SECURENINJA

SecureNinja
The CyberSecurity Experts

Shakeel Tufail
Chief Ninja (CEO)

Washington DC

Pentagon – Dept. of Defense

US Air Force

SecureNinja

Financial Regulatory Agency (FINRA)

CompUSA

AIG

America Online

JP Morgan

General Dynamics

Cigital

US NAVY

Fortify

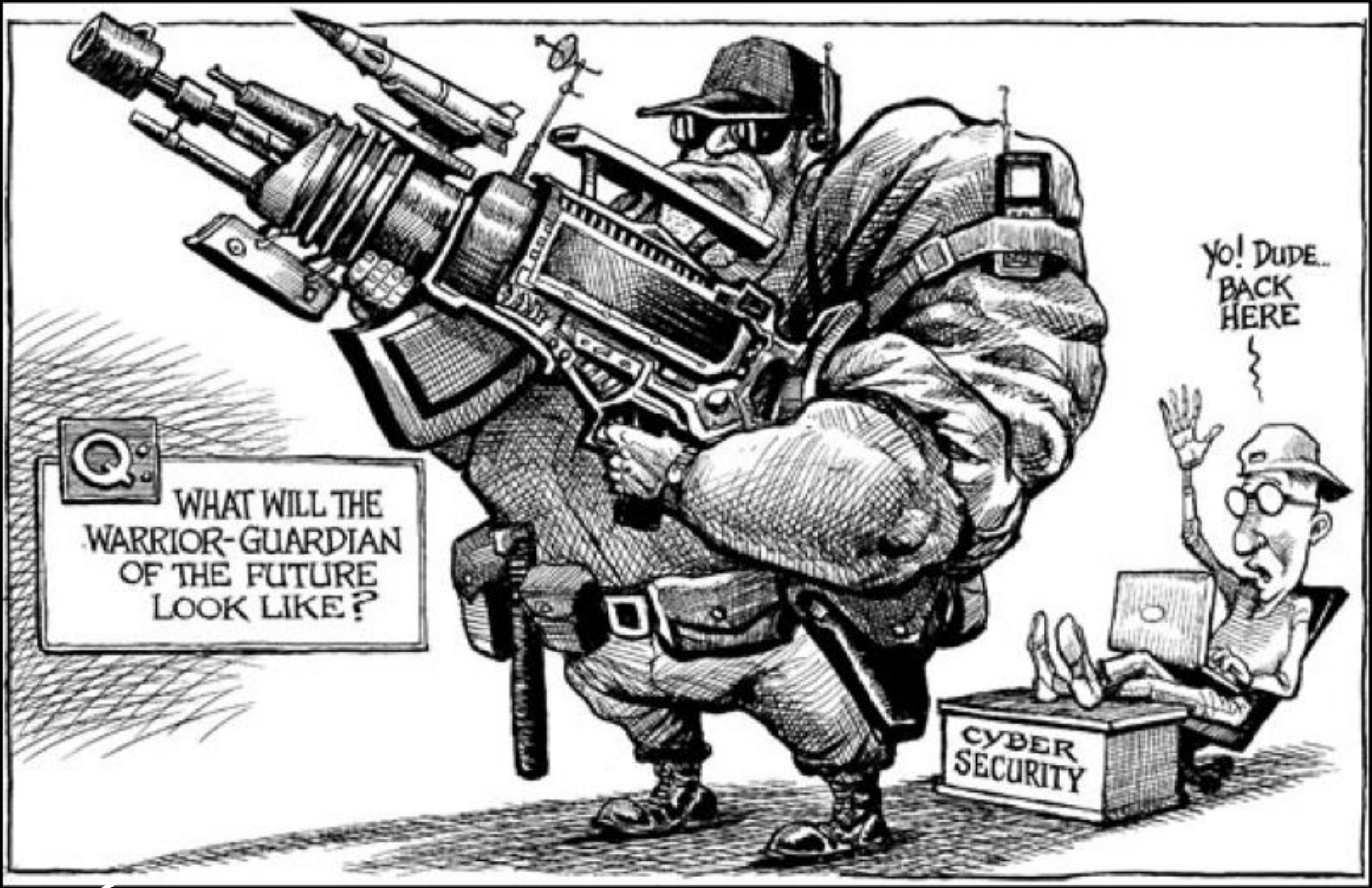
Bank of America

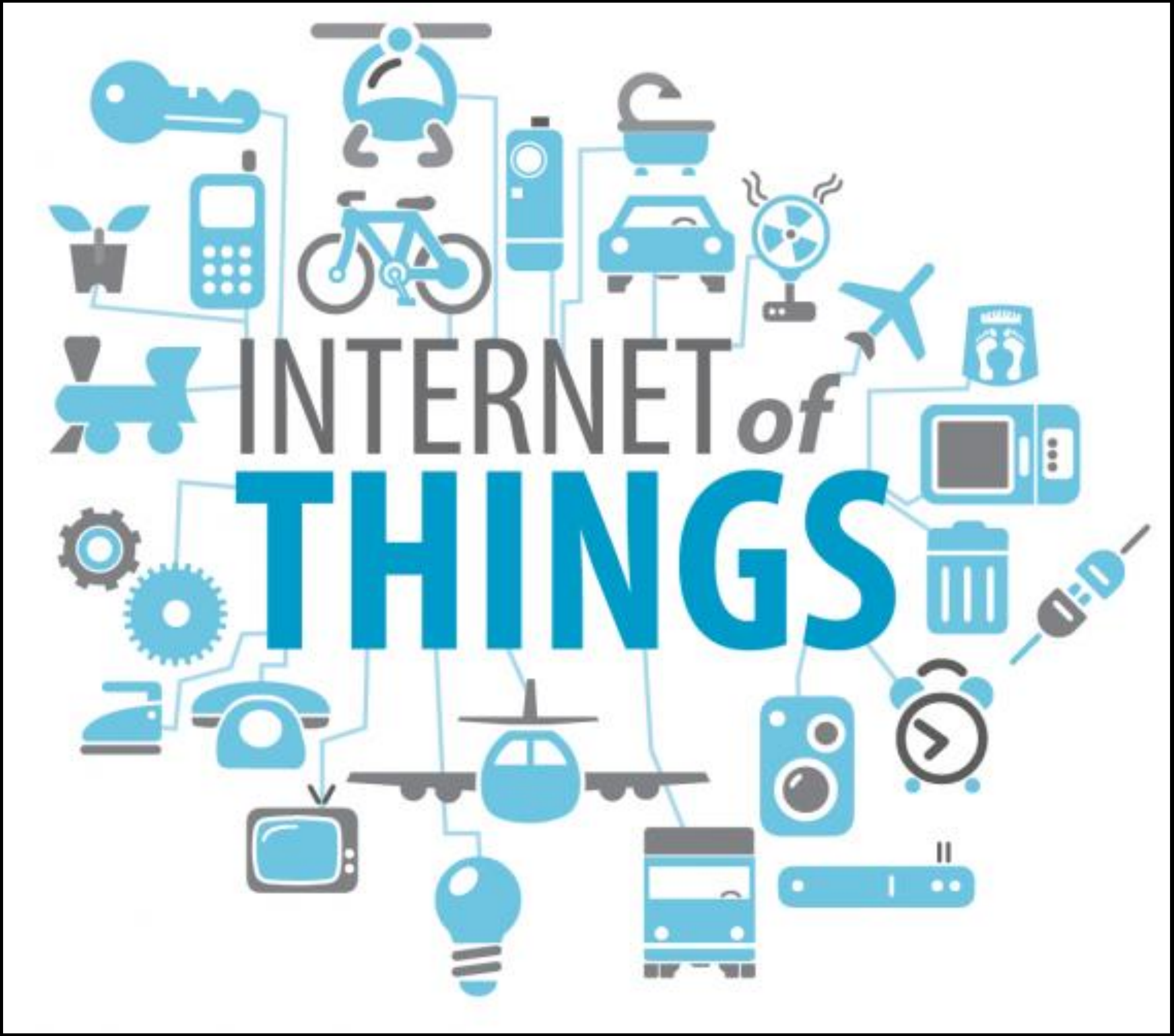
Hewlett Packard

What Are We Trying To Protect?

- The valuable properties of anything is considered an asset
  - Data – CIA, privacy, accountability
  - Time – Launch delay, processing delay, etc.
  - Money – can't make sales, can't process transactions
  - Reputation and Brand – loss of trust
  - Legal – compliance, contractual regulation
  - Government -Military, Intel; Mission Critical Systems

Data is the New Currency!


Q
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE.. BACK HERE
CYBER SECURITY

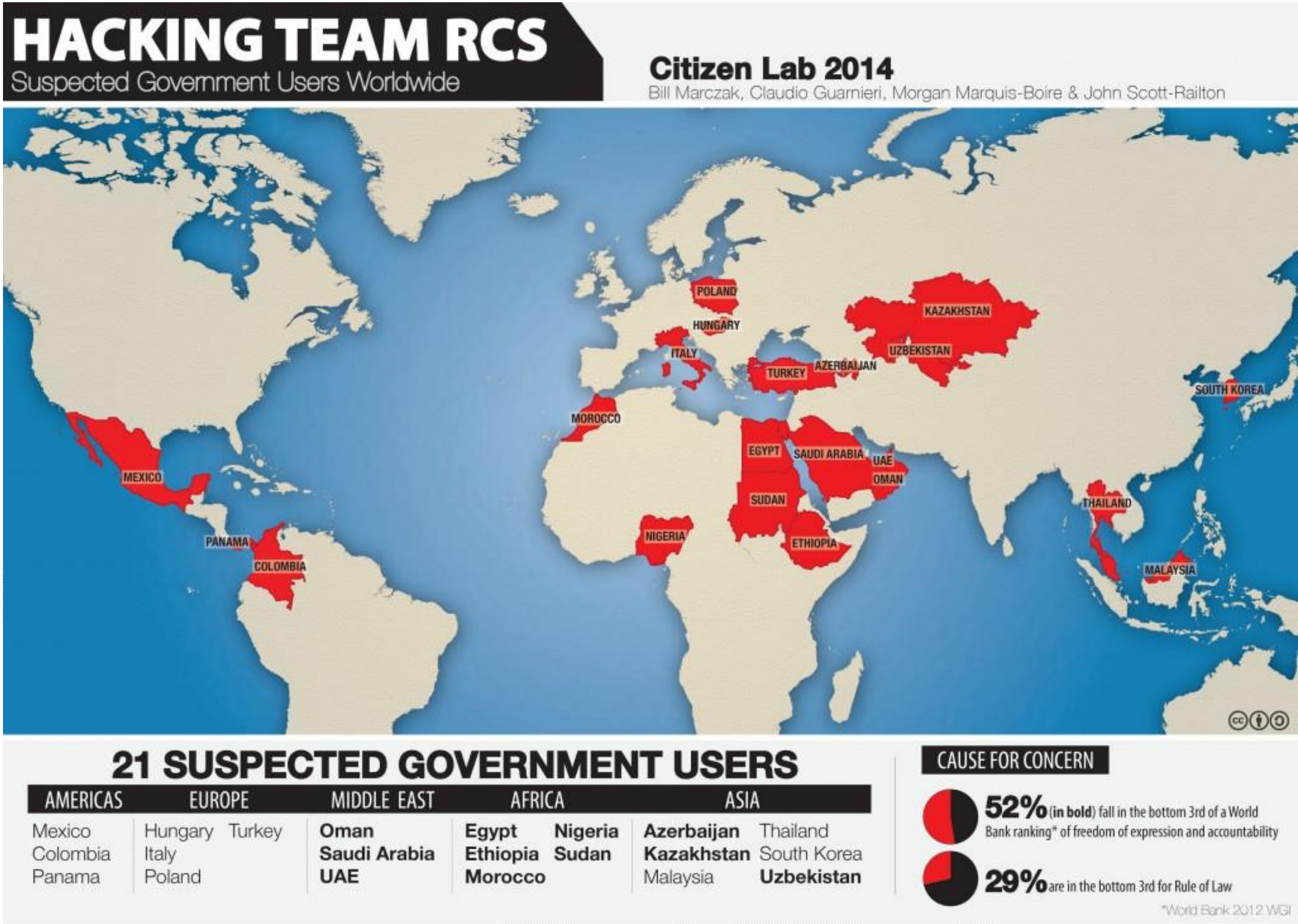

INTERNET of
THINGS

CyberSecurity Challenges

- More & More Connectivity
  - More users are connecting, not less!
  - Think mobile, web, internet, intranet, even Classified Systems
- Increasing System Complexity
  - Applications are getting bigger and more distributed faster than ever!
  - More technologies, languages, interfaces!
- Risk of External Vendors / 3rd Party Software
  - Systems are constantly evolving and changing on the fly!
  - More frameworks, plugins, open source software, API’s
- Too Much Reliance on Compliance & Standards
  - Cybersecurity regulations, rules, audits, etc. are increasing
- Lack of Experience & Knowledge
  - Training is required for ALL Job roles

Government Sponsored Malware?!

]HackingTeam[
~~Rely on us.~~
HACKED



HACKING TEAM RCS

Suspected Government Users Worldwide

Citizen Lab 2014

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire & John Scott-Railton

21 SUSPECTED GOVERNMENT USERS

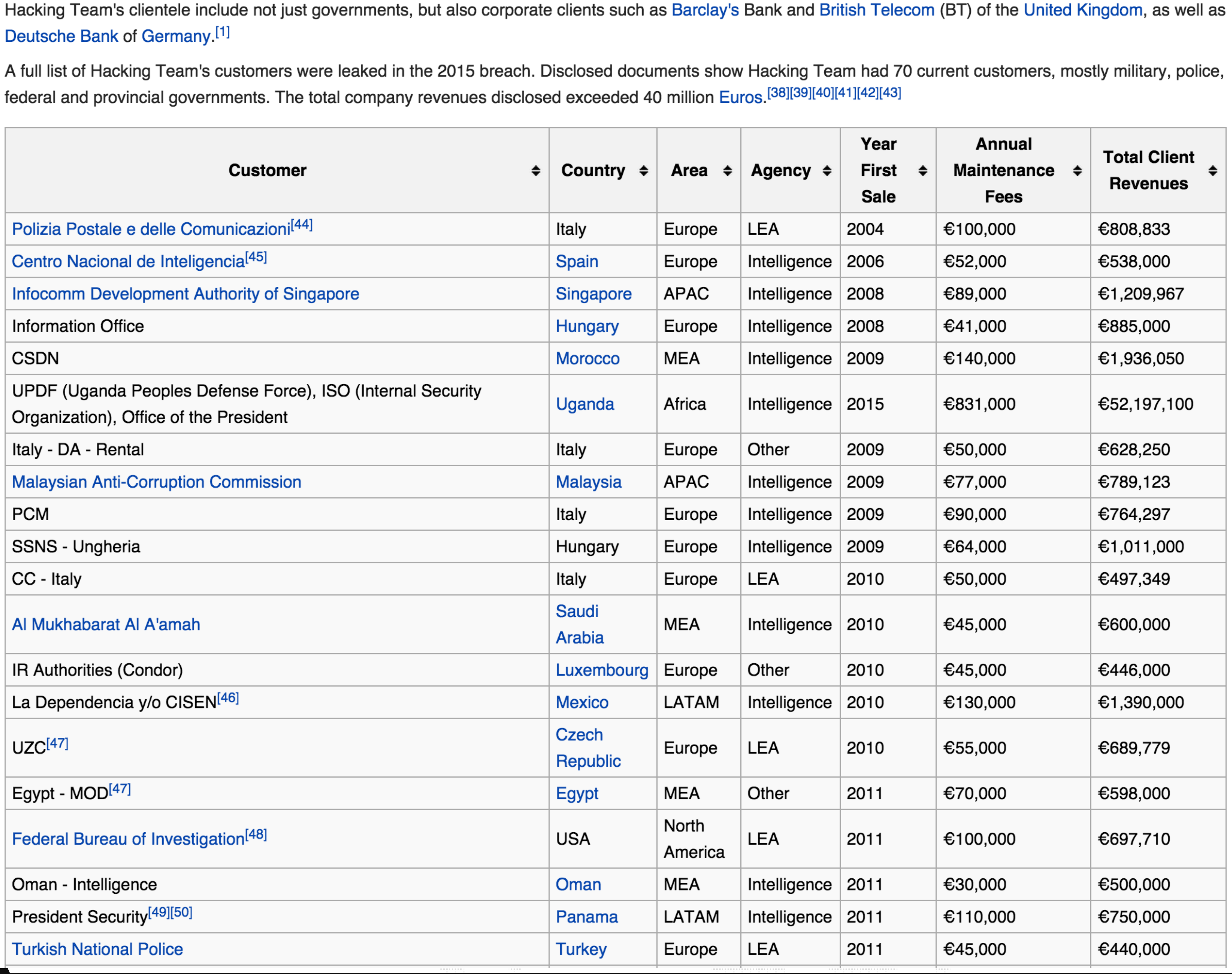
AMERICAS	EUROPE		MIDDLE EAST	AFRICA		ASIA	
Mexico	Hungary	Turkey	**Oman**	**Egypt**	**Nigeria**	**Azerbaijan**	Thailand
Colombia	Italy		**Saudi Arabia**	**Ethiopia**	**Sudan**	**Kazakhstan**	South Korea
Panama	Poland		**UAE**	**Morocco**		Malaysia	**Uzbekistan**

CAUSE FOR CONCERN

52% (**in bold**) fall in the bottom 3rd of a World Bank ranking* of freedom of expression and accountability

29% are in the bottom 3rd for Rule of Law

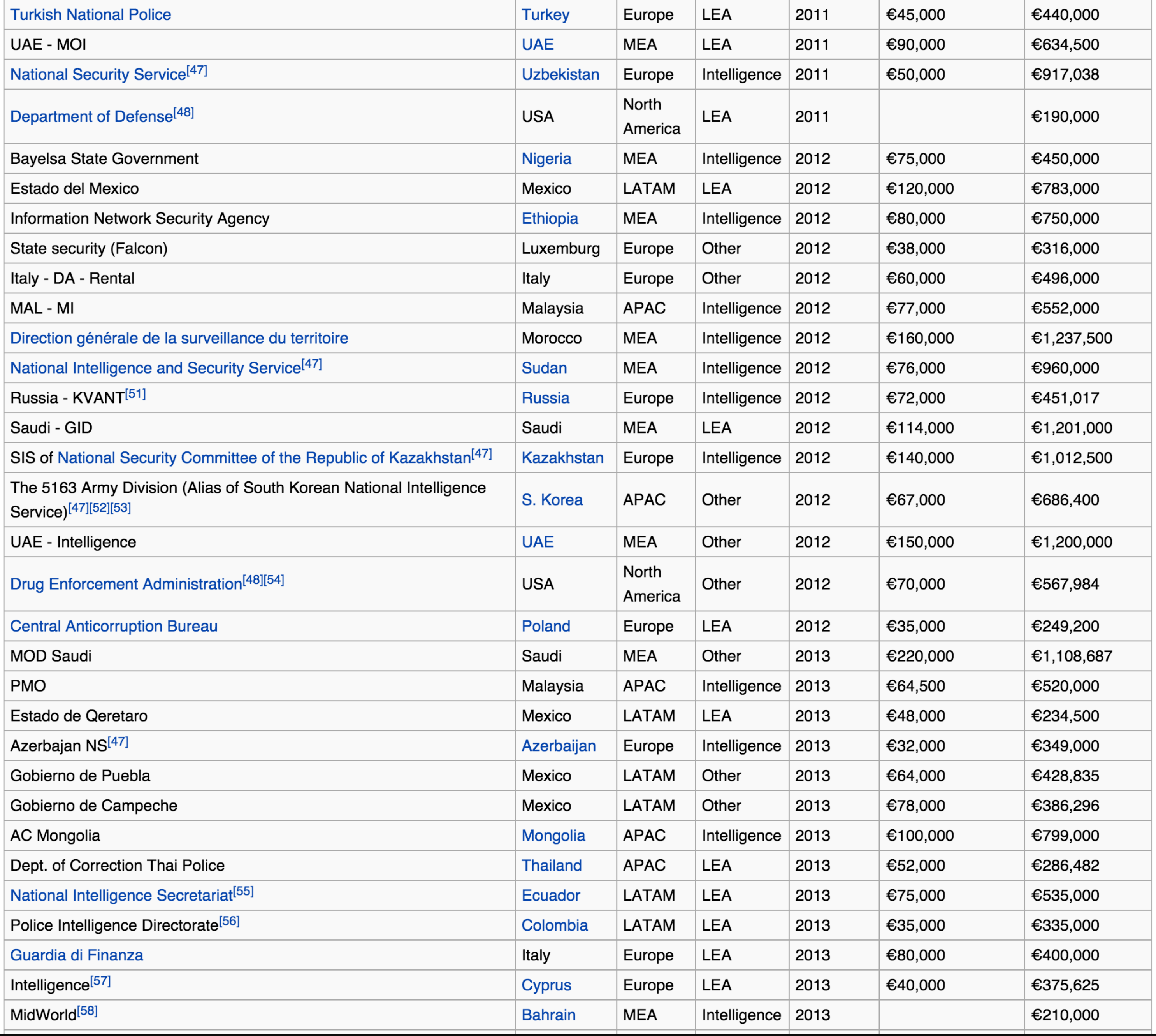
*World Bank 2012 WGI



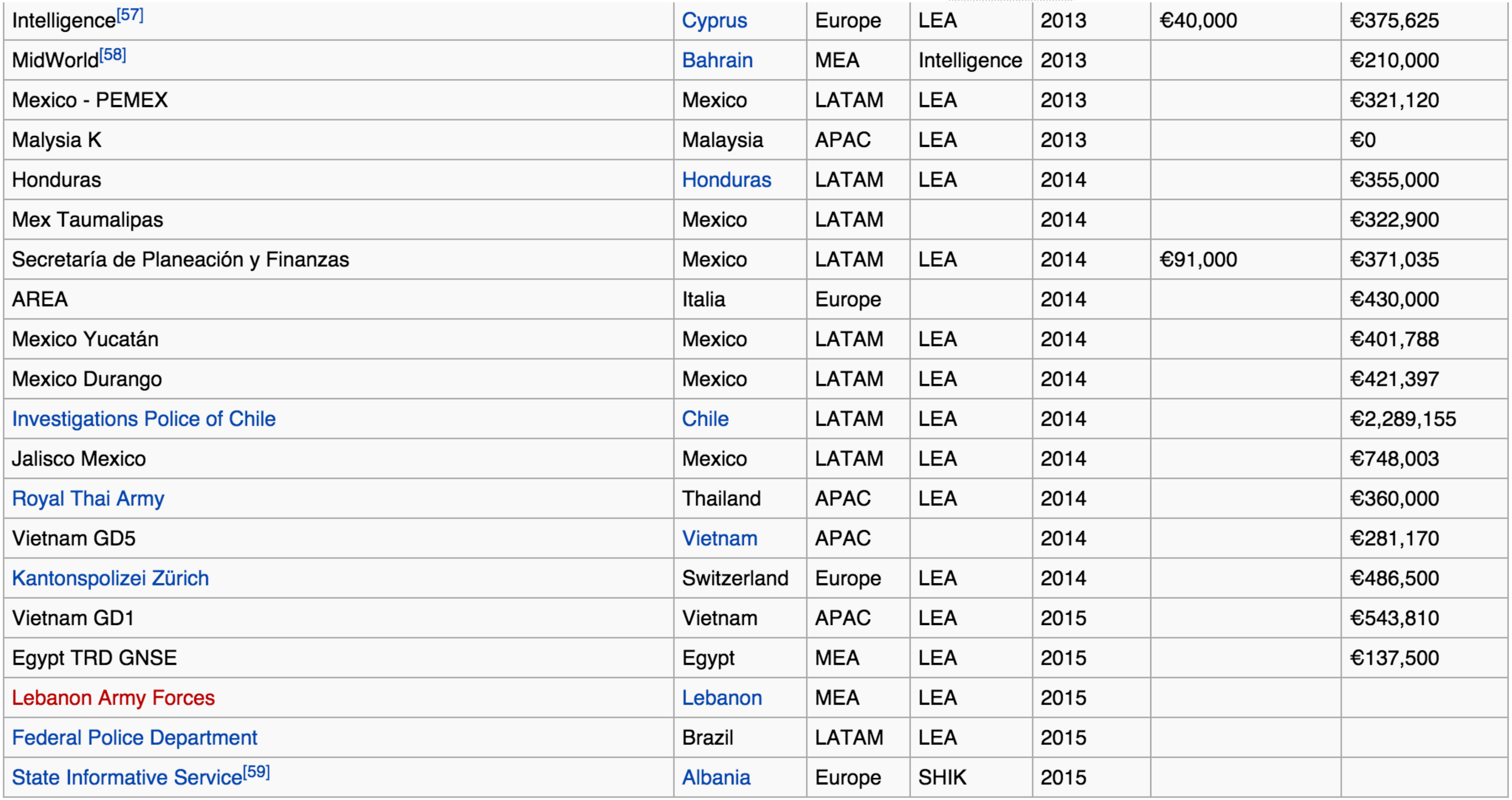
Hacking Team's clientele include not just governments, but also corporate clients such as Barclay's Bank and British Telecom (BT) of the United Kingdom, as well as Deutsche Bank of Germany.[1]

A full list of Hacking Team's customers were leaked in the 2015 breach. Disclosed documents show Hacking Team had 70 current customers, mostly military, police, federal and provincial governments. The total company revenues disclosed exceeded 40 million Euros.[38][39][40][41][42][43]

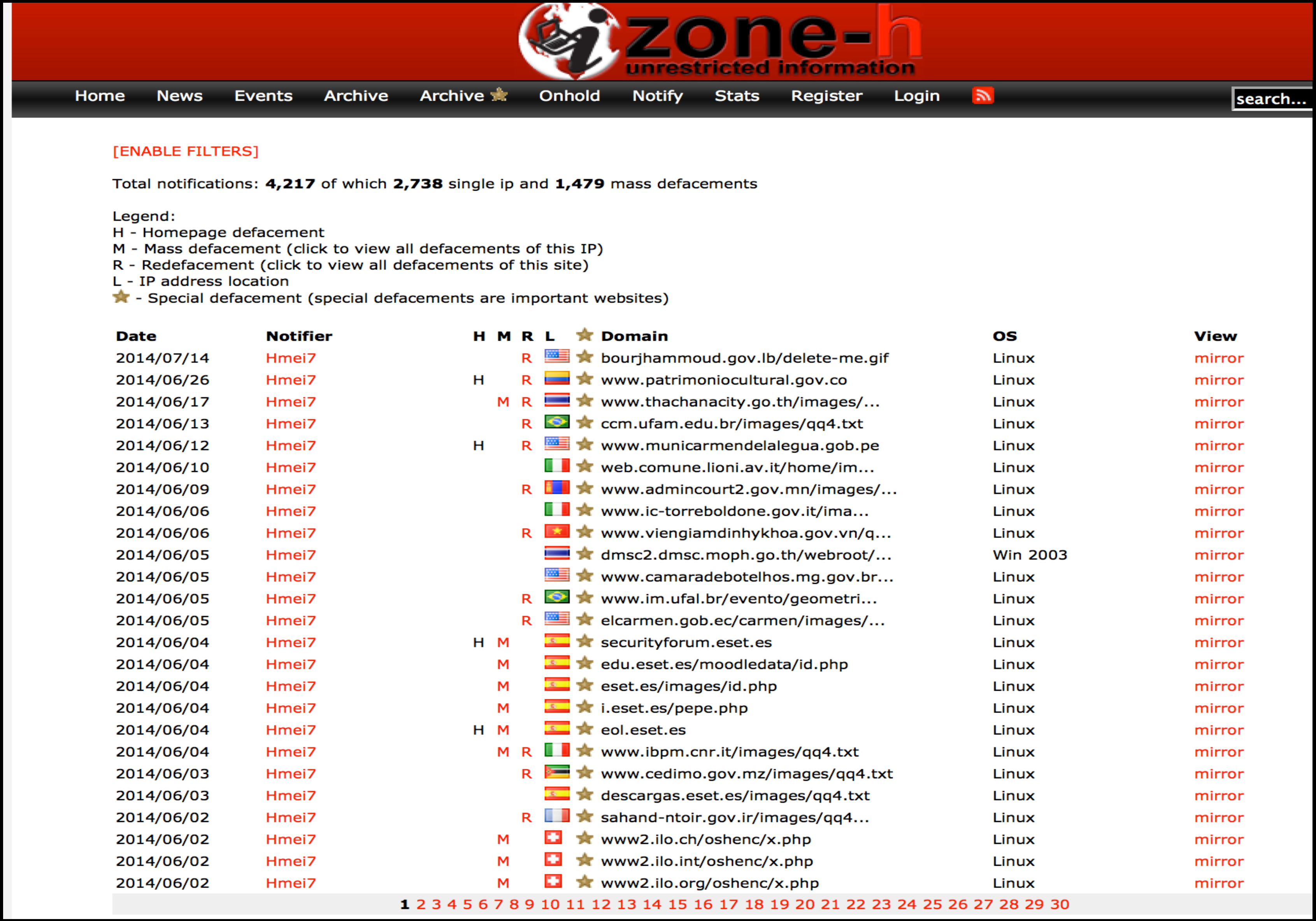
Customer	Country	Area	Agency	Year First Sale	Annual Maintenance Fees	Total Client Revenues
Polizia Postale e delle Comunicazioni[44]	Italy	Europe	LEA	2004	€100,000	€808,833
Centro Nacional de Inteligencia[45]	Spain	Europe	Intelligence	2006	€52,000	€538,000
Infocomm Development Authority of Singapore	Singapore	APAC	Intelligence	2008	€89,000	€1,209,967
Information Office	Hungary	Europe	Intelligence	2008	€41,000	€885,000
CSDN	Morocco	MEA	Intelligence	2009	€140,000	€1,936,050
UPDF (Uganda Peoples Defense Force), ISO (Internal Security Organization), Office of the President	Uganda	Africa	Intelligence	2015	€831,000	€52,197,100
Italy - DA - Rental	Italy	Europe	Other	2009	€50,000	€628,250
Malaysian Anti-Corruption Commission	Malaysia	APAC	Intelligence	2009	€77,000	€789,123
PCM	Italy	Europe	Intelligence	2009	€90,000	€764,297
SSNS - Ungheria	Hungary	Europe	Intelligence	2009	€64,000	€1,011,000
CC - Italy	Italy	Europe	LEA	2010	€50,000	€497,349
Al Mukhabarat Al A'amah	Saudi Arabia	MEA	Intelligence	2010	€45,000	€600,000
IR Authorities (Condor)	Luxembourg	Europe	Other	2010	€45,000	€446,000
La Dependencia y/o CISEN[46]	Mexico	LATAM	Intelligence	2010	€130,000	€1,390,000
UZC[47]	Czech Republic	Europe	LEA	2010	€55,000	€689,779
Egypt - MOD[47]	Egypt	MEA	Other	2011	€70,000	€598,000
Federal Bureau of Investigation[48]	USA	North America	LEA	2011	€100,000	€697,710
Oman - Intelligence	Oman	MEA	Intelligence	2011	€30,000	€500,000
President Security[49][50]	Panama	LATAM	Intelligence	2011	€110,000	€750,000
Turkish National Police	Turkey	Europe	LEA	2011	€45,000	€440,000



Turkish National Police	Turkey	Europe	LEA	2011	€45,000	€440,000
UAE - MOI	UAE	MEA	LEA	2011	€90,000	€634,500
National Security Service[47]	Uzbekistan	Europe	Intelligence	2011	€50,000	€917,038
Department of Defense[48]	USA	North America	LEA	2011		€190,000
Bayelsa State Government	Nigeria	MEA	Intelligence	2012	€75,000	€450,000
Estado del Mexico	Mexico	LATAM	LEA	2012	€120,000	€783,000
Information Network Security Agency	Ethiopia	MEA	Intelligence	2012	€80,000	€750,000
State security (Falcon)	Luxemburg	Europe	Other	2012	€38,000	€316,000
Italy - DA - Rental	Italy	Europe	Other	2012	€60,000	€496,000
MAL - MI	Malaysia	APAC	Intelligence	2012	€77,000	€552,000
Direction générale de la surveillance du territoire	Morocco	MEA	Intelligence	2012	€160,000	€1,237,500
National Intelligence and Security Service[47]	Sudan	MEA	Intelligence	2012	€76,000	€960,000
Russia - KVANT[51]	Russia	Europe	Intelligence	2012	€72,000	€451,017
Saudi - GID	Saudi	MEA	LEA	2012	€114,000	€1,201,000
SIS of National Security Committee of the Republic of Kazakhstan[47]	Kazakhstan	Europe	Intelligence	2012	€140,000	€1,012,500
The 5163 Army Division (Alias of South Korean National Intelligence Service)[47][52][53]	S. Korea	APAC	Other	2012	€67,000	€686,400
UAE - Intelligence	UAE	MEA	Other	2012	€150,000	€1,200,000
Drug Enforcement Administration[48][54]	USA	North America	Other	2012	€70,000	€567,984
Central Anticorruption Bureau	Poland	Europe	LEA	2012	€35,000	€249,200
MOD Saudi	Saudi	MEA	Other	2013	€220,000	€1,108,687
PMO	Malaysia	APAC	Intelligence	2013	€64,500	€520,000
Estado de Qeretaro	Mexico	LATAM	LEA	2013	€48,000	€234,500
Azerbajan NS[47]	Azerbaijan	Europe	Intelligence	2013	€32,000	€349,000
Gobierno de Puebla	Mexico	LATAM	Other	2013	€64,000	€428,835
Gobierno de Campeche	Mexico	LATAM	Other	2013	€78,000	€386,296
AC Mongolia	Mongolia	APAC	Intelligence	2013	€100,000	€799,000
Dept. of Correction Thai Police	Thailand	APAC	LEA	2013	€52,000	€286,482
National Intelligence Secretariat[55]	Ecuador	LATAM	LEA	2013	€75,000	€535,000
Police Intelligence Directorate[56]	Colombia	LATAM	LEA	2013	€35,000	€335,000
Guardia di Finanza	Italy	Europe	LEA	2013	€80,000	€400,000
Intelligence[57]	Cyprus	Europe	LEA	2013	€40,000	€375,625
MidWorld[58]	Bahrain	MEA	Intelligence	2013		€210,000



Intelligence[57]	Cyprus	Europe	LEA	2013	€40,000	€375,625
MidWorld[58]	Bahrain	MEA	Intelligence	2013		€210,000
Mexico - PEMEX	Mexico	LATAM	LEA	2013		€321,120
Malysia K	Malaysia	APAC	LEA	2013		€0
Honduras	Honduras	LATAM	LEA	2014		€355,000
Mex Taumalipas	Mexico	LATAM		2014		€322,900
Secretaría de Planeación y Finanzas	Mexico	LATAM	LEA	2014	€91,000	€371,035
AREA	Italia	Europe		2014		€430,000
Mexico Yucatán	Mexico	LATAM	LEA	2014		€401,788
Mexico Durango	Mexico	LATAM	LEA	2014		€421,397
Investigations Police of Chile	Chile	LATAM	LEA	2014		€2,289,155
Jalisco Mexico	Mexico	LATAM	LEA	2014		€748,003
Royal Thai Army	Thailand	APAC	LEA	2014		€360,000
Vietnam GD5	Vietnam	APAC		2014		€281,170
Kantonspolizei Zürich	Switzerland	Europe	LEA	2014		€486,500
Vietnam GD1	Vietnam	APAC	LEA	2015		€543,810
Egypt TRD GNSE	Egypt	MEA	LEA	2015		€137,500
Lebanon Army Forces	Lebanon	MEA	LEA	2015		
Federal Police Department	Brazil	LATAM	LEA	2015		
State Informative Service[59]	Albania	Europe	SHIK	2015		



[ENABLE FILTERS]

Total notifications: **4,217** of which **2,738** single ip and **1,479** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2014/07/14	Hmei7			R	🇺🇸	★	bourjhammoud.gov.lb/delete-me.gif	Linux	mirror
2014/06/26	Hmei7	H		R	🇨🇴	★	www.patrimoniocultural.gov.co	Linux	mirror
2014/06/17	Hmei7		M	R	🇹🇭	★	www.thachanacity.go.th/images/...	Linux	mirror
2014/06/13	Hmei7			R	🇧🇷	★	ccm.ufam.edu.br/images/qq4.txt	Linux	mirror
2014/06/12	Hmei7	H		R	🇺🇸	★	www.municarmendelalegua.gob.pe	Linux	mirror
2014/06/10	Hmei7				🇮🇹	★	web.comune.lioni.av.it/home/im...	Linux	mirror
2014/06/09	Hmei7			R	🇲🇳	★	www.admincourt2.gov.mn/images/...	Linux	mirror
2014/06/06	Hmei7				🇮🇹	★	www.ic-torreboldone.gov.it/ima...	Linux	mirror
2014/06/06	Hmei7			R	🇻🇳	★	www.viengiamdinhykhoa.gov.vn/q...	Linux	mirror
2014/06/05	Hmei7				🇹🇭	★	dmsc2.dmsc.moph.go.th/webroot/...	Win 2003	mirror
2014/06/05	Hmei7				🇺🇸	★	www.camaradebotelhos.mg.gov.br...	Linux	mirror
2014/06/05	Hmei7			R	🇧🇷	★	www.im.ufal.br/evento/geometri...	Linux	mirror
2014/06/05	Hmei7			R	🇺🇸	★	elcarmen.gob.ec/carmen/images/...	Linux	mirror
2014/06/04	Hmei7	H	M		🇪🇸	★	securityforum.eset.es	Linux	mirror
2014/06/04	Hmei7		M		🇪🇸	★	edu.eset.es/moodledata/id.php	Linux	mirror
2014/06/04	Hmei7		M		🇪🇸	★	eset.es/images/id.php	Linux	mirror
2014/06/04	Hmei7		M		🇪🇸	★	i.eset.es/pepe.php	Linux	mirror
2014/06/04	Hmei7	H	M		🇪🇸	★	eol.eset.es	Linux	mirror
2014/06/04	Hmei7		M	R	🇮🇹	★	www.ibpm.cnr.it/images/qq4.txt	Linux	mirror
2014/06/03	Hmei7			R	🇲🇿	★	www.cedimo.gov.mz/images/qq4.txt	Linux	mirror
2014/06/03	Hmei7				🇪🇸	★	descargas.eset.es/images/qq4.txt	Linux	mirror
2014/06/02	Hmei7			R	🇫🇷	★	sahand-ntoir.gov.ir/images/qq4...	Linux	mirror
2014/06/02	Hmei7		M		🇨🇭	★	www2.ilo.ch/oshenc/x.php	Linux	mirror
2014/06/02	Hmei7		M		🇨🇭	★	www2.ilo.int/oshenc/x.php	Linux	mirror
2014/06/02	Hmei7		M		🇨🇭	★	www2.ilo.org/oshenc/x.php	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

- Hackers are constantly researching for new vulnerabilities and attack vectors
- Attackers have copious time & patience
- We must be proactive – build security in
- We must think like an attacker
- We must be as knowledgeable

Thank You!

Watch SecureNinjaTV on www.youtube.com/Secureninja