Armageddon Redux

The changing face of the Infocalypse

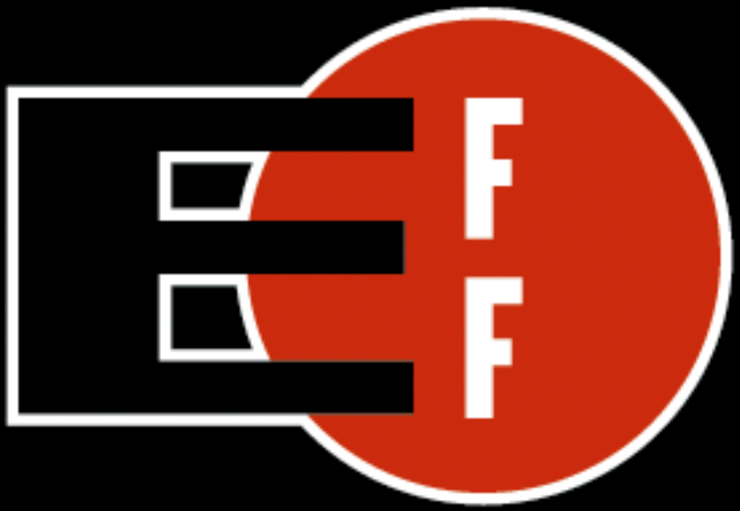
DISCLAIMER

- The views expressed in this talk are my own and not approved by or representative of my employer or this conference.

WHOIS @headhntr

- http://twitter.com/headhntr
- Incident Responder

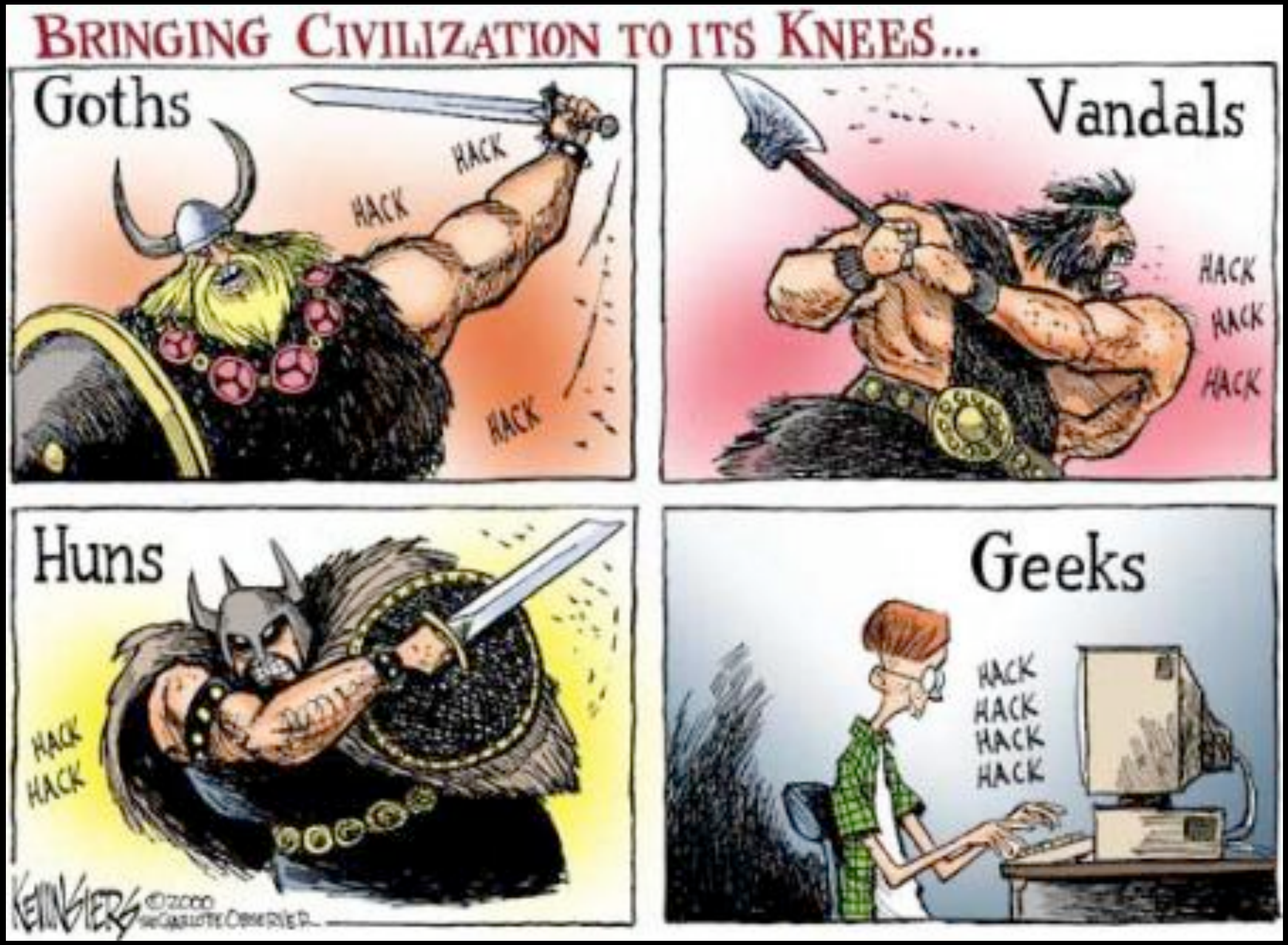
EFF / Hackerspaces



DeepSec

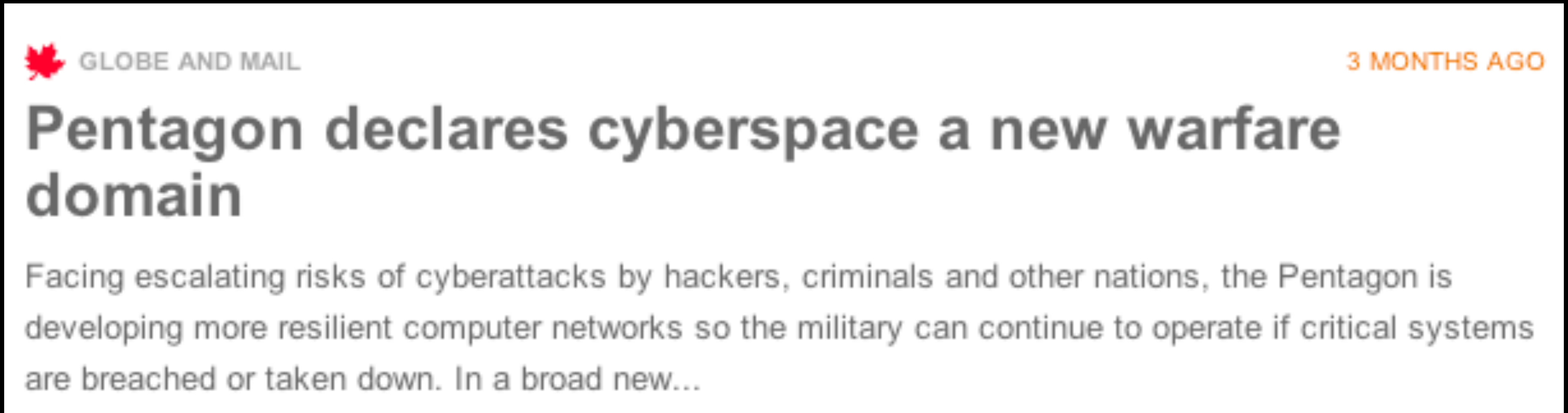
headhntr

Blended Threats


BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS ©2000 THE CHARLOTTE OBSERVER

Want 2 Cyber?

Cyber is the new air



GLOBE AND MAIL

3 MONTHS AGO

Pentagon declares cyberspace a new warfare domain

Facing escalating risks of cyberattacks by hackers, criminals and other nations, the Pentagon is developing more resilient computer networks so the military can continue to operate if critical systems are breached or taken down. In a broad new...

Blackhat 2010

“Describing the Internet as the "fifth military domain" with air, land, sea and space being the other four, Hayden said that cyberspace was the first man-made location for warfare.”

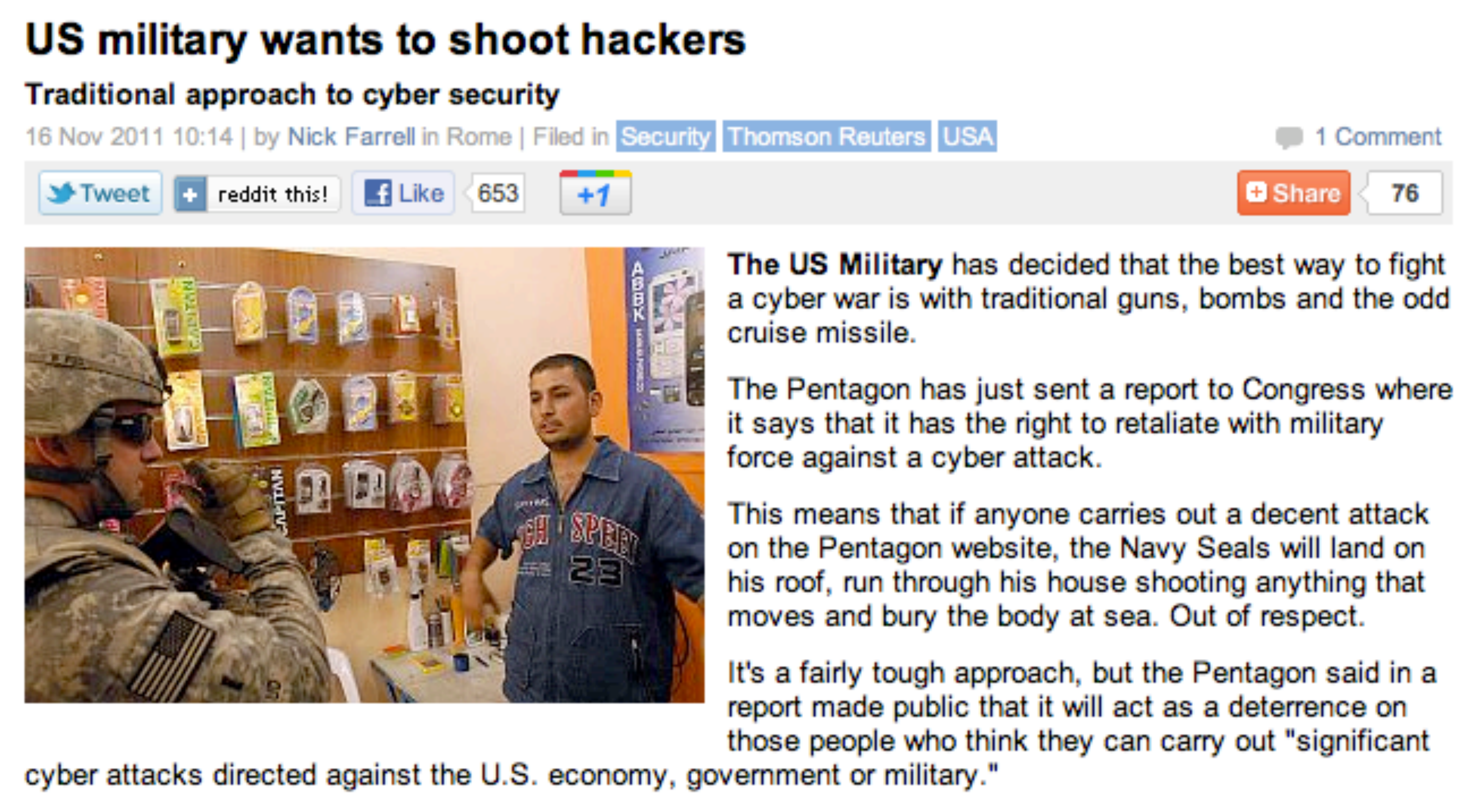
Retired General Michael Hayden, former head of the CIA and NSA.

"Cyberspace is real. And so are the risks that come with it. From now on, our digital infrastructure, the networks and computers we depend on every day, will be treated as they should be, as a strategic national asset."

Barack Obama,
President USA

The 5th Dimension of War

Innovations in technology are changing the tactics of modern-day conflict. There are new tools in today's arsenal of weapons. Helped by advances in electro-magnetics and modern information and communications technology, a new form of electronic warfare has been created. It is called cyberwar and is increasingly recognised by governments and the military as posing a potentially grave threat.



US military wants to shoot hackers

Traditional approach to cyber security

16 Nov 2011 10:14 | by Nick Farrell in Rome | Filed in Security Thomson Reuters USA

1 Comment

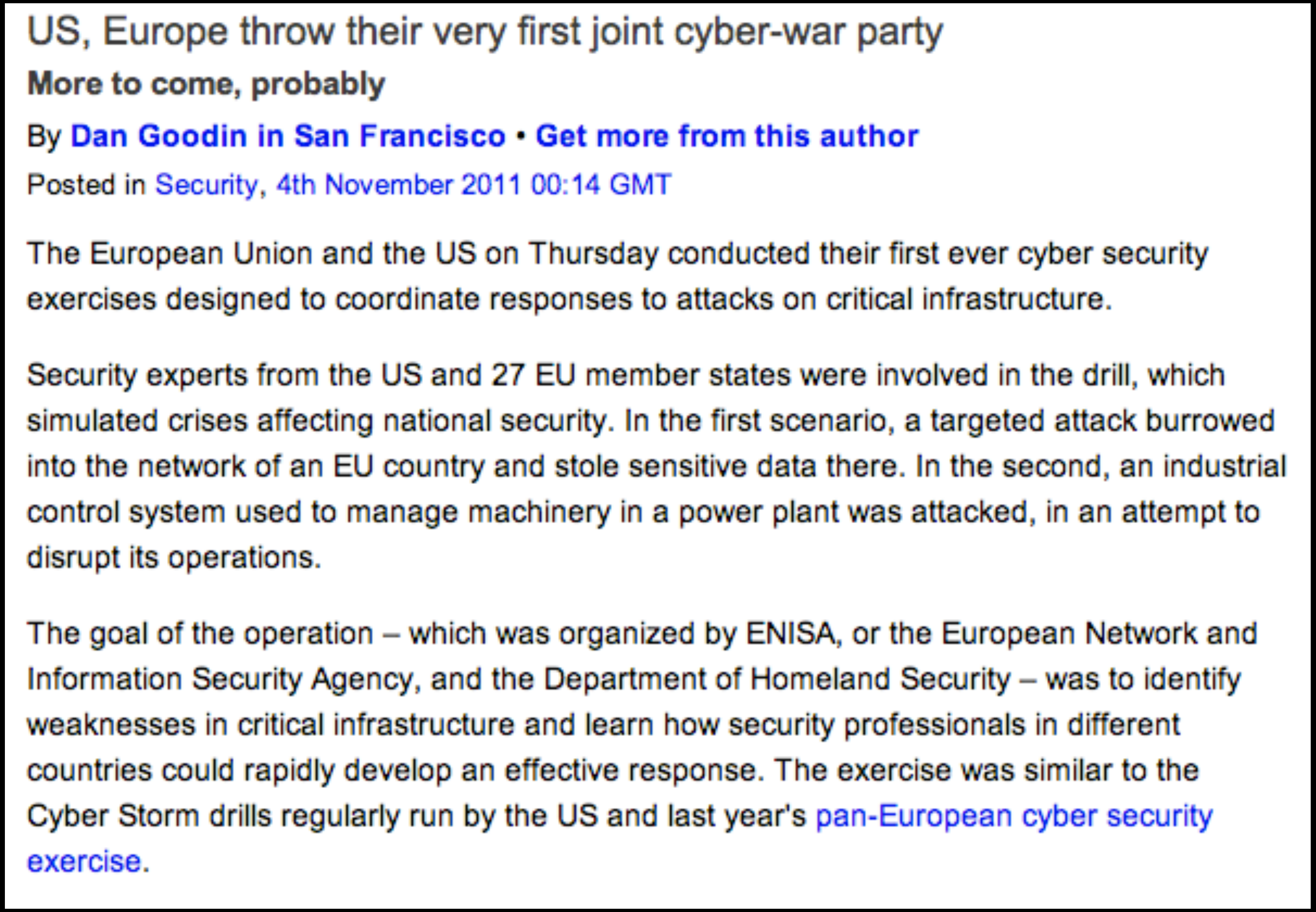
The US Military has decided that the best way to fight a cyber war is with traditional guns, bombs and the odd cruise missile.

The Pentagon has just sent a report to Congress where it says that it has the right to retaliate with military force against a cyber attack.

This means that if anyone carries out a decent attack on the Pentagon website, the Navy Seals will land on his roof, run through his house shooting anything that moves and bury the body at sea. Out of respect.

It's a fairly tough approach, but the Pentagon said in a report made public that it will act as a deterrence on those people who think they can carry out "significant cyber attacks directed against the U.S. economy, government or military."

headhntr



US, Europe throw their very first joint cyber-war party

More to come, probably

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 4th November 2011 00:14 GMT

The European Union and the US on Thursday conducted their first ever cyber security exercises designed to coordinate responses to attacks on critical infrastructure.

Security experts from the US and 27 EU member states were involved in the drill, which simulated crises affecting national security. In the first scenario, a targeted attack burrowed into the network of an EU country and stole sensitive data there. In the second, an industrial control system used to manage machinery in a power plant was attacked, in an attempt to disrupt its operations.

The goal of the operation – which was organized by ENISA, or the European Network and Information Security Agency, and the Department of Homeland Security – was to identify weaknesses in critical infrastructure and learn how security professionals in different countries could rapidly develop an effective response. The exercise was similar to the Cyber Storm drills regularly run by the US and last year's pan-European cyber security exercise.

"...actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

Richard Clarke
US National Security Council

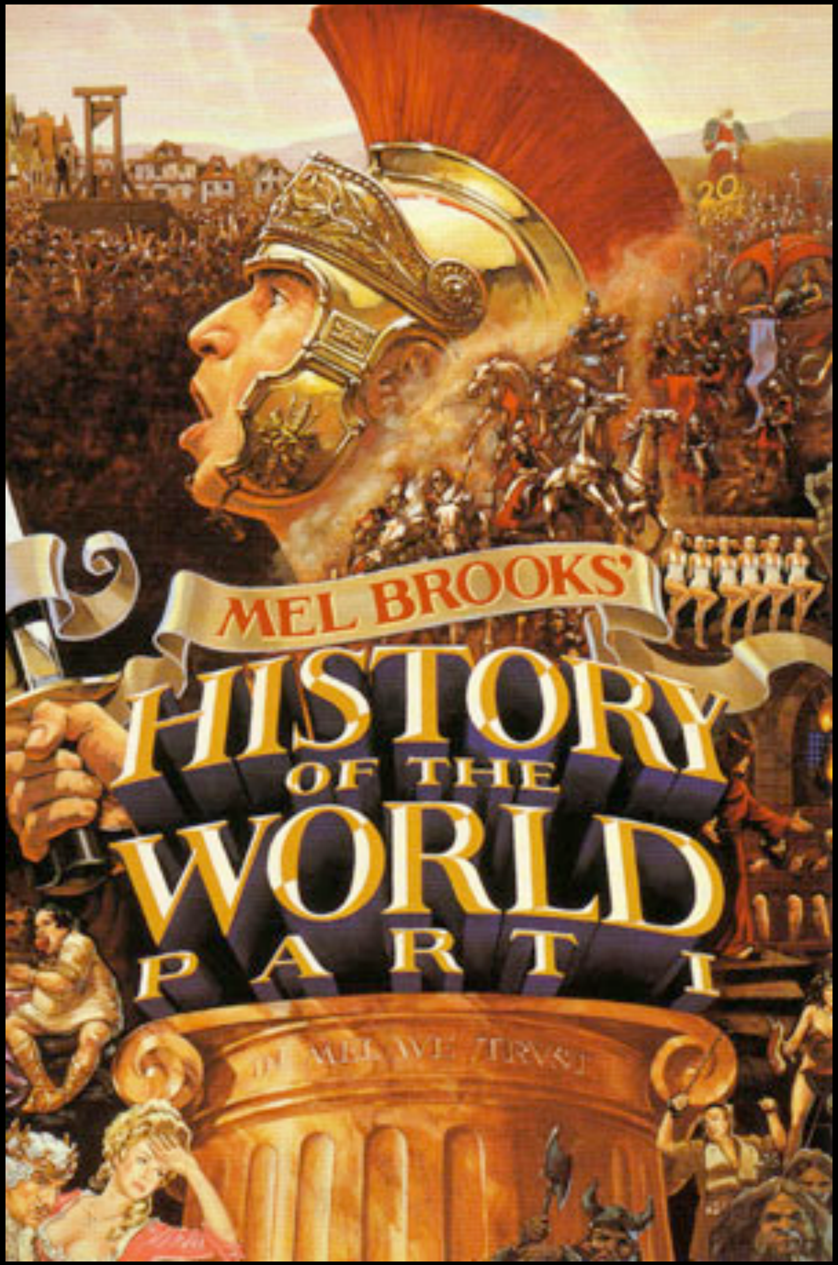
Cyberwar/Cyber-terrorism

- Politically motivated hacking
- Sabotage
- Espionage

Memory Lane

- DDoS to APT

- Buzzword Bingo



‘Cyberwar’ Lore

- April-May 2007: Estonian DDoS
- June-July 2008: Lithuania .gov web defacements.
- August 2008: Georgian web site intrusions

‘Cyberwar’ Lore

- 2007 - Syria: Operation Orchard
- 2010 - Iranian Cyber Army
- 2010 - Indian defacements
- 2010 - Stuxnet

Stuxnet

headhntr

Stuxnet

```
.... 0x81C47C00:lsass.exe 1928 668 4 65 2011-06-03 04:26:55
.... 0x81E18B28:svchost.exe 1080 668 5 80 2010-10-29 17:08:55
.... 0x8205ADA0:alg.exe 188 668 6 107 2010-10-29 17:09:09
.... 0x823315D8:vmacthlp.exe 844 668 1 25 2010-10-29 17:08:55
.... 0x81E0EDA0:jqs.exe 1580 668 5 148 2010-10-29 17:09:05
.... 0x81C498C8:lsass.exe 868 668 2 23 2011-06-03 04:26:55
.... 0x82279998:imapi.exe 756 668 4 116 2010-10-29 17:11:54
... 0x81E70020:lsass.exe 680 624 19 342 2010-10-29 17:08:54
```

```
Pid: 680 Priority: 9
Pid: 868 Priority: 8
Pid: 1928 Priority: 8
```

Stuxnet

```
!This program cannot be run in DOS mode.
Rich
.verif
.text
.bin
.reloc
ZwMapViewOfSection
ZwCreateSection
ZwOpenFile
ZwClose
ZwQueryAttributesFile
ZwQuerySection
TerminateProcess
GetCurrentProcess
CloseHandle
WaitForSingleObject
OpenProcess
```

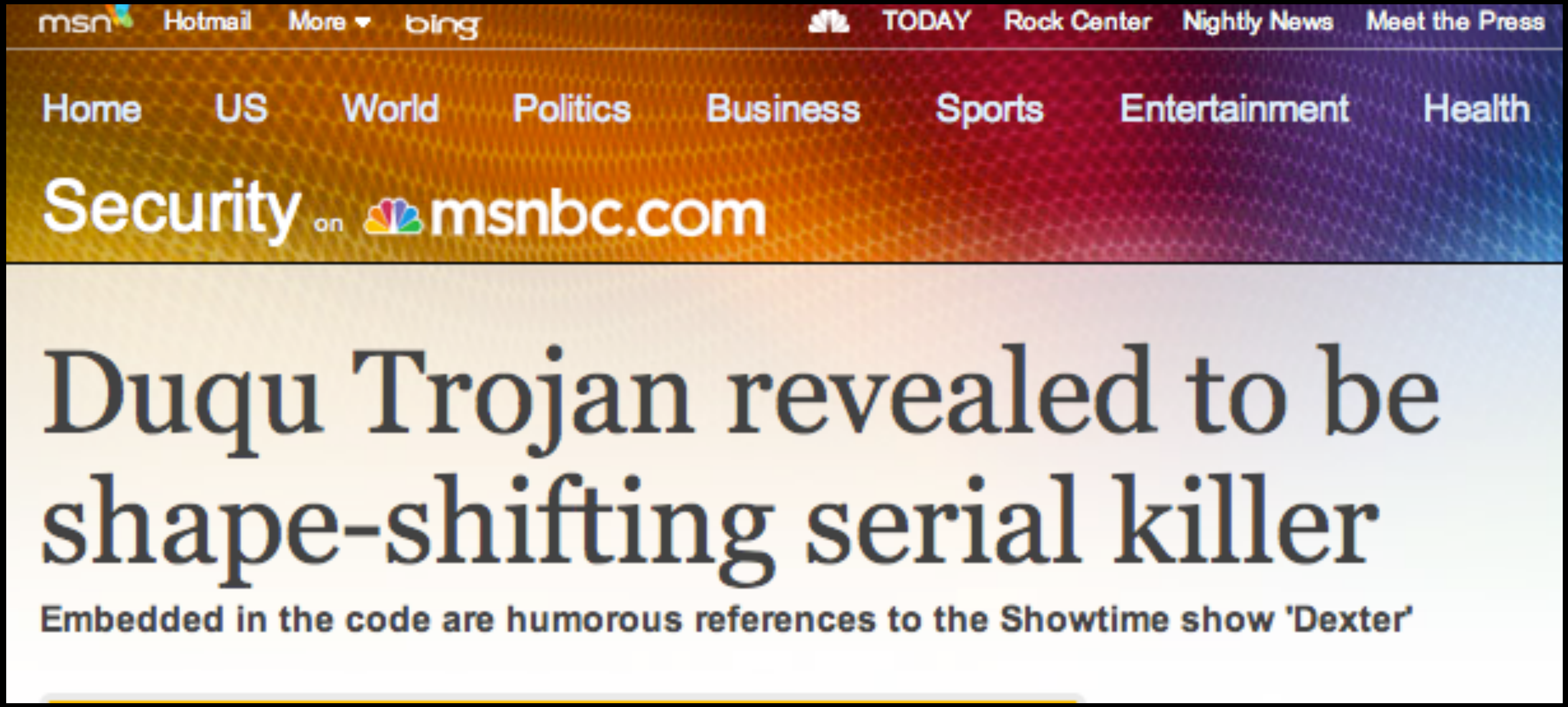
Duqu

“Duqu Worm Causing Collateral Damage in a Silent Cyber-War” - eWeek

“Cyberwar becoming a reality?” - Techweek

“Cyberwarfare: What Goes Around Comes Around” - Eurasia Review

Duqu

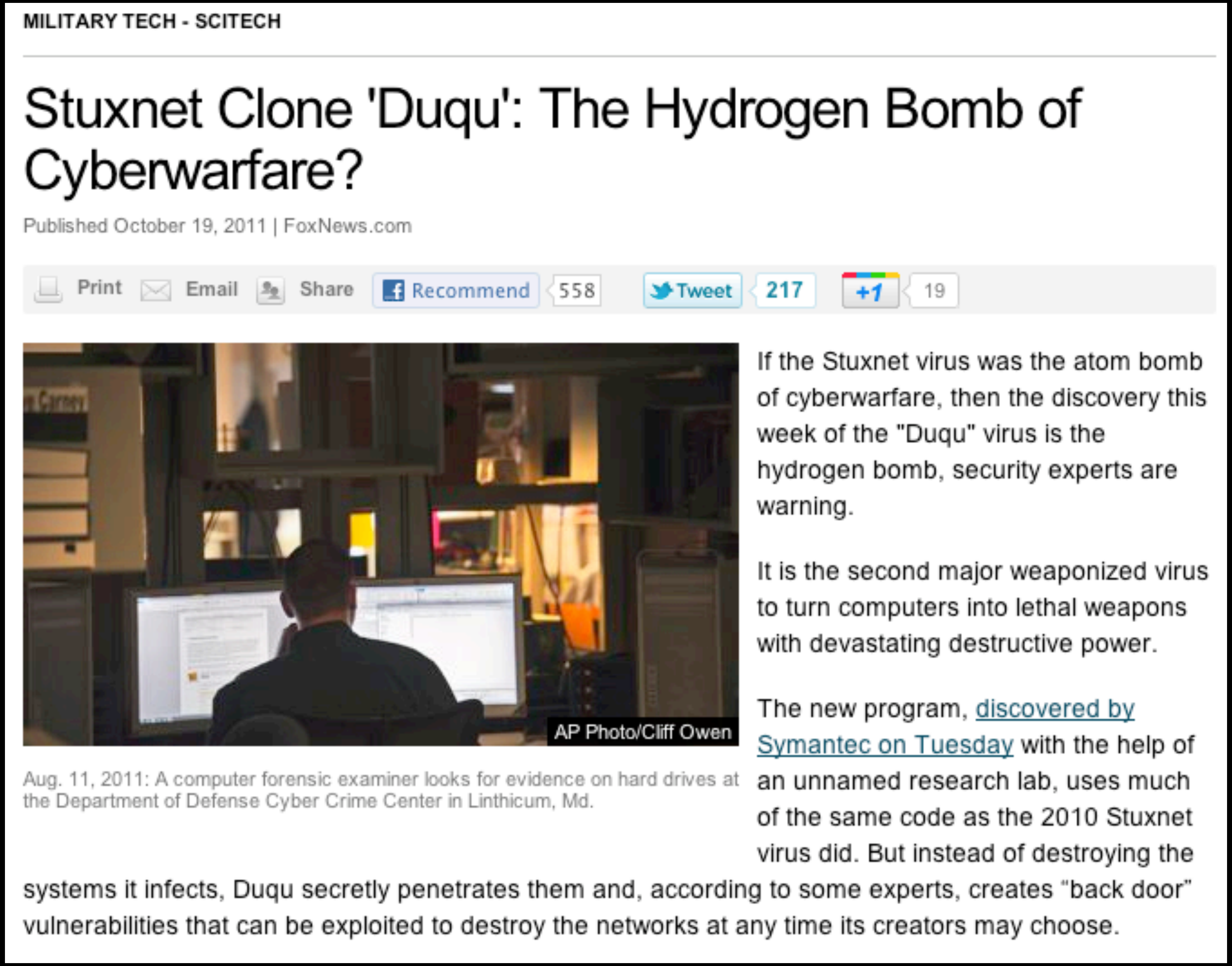


Duqu Trojan revealed to be shape-shifting serial killer

Embedded in the code are humorous references to the Showtime show 'Dexter'

headhntr

Duqu



MILITARY TECH - SCITECH

Stuxnet Clone 'Duqu': The Hydrogen Bomb of Cyberwarfare?

Published October 19, 2011 | FoxNews.com

Aug. 11, 2011: A computer forensic examiner looks for evidence on hard drives at the Department of Defense Cyber Crime Center in Linthicum, Md.

If the Stuxnet virus was the atom bomb of cyberwarfare, then the discovery this week of the "Duqu" virus is the hydrogen bomb, security experts are warning.

It is the second major weaponized virus to turn computers into lethal weapons with devastating destructive power.

The new program, discovered by Symantec on Tuesday with the help of an unnamed research lab, uses much of the same code as the 2010 Stuxnet virus did. But instead of destroying the systems it infects, Duqu secretly penetrates them and, according to some experts, creates "back door" vulnerabilities that can be exploited to destroy the networks at any time its creators may choose.

headhntr

History of APT

- 1998-2000 - Moonlight Maze
- 2002-? - Byzantine Hades
- 2003-2005 - Titan Rain
- 2006-2011 - Shady Rat
- 2009 - Ghostnet
- 2009 - Aurora
- 2009 - Night Dragon
- 2010 - Stuxnet
- 2010 - French Government
- 2011 - Lockheed Martin / RSA
- 2011 - Commodo / Diginotar
- 2011 - Nitro

Byzantine Hades

- Diplomatic Security Daily
  5 Nov 2008 SECRET//NOFORN

"

Byzantine Hades, a cover term for a series of related computer network intrusions with a believed nexus to China, has affected U.S. and foreign governments as well as cleared defense contractors since at least 2003.

"

Byzantine Hades

- Diplomatic Security Daily
  3 Nov 2008 SECRET//NOFORN

“Since late 2002, USG organizations have been targeted with social-engineering online attacks by BC (Byzantine Candor) actors. BC, an intrusion subset of Byzantine Hades activity, is a series of related computer network intrusions affecting U.S. and foreign systems and is believed to originate from the PRC.

BC intruders have relied on techniques including exploiting Windows system vulnerabilities and stealing login credentials to gain access to hundreds of USG and cleared defense contractor systems over the years. In the U.S., the majority of the systems BC actors have targeted belong to the U.S. Army, but targets also include other DoD services as well as DoS, Department of Energy, additional USG entities, and commercial systems and networks.”

Byzantine Hades

- Diplomatic Security Daily
  3 Nov 2008 SECRET//NOFORN

“Air Force Office of Special Investigations (AFOSI) reporting indicates, on March 11, Byzantine Candor (BC) actors gained access to one system at the ISP, onto which the actors transferred multiple files, including several C&C tools.”

“From April through October 13, the BC actors used this computer system to conduct CNE on multiple victims. During this time period, the actors exfiltrated at least 50 megabytes of e-mail messages and attached documents, as well as a complete list of usernames and passwords from an unspecified USG agency.”

“...a malicious file named salaryincrease-surveyandforecast.zip”

Byzantine Hades

- Diplomatic Security Daily
  Thu, 2 Apr 2009 SECRET//NOFORN

"

Sensitive reports indicate the domains www.indexnews.org, www.indexindian.com, www.lookbytheway.net, and www.macfeeresponse.org were involved in Byzantine Hades (BH) intrusion activity in 2006. All four domains were registered in Chengdu, China. The IP addresses associated with these domains substantiate this as the location. Subsequent analysis of registration information also leads to a tenuous connection between these hostile domains and the People's Liberation Army (PLA) Chengdu Military Region First Technical Reconnaissance Bureau (TRB).

"

Byzantine Hades

- Diplomatic Security Daily
  18 Dec 2008 SECRET//NOFORN

“Byzantine Anchor, a subset of Byzantine Hades, refers to a group of associated computer network intrusions with an apparent nexus to China. Numerous sensitive reports have identified an apparent relationship between the Chinese hacker group Javaphile and BA intrusion activity based on overlapping characteristics. IP addresses that have been involved in BA CNE attempts have also hosted the Javaphile.org webpage and been the source of Javaphile-linked bulletin board postings. Furthermore, Javaphile and BA have been associated due to the use of the customized command-and-control tool dubbed eRACS developed by Javaphile member 'Ericool8' -- one of many aliases used by Javaphile’s leader Yinan Peng.”

Byzantine Hades

- Diplomatic Security Daily
  18 Dec 2008 SECRET//NOFORN

"On July 30, 2008, an incident was attributed to BA wherein a compromised system located at the Pentagon downloaded and installed the eRACS tool from IP 203.81.177.121."

Byzantine Hades

- Diplomatic Security Daily
  18 Dec 2008 SECRET//NOFORN

“he Government of Germany (GoG) has previously asserted publicly that Chinese actors have conducted intrusions into GoG networks. However, in the closed Berlin Talks, additional detail and perspective were provided.”

Moonlight Maze

Titan Rain

headhntr

Aurora

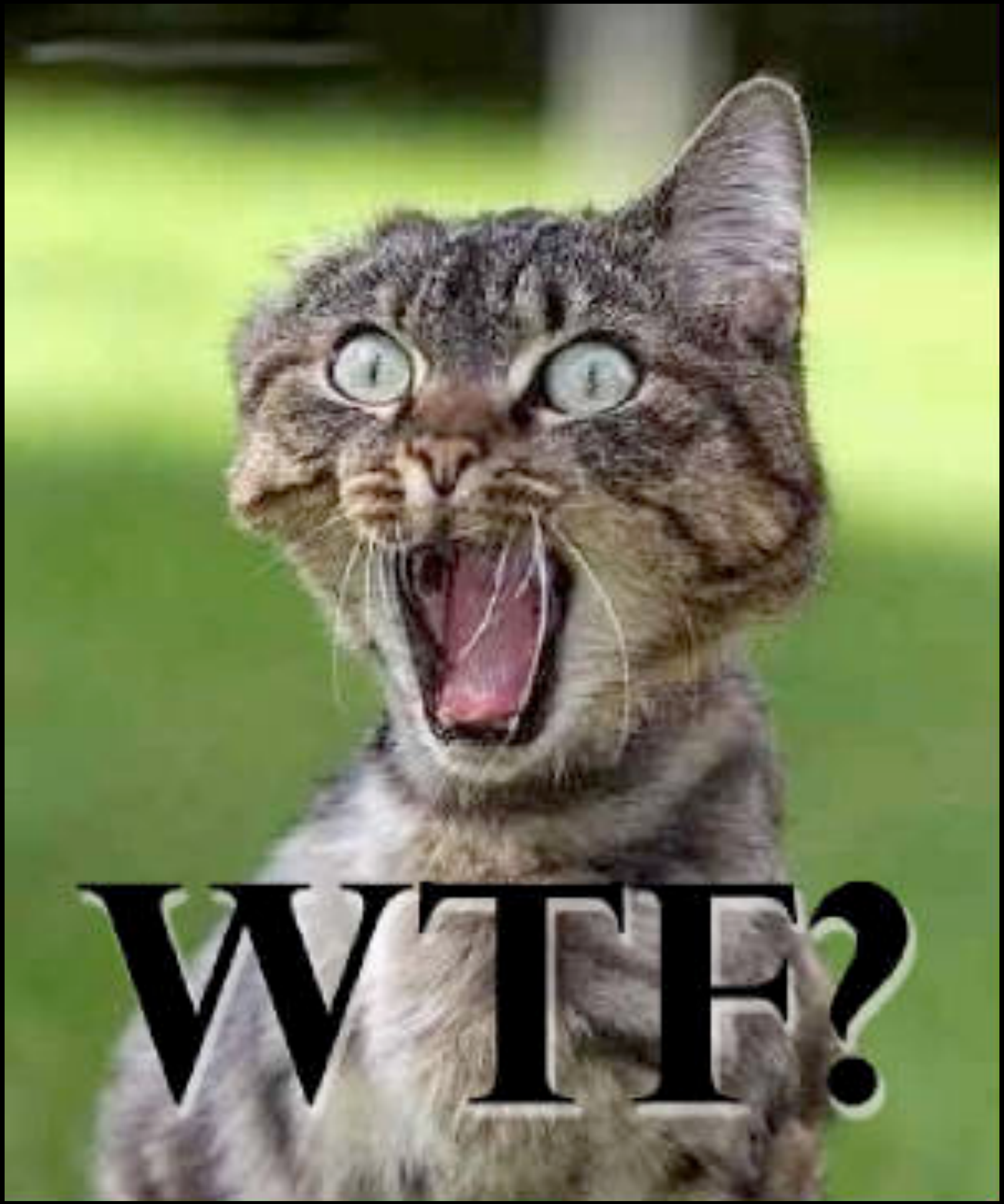
OPERATION AURORA
How To Respond To The Recent Microsoft Internet Explorer Vulnerability

Shady Rat

headhntr

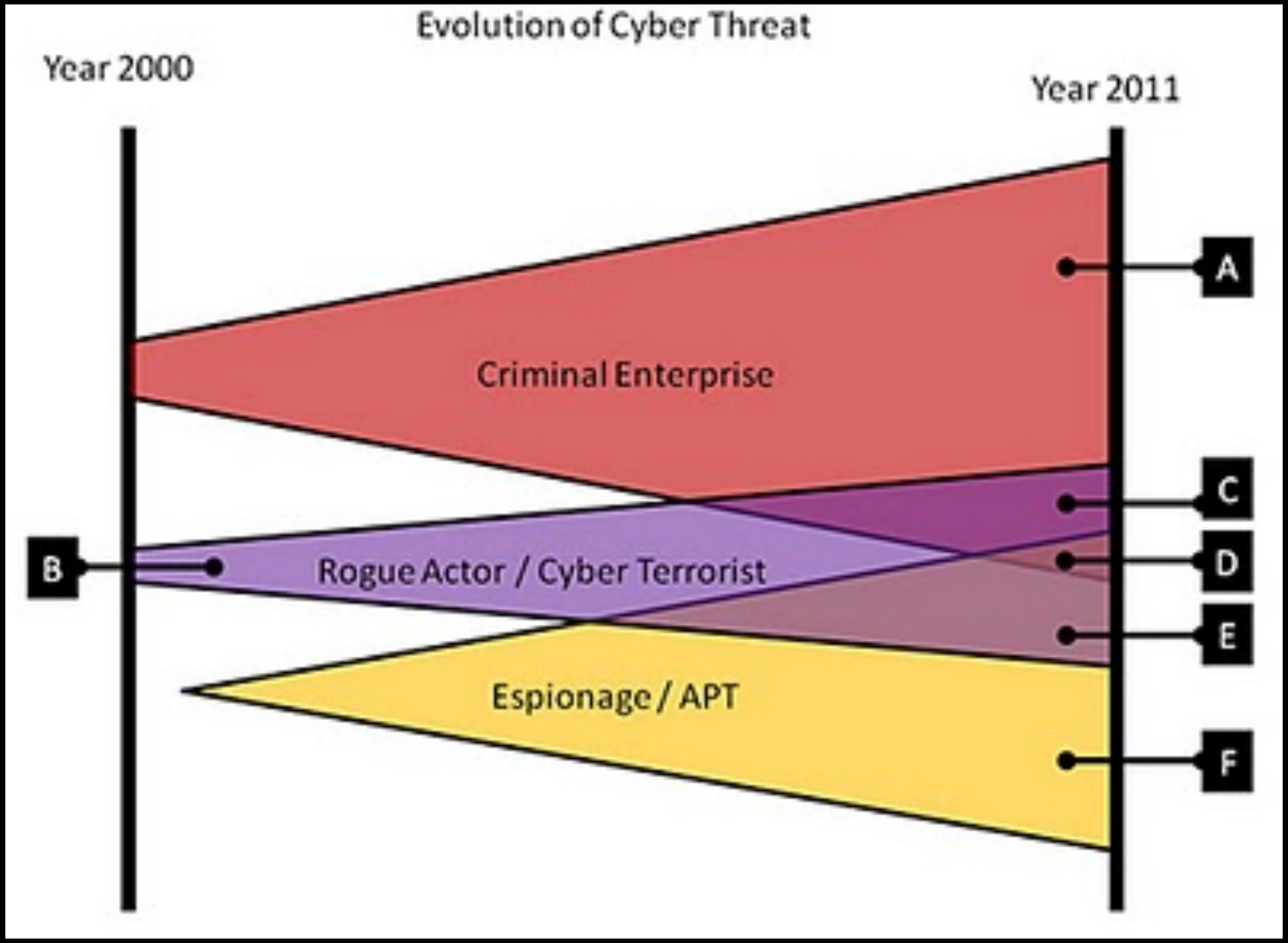
Current Events

- RSA / Lockheed
- Commodo / Diginotar CA compromises
- Nitro



WTF?

Threat Landscape



headhntr

Threat distinction

vs

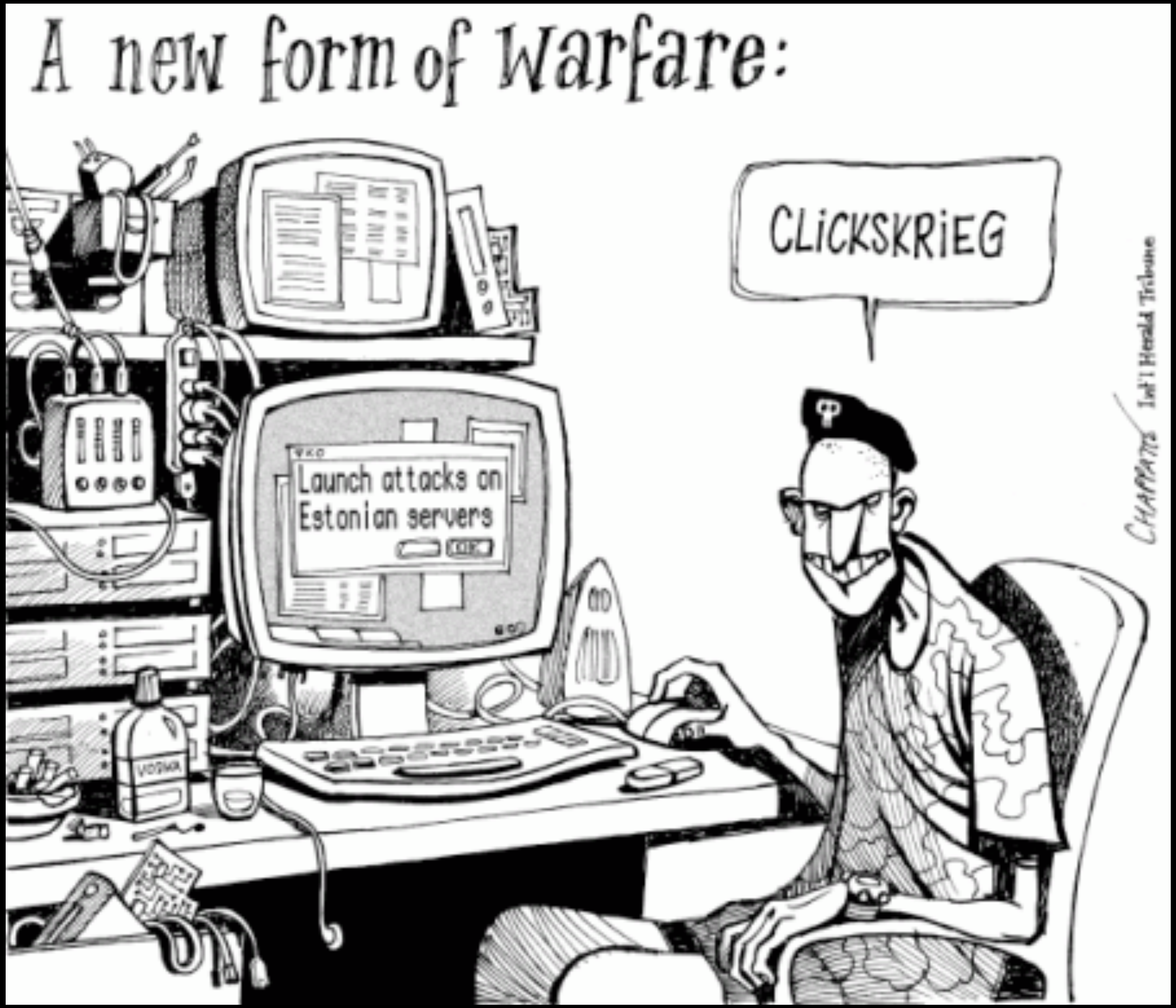
Framing the argument

Some of this stuff sounds bad:

- operation orchard
- Stuxnet

Cyber-war vs Cyber-terrorism vs WAR

Why War metaphors?



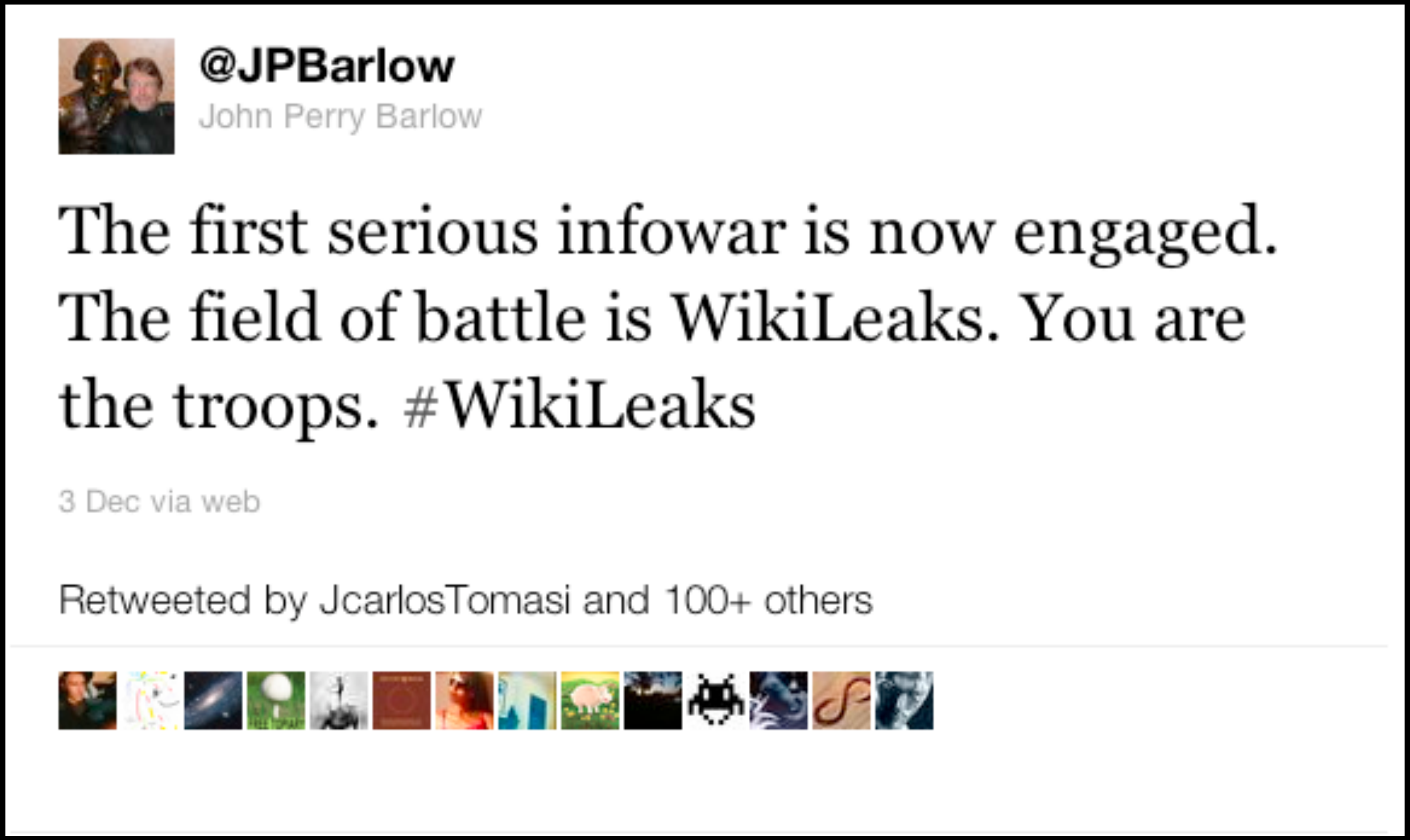
headhntr

Pathology of the Own3d

- Shock -> Dismissal -> Hubris

- Shock -> Dismissal -> Abrogation

War Metaphors Backfire



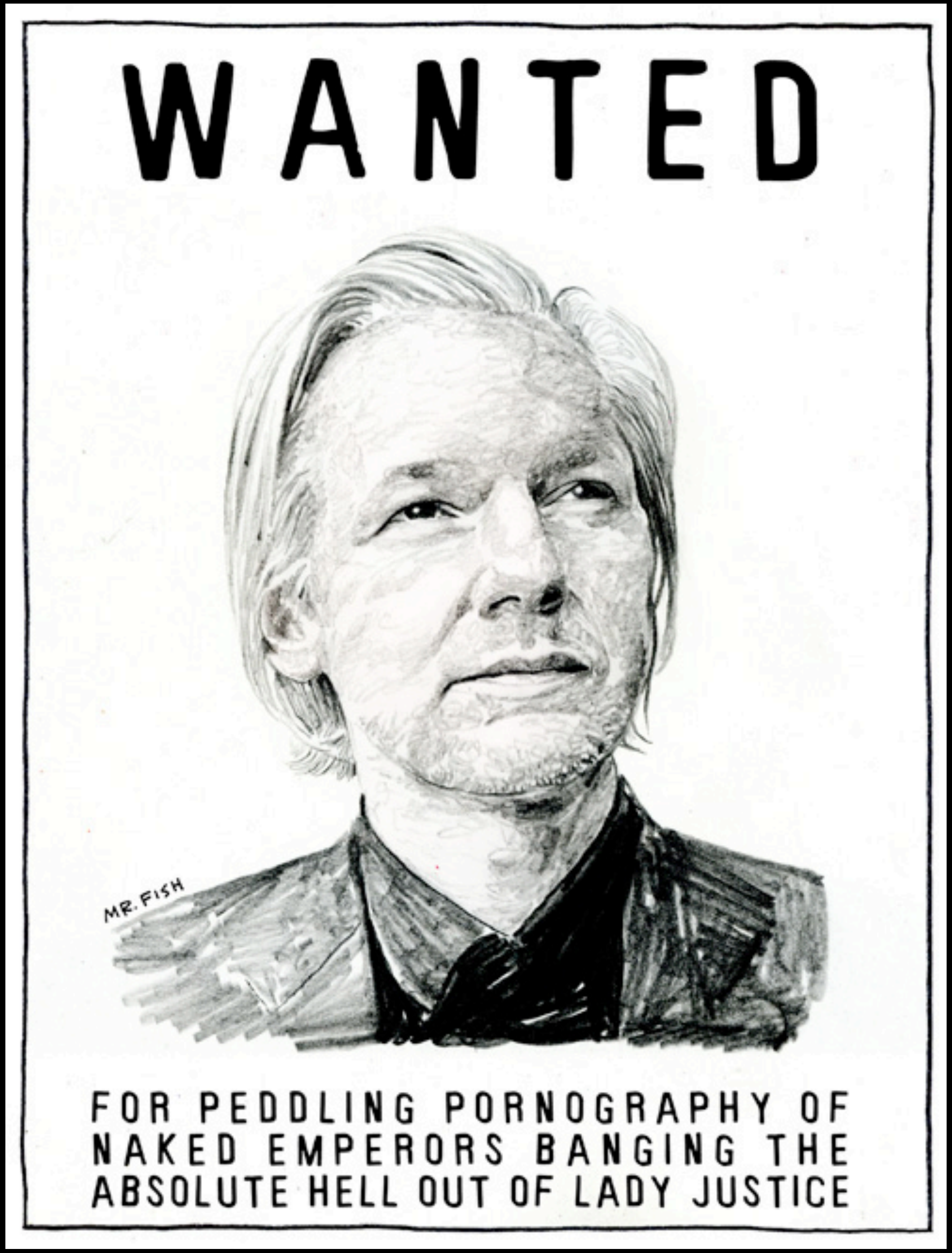
@JPBarlow
John Perry Barlow

The first serious infowar is now engaged. The field of battle is WikiLeaks. You are the troops. #WikiLeaks

3 Dec via web

Retweeted by JcarlosTomasi and 100+ others

Cyber-terrorist


WANTED
MR. FISH
FOR PEDDLING PORNOGRAPHY OF
NAKED EMPERORS BANGING THE
ABSOLUTE HELL OUT OF LADY JUSTICE

headhntr

Cyberwar Profiteering

- War = $$$$

It's not just the Sexy

headhntr

The Infocalypse

The Economist

JULY 3RD–9TH 2010

Economist.com

Victory for the gun lobby

Who will run Brazil?

Rewriting Wall Street's rules

How Big Oil became Big Gas

The link between IQ and disease

Cyberwar

The threat from the internet

headhntr

Reality Check

What actually happens during a war?

- First casualty is civil liberties
- People who disagree with us =

"terrorist" or "enemy"

- Government = safety net
- Patriotism escalates, dissent disappears
- What else?

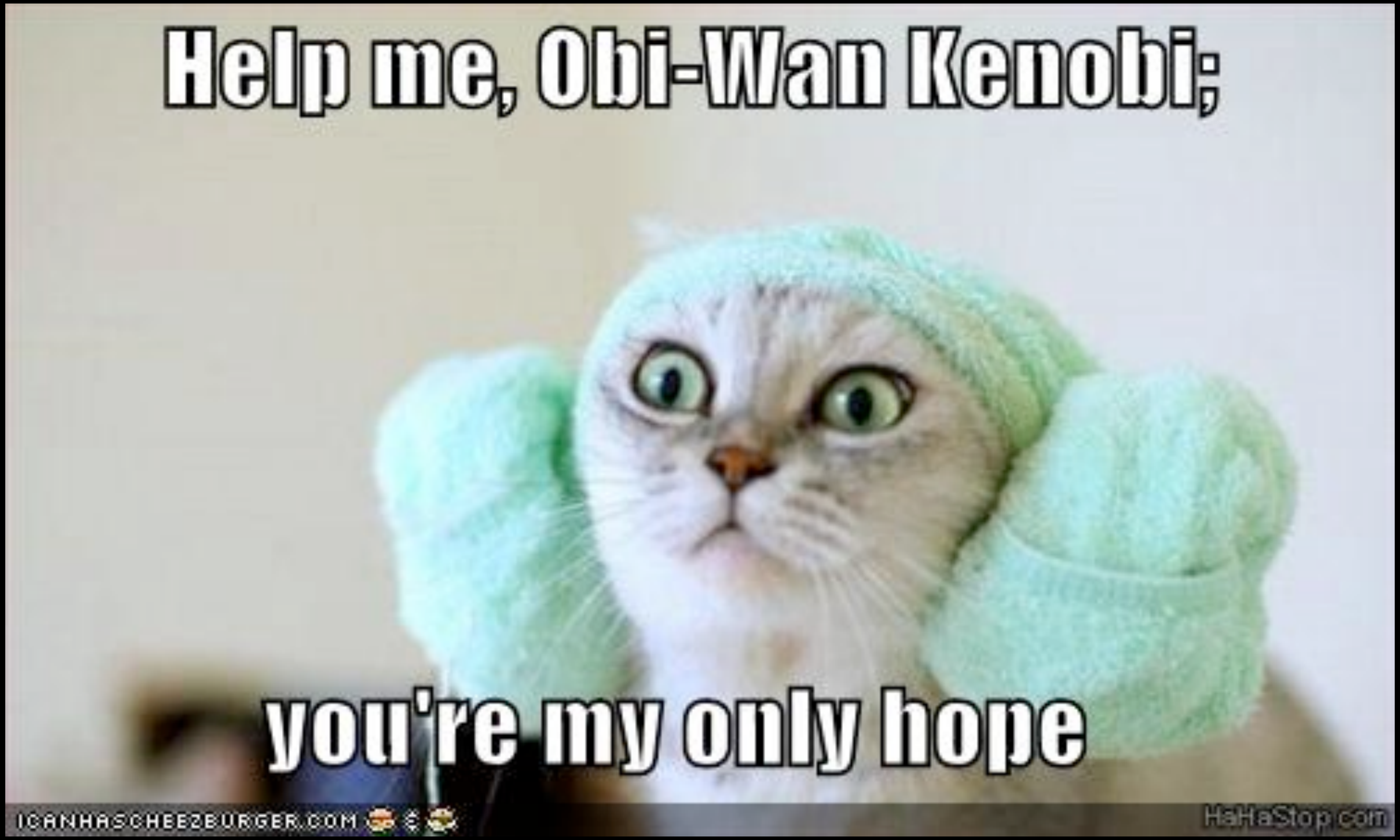
Danger

There's a power struggle going on for control of our nation's cyber security strategy, and the NSA and DoD are winning. If we frame the debate in terms of war, if we accept the military's expansive cyberspace definition of "war," we feed our fears.

We reinforce the notion that we're helpless -- what person or organization can defend itself in a war? -- and others need to protect us. We invite the military to takeover security, and to ignore the limits on power that often get jettisoned during wartime.

-- Bruce Schneier

Hope !



headhntr

There is no Cyberwar

"I think that is a terrible metaphor and I think that is a terrible concept," Schmidt said. "There are no winners in that environment."

Every time you say "CYBERWAR" you lose a civil liberty.

headhntr

Packets are not bullets and once you start talking like they are, you reach all kinds of very wrong conclusions about what kind of actions are justified.

Questions

????