀØ ÀÊÊÀÓÍÒ ÍÀ ÑÅÐÂÅÐÅ Â ÑØÀ ÁÛË ÇÀÁËÎÊÈÐÎÂÀÍ, Â ÄÑß ÈÍÔÐÀÑÒÐÓÊ-ÓÄÀËÅÍÀ. ÊÐÏÀ ÒÎÃÎ, ÏÐÎÅÊÒ STOPGEORGIA.RU ÏÐÅÄÐÅÑß ÌÅÑÑÈÐÎÂÀÍÍÎÉ ÊÐÈÒÈÊÅ ÑÎ ÑÒÎÐÎÍÛ ÇÀÏÀÄÍÛÕ ÑÌÈ.**

**ÍÀ ÄÀÍÍÛÉ ÌÎÌÅÍÒ ÏÐÎÅÊÒ STOPGEORGIA.RU ÏÐÈÑÒÓÏÀÅÒ È ÏÐÎÄÎËÆÀÅÒ ÓÍÈ×ÒÎÆÅÍÈÅ ÍÀÑ ÍÅÏÐÈßÒÍÛ ÍÀÒÈÑÒÎ ÃÐÓÇÈÈ È ÇÀÏÀÄÀ!**

# Denial of Service Attacks

Georgian banks, telecommunication corporations, government websites, non-state sponsored Russian newspapers, political opposition (Eg. www.kasparov.ru)

All attacked in a coordinated fashion in the middle of the night August 8, 2008

# Attacks in RBN Format

- ICMP traffic, not tcp
- Attacks generated from known RBN registrants (Eg. Incasher.net)
- Attacks traced to ‘Abdullah Operation’ on Turkish ISPs with known registered domain names from Ukraine (WHOIS directory)

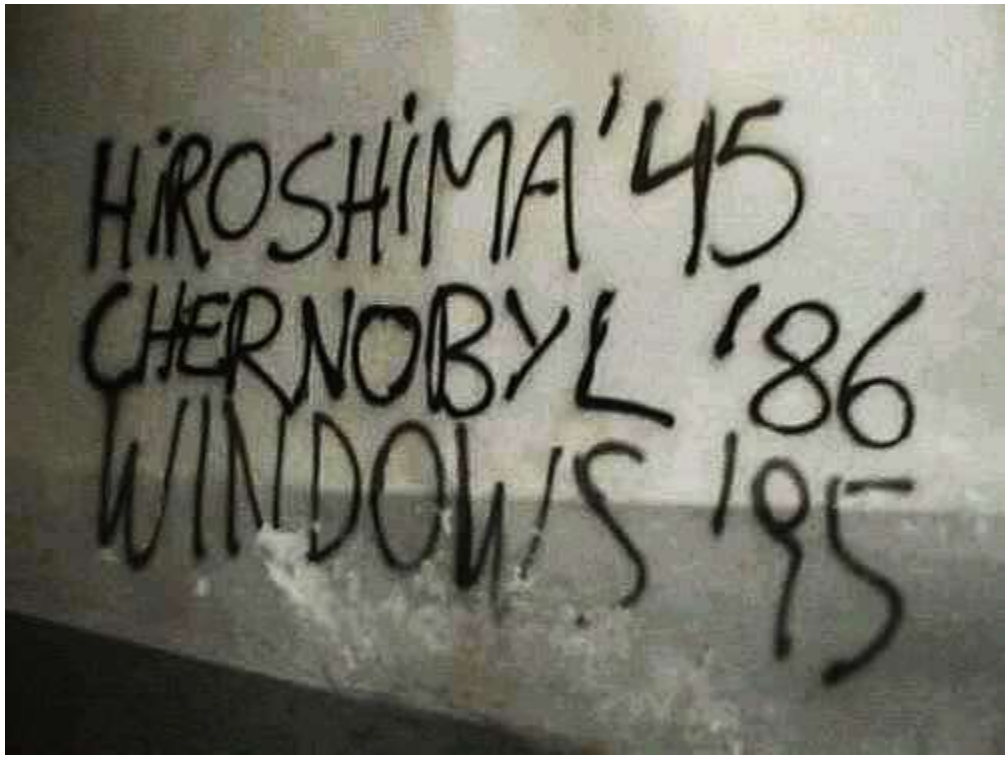
# Russia Bombs Georgia

Bombs are dropped hours after cyber-attacks.

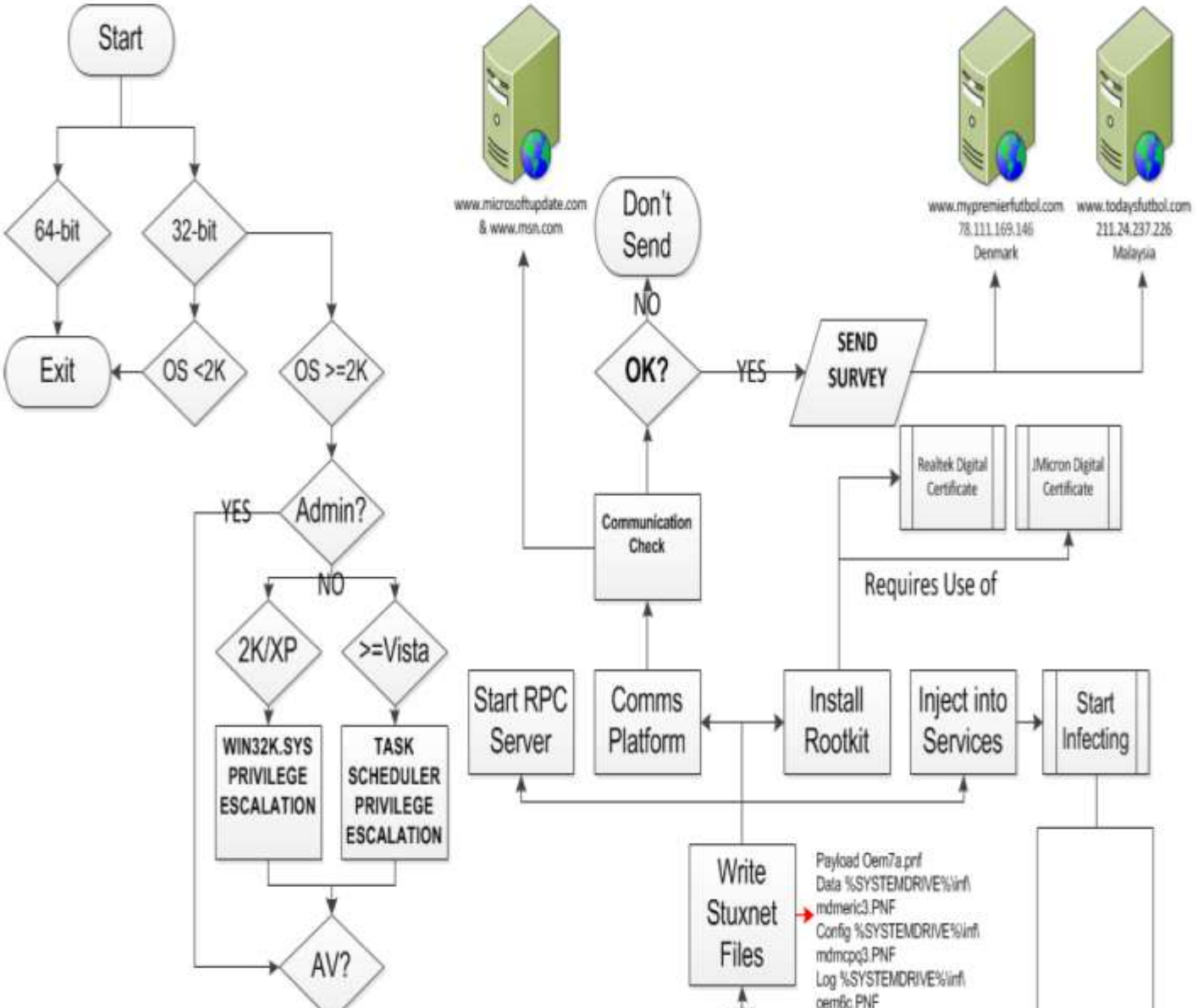
# Media is slow to pick up coverage of events

- To the outside world, all attacked Georgian websites appear to be functioning
- As they stood on August 7
- DNS resolvers are not working - have been subverted!

# Connected to Critical Infrastructure



Firefox whitepaper.pdf (application/pdf Object)
www.vulnerabilityassessment.co.uk/education/whitepaper.pdf
storm botnet stuxnet code
Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media Windows
Bookmarks



# Cyberwar is becoming a real threat

# Duqu

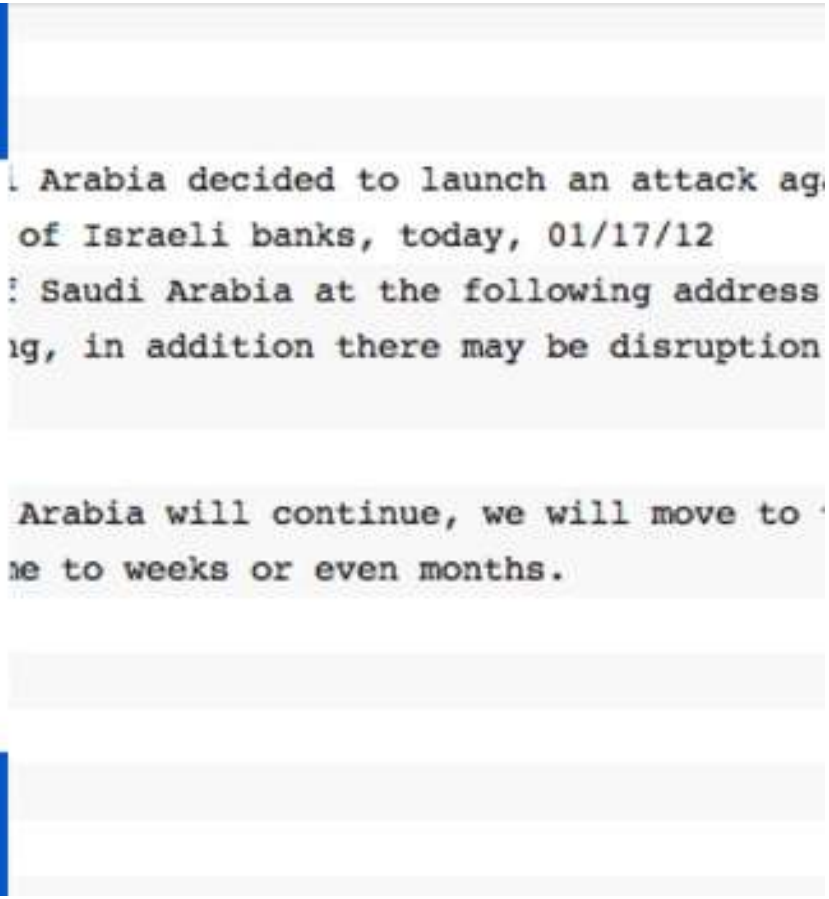
# Flame

FLAME PROPS_
lame_props = {}
flame_props FLAME_ID_C
flame_props FLAME_TIME_
flame_props FLAME_LOG_PE
flame_props FLAME_VERSION_
flame_props SUCCESSFUL_IN
flame_props INTERNET_CHEC
flame_props BPS_CONFIG =
flame_props BPS_KEY = "B
flame_props PROXY_SERVE
lame_props getFlameId
config.hasKey(f

# Gauss

**A portrait of Carl Friedrich Gauss by Gottlieb Biermann (1824-1908).** Photo: A. Wittman

# Political and religious based hacking on the rise



# “Cutting Sword of Justice”

# All Saudi Arabian Ministry of Defense websites hacked by Syrian Electronic Army

PAKISTAN HAXORS
CREW

# China Philippines

## Spratley Islands and Scarborough Shoals

"Threatening world peace with ICBMs and Nuclear weapons/Wasting money while his people starve to death."

# Stealth

Your average espionage attack lasts for 458 days until the organisation discovers it has been attacked.

Many of these attacks are the cyber equivalent of advance persistent attacks.

# Over-cover  Intelligence

- Professional security experts gravitating to lucrative over-cover intelligence of exploits trade
- Governments, businesses and organisations purchasing vulnerability and exploit information but turning a blindeye to how it is obtained

# Dangers

- Difficulty in traceback to the true source of an attack.

# Should this be part of the cybersecurity agenda?

# twitter data logs as surveillance

# Aaron Schwartz

Twitter / wikileaks: Was Aaron Swartz targeted as ... - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Twitter / wikileaks: Was Aaron Swartz target...

Twitter, Inc. (US) https://twitter.com/wikileaks/status/295346723587497984

Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media Windows

Search

**WikiLeaks**
@wikileaks

Was Aaron Swartz targeted as part
boston crackdown against #WikiLea
CCTVCambridge cctvcambridge.org
/SwartzCambridg... #aaronswartz

Reply Retweet Favorite More

109 RETWEETS 32 FAVORITES

5:45 PM - Jan 26, 2013

**Cowboys Fan 2012** @JustOrchids1
@wikileaks i dont believe for a second that aa
swartz committed suicide & someone needs 2
out who did it
Details

**Professor Jerry** @ProfessorJerry
@wikileaks our nation have been infiltrated fro
within,our freedoms and constitution is being s
compromised by pres obama & his ?

Twitter / wikileaks: CRS Report (31 Jan 2013): ... - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Twitter / wikileaks: CRS Report (31 Jan 2013...

Twitter, Inc. (US) https://twitter.com/wikileaks/status/302077278966394881

Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media Windows

Search

**WikiLeaks**
@wikileaks

CRS Report (31 Jan 2013): Criminal Prohibitions on the Publication of C Defense Information (PDF) bit.ly/X #wikileaks

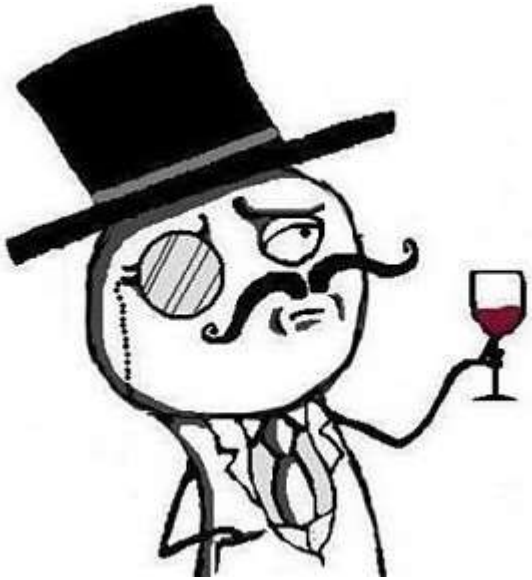
Reply Retweet Favorite More

29 RETWEETS 4 FAVORITES

7:30 AM - Feb 14, 2013

**Rixstep News** @rixstepnews
@wikileaks Why won't GOP start impeachmen proceedings against Obama?
Details

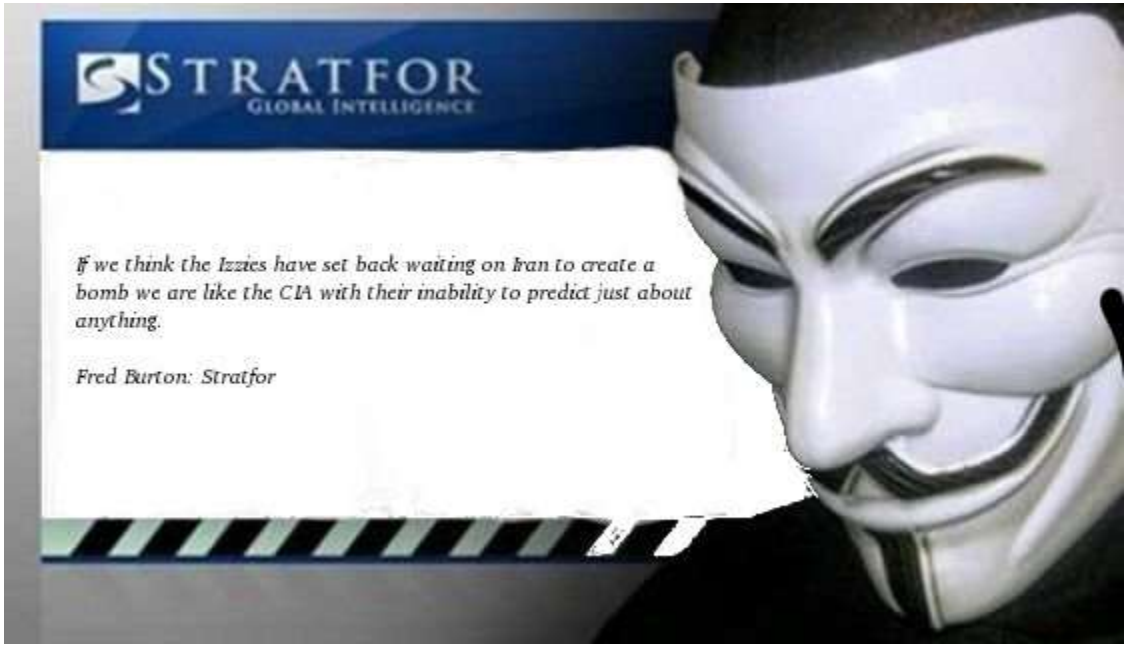
**AGITATE THE STATE** @digitalfolklore
@wikileaks fix the url on the main page...the fu needs to be edited..or add -> net
Details



MasterCard

PayPal®

# Stratfor, US State Governement and Investment Firm George K. Baum and Company



# Crimes or Protests

| OFFLINE | ONLINE |
| --- | --- |
| Sit-ins | Virtual Sit-ins |
| Barricades | Denial of Service Attacks & Website Redirection |
| Political Graffiti | Website Defacements |
| Wildcat Strikes | Denial of Service Attacks & Website Redirection |
| Underground Presses | Site Parodies, Blogs, Facebook Protest |
| Petitions | Web-Petitions (Eg. Facebook Likes) |

# Responses

# Governments Cybersecurity Strategies

*National Security Strategy (UK)
*Canada's Cyber Security Strategy
*Conceptual Views Regarding the Activities of Armed Forces of the Russian Federation in Information Space

*The UK Cyber Security Strategy: Protecting and Promoting the UK in a
*Digitized World
US Strategy for Operating in Cyberspace

*Strong and Secure: A Strategy for Australian National Security
*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
*US Cybersecurity Executive Order

# What does cyber diplomacy look like?

And cyberpeace?

# Has security through obscurity been replaced by security of absurdity?