



**“Infiltrare, Manipolare, Compromettere e Distruggere:
i Social Media come Campo di Battaglia”**

HACKINBO

I Social Media come Campo di Battaglia

→ Chi sono (in 60 secondi)

Andrea Zapparoli Manzoni

- Founder, CEO, **iDIALOGHI**
- «Cyberworld» WG Member at **OSN/Ce.Mi.S.S.**
- **APASS Board** Member / Information Warfare lead res.
- **Assintel Board** Member / ICT Security WG leader
- **Clusit Board** Member / lecturer (SCADA, Social Media Sec, Mobile, Anti-fraud, DLP, Cyber Intelligence...)
- Co-author of the **Clusit Report** (2012, 2013 and 2014)

iDIALOGHI



I Social Media come Campo di Battaglia

→ Chi sono (in altri 30 secondi)



<http://social.clusit.it/>

I Social Media come Campo di Battaglia

→ Chi sono (ultimi 30 secondi, giuro)



<http://clusit.it/rapportoclusit/>

I Social Media come Campo di Battaglia

→ Disclaimer

Le opinioni qui espresse sono quelle dell'Autore / Speaker e non riflettono le opinioni di CLUSIT, né quelle del gruppo di lavoro "Cyber World" OSN – Ce.Mi.S.S., né quelle delle Imprese private, delle Associazioni e delle Community di sicurezza con le quali sto lavorando e/o che sostengo.



I Social Media come Campo di Battaglia

→ Menu del giorno (andando di corsa)

- Cosa sono i Social... veramente ?
- I Social come armi, come campo di battaglia e come bersaglio
- I Social come C⁴ISR e canale di reclutamento per Hacktivist e Terroristi
- I Social come paradiso per il Cyber Crime
- SocMInt (Social Media Intelligence)
- Sorveglianza ,Spionaggio governativo e Cyber Offense: LEAs, 3-letters Agencies e militari
- Gatekeepers, PsyOps di massa, Rivoluzioni “colorate”, “Primavere”...
- Social Drones e la Internet of Bots
- Visioni dal futuro



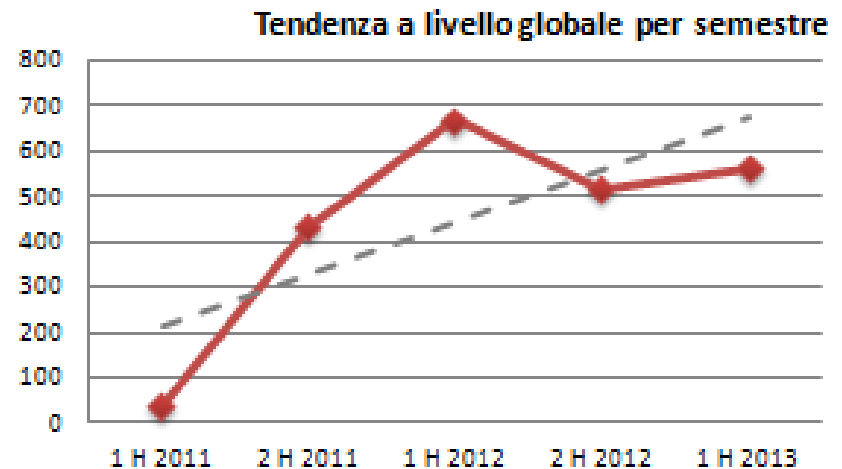
I Social Media come Campo di Battaglia

→ It's a Jungle Out There

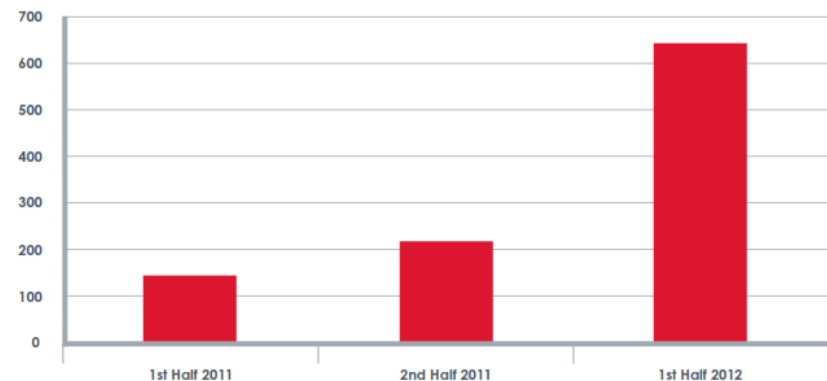
Nel **2012** le (sole) aziende private hanno speso globalmente **20 miliardi di USD** per sistemi di sicurezza “avanzata”, su un budget complessivo per l’ICT Security di **60 miliardi di USD**. Nel **2013** questa spesa è aumentata del **15%**, mentre le perdite causate da attacchi informatici sono aumentate del **26%**. **La cyber insicurezza è diventata la norma.**

Dalle analisi Clusit, che sono sostanzialmente in linea con quelle di altri osservatori (privati ed istituzionali), **la frequenza degli attacchi sui Social contro privati, aziende ed istituzioni a livello globale è aumentata del 660% tra il 2011 ed il 2013.**

➡ Che @#@#! succede ?



© Clusit - Rapporto 2013 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2013



© Clusit - Rapporto 2013 sulla Sicurezza ICT in Italia

I Social Media come Campo di Battaglia

→ Le dinamiche in atto

VITTIME PER TIPOLOGIA	2011	2012	2013	Variazioni 2013 su 2011
Institutions: Gov - Mil - LEAs - Intelligence	153	374	402	162,75%
Others	97	194	146	50,52%
Industry: Entertainment / News	76	175	147	93,42%
Industry: Online Services / Cloud	15	136	114	660,00%
Institutions: Research - Education	26	104	70	169,23%
Industry: Banking / Finance	17	59	108	535,29%
Industry: Software / Hardware Vendor	27	59	46	70,37%
Industry: Telco	11	19	19	72,73%
Gov. Contractors / Consulting	18	15	2	-88,89%
Industry: Security Industry:	17	14	6	-64,71%
Religion	0	14	7	-
Industry: Health	10	11	11	10,00%
Industry: Chemical / Medical	2	9	1	-50,00%
Critical Infrastructures	-	-	37	-
Industry: Automotive	-	-	17	-
Org / ONG	-	-	19	-



© Clusit - Rapporto 2014 sulla Sicurezza ICT in Italia

I Social Media come Campo di Battaglia

→ Cosa sono i Social Media... veramente?

*“I Social Media sono un insieme di piattaforme **Web 2.0** tramite le quali gli **utenti** interagiscono **direttamente**, producendo e condividendo **contenuti** propri e/o elaborando contenuti altrui, **in tempo reale**”.*

Questo è certamente vero, **però**...

- **Perché** sono per lo più gratuiti?
- Di **chi** sono? **Chi** li controlla?
- **Come** sono regolati contrattualmente?
- **Cosa** ci fanno con i **social graph**?
- E con i **dati** immessi dagli utenti?
- E con le **foto**?
- Sono “**filtrati**”?
- Sono “**neutrali**”?
- Sono “**liberi**”
- Sono “**sicuri**”?



I Social Media come Campo di Battaglia

→ Cosa sono i Social Media... veramente?



Si tratta di “popolazioni” molto diverse.... Ma rende bene l’idea....

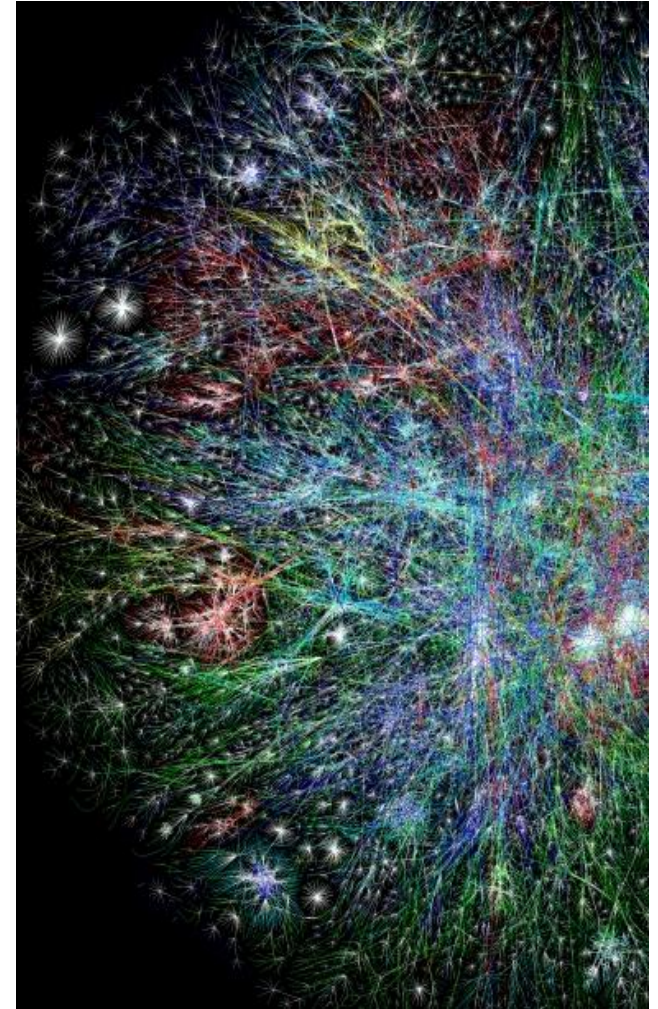
I Social Media come Campo di Battaglia

→ Gli attori e le forze in campo

La **prima** caratteristica della conflittualità portata nel cyberspazio è che gli attori si possono avvalere di uno **spettro molto ampio** di tecniche **alla portata di un numero crescente di attori**, che le applicano per **scopi**, **con modalità ed intensità variabili** e contro **ogni genere di bersaglio** (infrastrutture critiche, sistemi governativi, sistemi militari, aziende di ogni dimensione, banche, media, gruppi di interesse, privati cittadini, ...) **I Social oggi sono al primo posto come superficie di attacco.**

- Stati Nazionali (Mil)
- IC / LEAs
- Cybercrime organizzato
- Hacktivisti
- Spie industriali
- Terroristi
- Corporations
- Mercenari

Tutti contro tutti



I Social Media come Campo di Battaglia

→ I Social Media sono anche armi

Nel corso degli ultimi 3-4 anni i Social Media sono diventati **armi a tutti gli effetti**, e fanno ormai parte dell'arsenale di strumenti "cyber" a disposizione di **eserciti, servizi segreti, polizie, terroristi, mercenari, gruppi antagonisti e corporations**.

Alcuni fatti (noti) tra i più eclatanti:

- Utilizzati attivamente da **Anonymous, S.E.A.** e terroristi vari
- Utilizzati attivamente dai **Governi** (Iran, Siria, Cina, USA, UK, Francia, Russia, etc) e dai relativi **Servizi Segreti**
- Utilizzati come **C⁴ISR** ¹ dai **ribelli** delle "primavere arabe", in **Ucraina** (EuroMaidan), in **Venezuela**, in **Libia** dalle **Forze Speciali** (a supporto di operazioni **NATO**), etc
- Utilizzati da **Aziende** contro concorrenti ed attivisti

¹ Command, Control, Computers, Communications, Intelligence, Surveillance and Reconnaissance



I Social Media come Campo di Battaglia

→ I Social Media sono (quindi) un bersaglio

Essendo diventati a tutti gli effetti un' **arma** ed un **campo di battaglia**, i Social Media sono inevitabilmente anche diventati un **obiettivo**.

Questo significa che in qualsiasi momento potrebbero essere **attaccati**, **bloccati** e **resi irraggiungibili**, oppure più semplicemente **inutilizzabili**.

In effetti è **già successo**, a causa di:

- rivolte, insurrezioni e guerre civili
- attacchi cyber di vario genere e scopo
- azioni di sabotaggio e di protesta
- censura di Stato (Cina, Turchia, etc)

(Meglio non darli troppo per **scontati**)....



























I Social Media come Campo di Battaglia

→ I Social Media sono il Paradiso del Cyber Crime

Oggi i Social Media sono diventati una dei **principali terreni di caccia** per il **cybercrime organizzato trans-nazionale**, che ha raggiunto un “giro d'affari” nel 2012 (stimato) di **15-20 miliardi di dollari**, in crescita del **150%** sull'anno precedente.

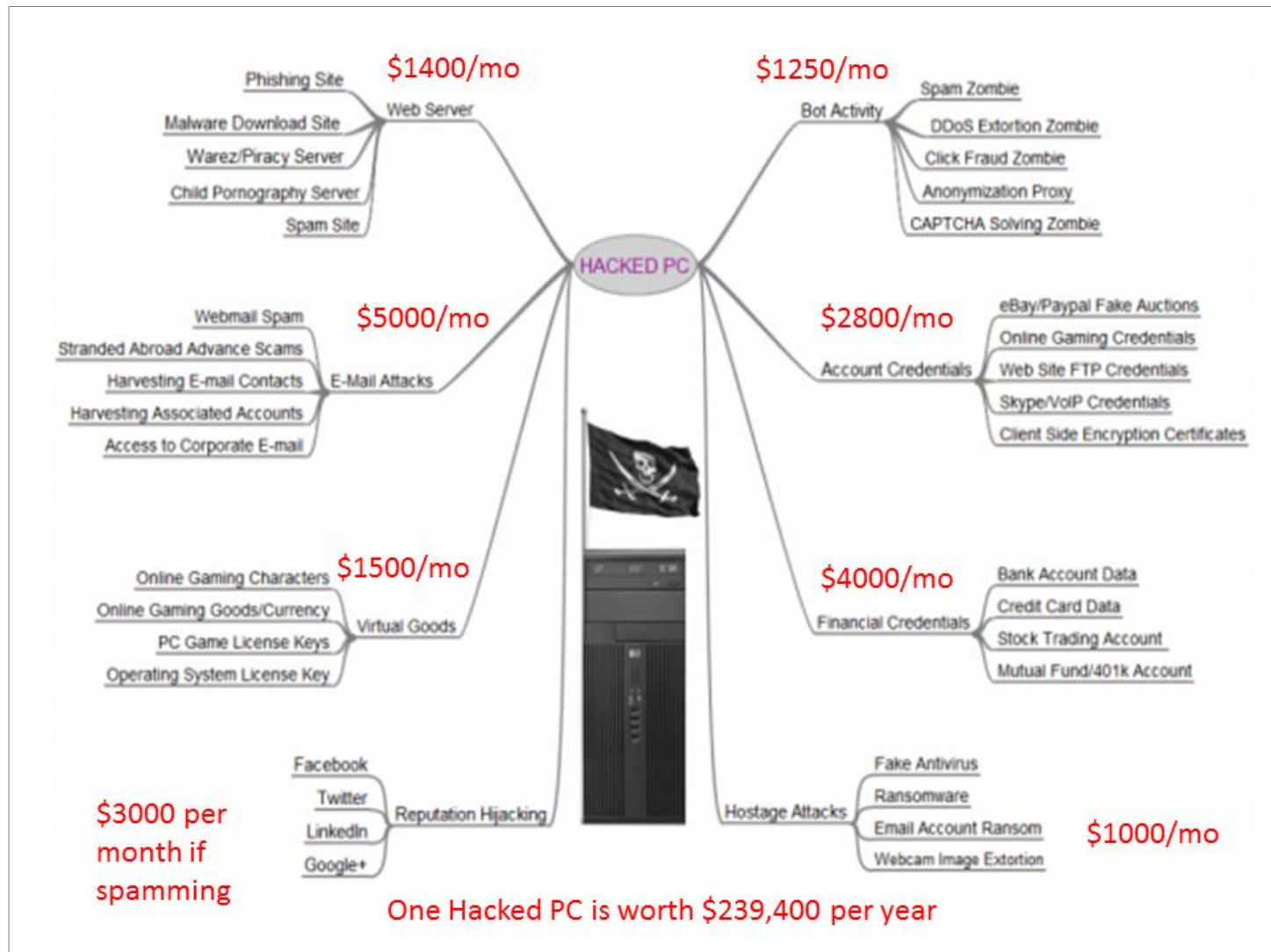
Il **costo totale worldwide del solo cyber crime** (perdite dirette, costi & tempo dedicati a rimediare agli attacchi) nel 2012 è stato stimato in **388 Md \$**, e quasi **500 Md \$** nel 2013. Se il trend continua, nel 2014 questi costi saranno pari a **metà del PIL italiano....**

Una quota **crescente** di queste perdite derivano dall'uso **sconsiderato e superficiale** dei social networks e dal fatto che i SN fanno “**security theater**”, non vera security. Di conseguenza, il **ROI** per gli attaccanti è **massimo**, ed i **rischi minimi**.

Date	Author	Description	Organization	Attack
PCS Consultants				
Aug 1		Another U.S. Government contractor, PCS Consultants gets hacked by Anonymous & Antisec. Hackers extract website Database and leak it on the internet via Twitter on Pastebin (as usual). Leaked data include Admins and 110 users' emails, plus passwords in encrypted hashes.		SQI?
Vitroclot				
Aug 2		72 hours after the first defacement, Vitroclot, a contractor of Italian Cyber Police, is hacked and defaced again by Anonymous.		SQI? Defacement
United Nations (Shady RAT)				
Aug 3		In an interview to Vanity Fair (as to say, information security is a fashion), a Mofee Security Researcher declares UN and other international institutions have been victims of a large scale Remote Access Tool based attack from a Foreign Country. The attack is dubbed shady RAT and suspects are directed to China.		Remote Access Tool
Colombia				
Aug 3		Anonymous and Colombian Hackers shut down the websites of Colombia's president, the interior and justice ministry, the intelligence service DAS and the governing party. The hacker attack was meant as a protest against government censorship.		DDoS
The Sun and News Corp. International				
Aug 3		Britain's Rupert Murdoch-owned tabloid The Sun sends a message to readers warning them that computer hackers may have published their data online after an attack on the paper's website last month. A hacker styled 'Baltag' claims to have posted details taken from The Sun on the Pastebin.		SQI?
Front National				
Aug 3		As a consequence of the Maitre de Ode, Anonymous France claims to have hacked a server belonging to Front National, leaking a list of 100 leaders of the party.		?
Citi Cards Japan (CitiGroup)				
Aug 5		Eight weeks after a hacker cracked its credit card database, the company's credit card unit in Japan, Citi Card, reported in a message to its user base that "certain personal information of 92,408 customers has allegedly been obtained and sold to a third party illegally." Estimated cost of the breach is about \$19.8 million.		unfaithful outsourcing
Law Enforcement Agencies				
Aug 6		After the first attack to Law Enforcement Institutions in July, Anonymous and LulzSec, as part of what they define the Shooingsheffsaturday, leak again 10 Gb of Data from the same Law Enforcement Agencies, including private police emails, training files, switch info and personal info. The attack was made in retaliation for anonymous arrests.		SQI?
SAPPE (Sindacato Autonomo Polizia Penitenziaria)				
Aug 6		Anonymous defaces the Web Site of SAPPE (Independent Union of Prison Guards) and leaves a message on Pastebin (hosted in Italian) claiming more rights for detainees.		SQI?
Polícia Federal (Brazilian Police)				
Aug 6		LulzSec Brazil hacks Brazilian Police and discloses a gp of data from what they defined the Pandora's Box.		USB Key Stolen?
Syrian Ministry of Defense				
Aug 7		The Syrian Ministry of defense is hacked by Anonymous which defaces the web site and post a note supporting the Syrian people.		Defacement
Anonplus (Anonymous Social Network)				
		In retaliation for the defacement of the Syrian		











I Social Media come Campo di Battaglia

→ Cosa fanno con un device compromesso ? Soldi !!



I Social Media come Campo di Battaglia

→ E con milioni di device compromessi ? Montagne di soldi !

Популярность HTTP доменов (HTTP Domain Popularity)		(Number of Passwords) ↓
Домен (Domain)		Количество паролей
 www.facebook.com		318121 (57.06%)
 login.yahoo.com		59549 (10.68%)
 accounts.google.com		54437 (9.76%)
 twitter.com		21708 (3.89%)
 www.google.com		16095 (2.89%)
 www.odnoklassniki.ru		9321 (1.67%)
 www.linkedin.com		8490 (1.52%)
 th-th.facebook.com		8008 (1.44%)
 agateway.adp.com		7978 (1.43%)
 vk.com		6867 (1.23%)
		Показать все (20)

Un po' di account in vendita su un (piccolo) forum russo: notare i domini

I Social Media come Campo di Battaglia

→ Per esempio....

PHISHING AD AGOSTO 2013

Target	Numero di rilevazioni
Facebook	339 961 838
Google	151 214 587
Yahoo	45 697 916
Amazon	30 924 913
Twitter	23 834 061
Apple	12 364 660
eBay	10 686 982

Kaspersky 2013

Massive German hack sees one fifth of population's passwords stolen

January 23, 2014

The passwords and other details of 16 million email users in Germany have been stolen– the equivalent of almost a fifth of the German population being at risk.

More than half of the hacked accounts ended in '.de,' the Internet country code for Germany.

Researchers and prosecutors found the hacked accounts while conducting research on a botnet, a network of computers infected with malware.

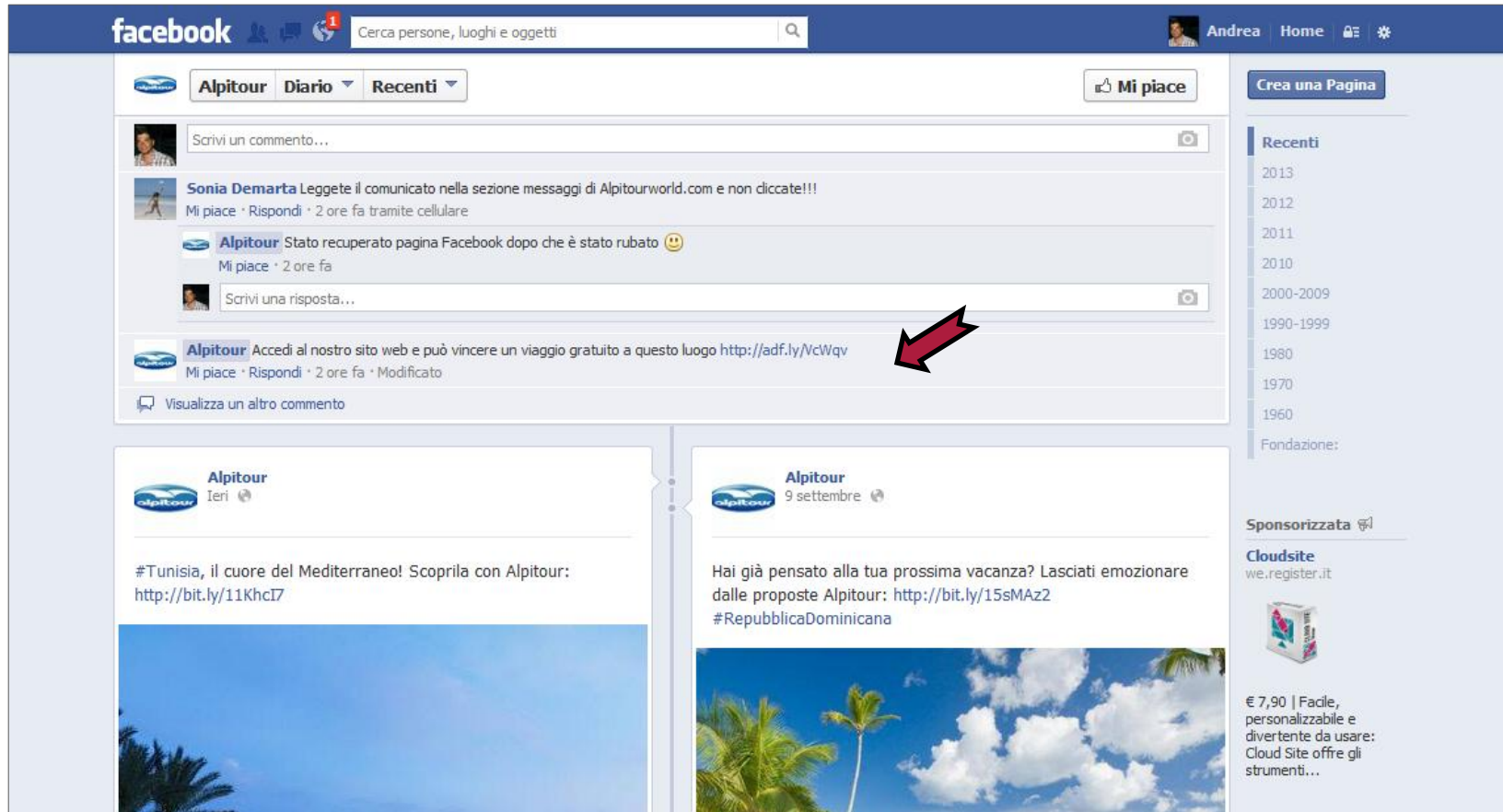
Germany's Federal Office for Information Security (BSI) has created a website to help people find out whether or not their e-mail was among those hacked.

...e in Italia ?

I Social Media come Campo di Battaglia

→ Conseguenze (esempio italiano)

L'attacco di Cybercriminali (egiziani) al Gruppo Alpitour su Facebook ha esposto **120.000 "friends"** (incluse numerose agenzie di viaggi) al malware Zeus per **50 ore**.



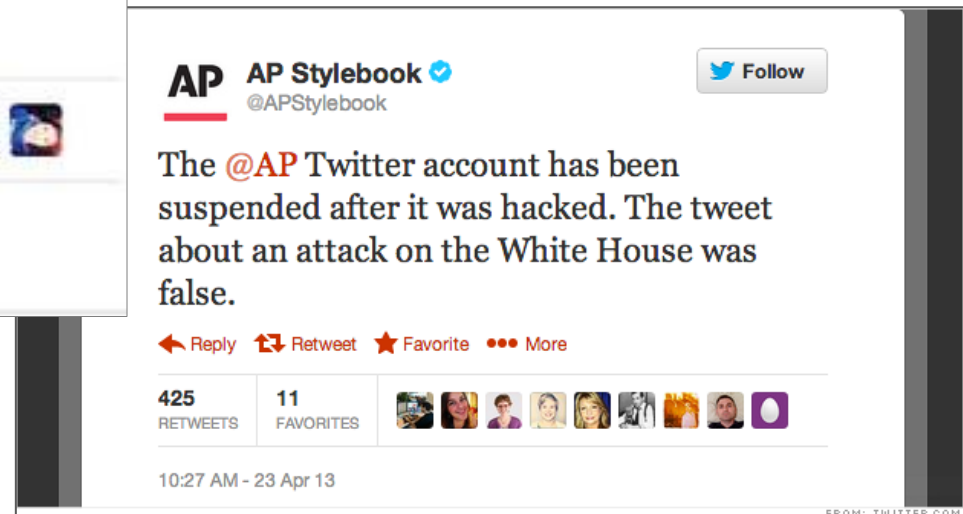
© 2014 iDIALOGHI Srl - Cyber Security Training & Consulting

I Social Media come Campo di Battaglia

→ Una dimostrazione di capability....



Hacktivism ? Hmmm.....

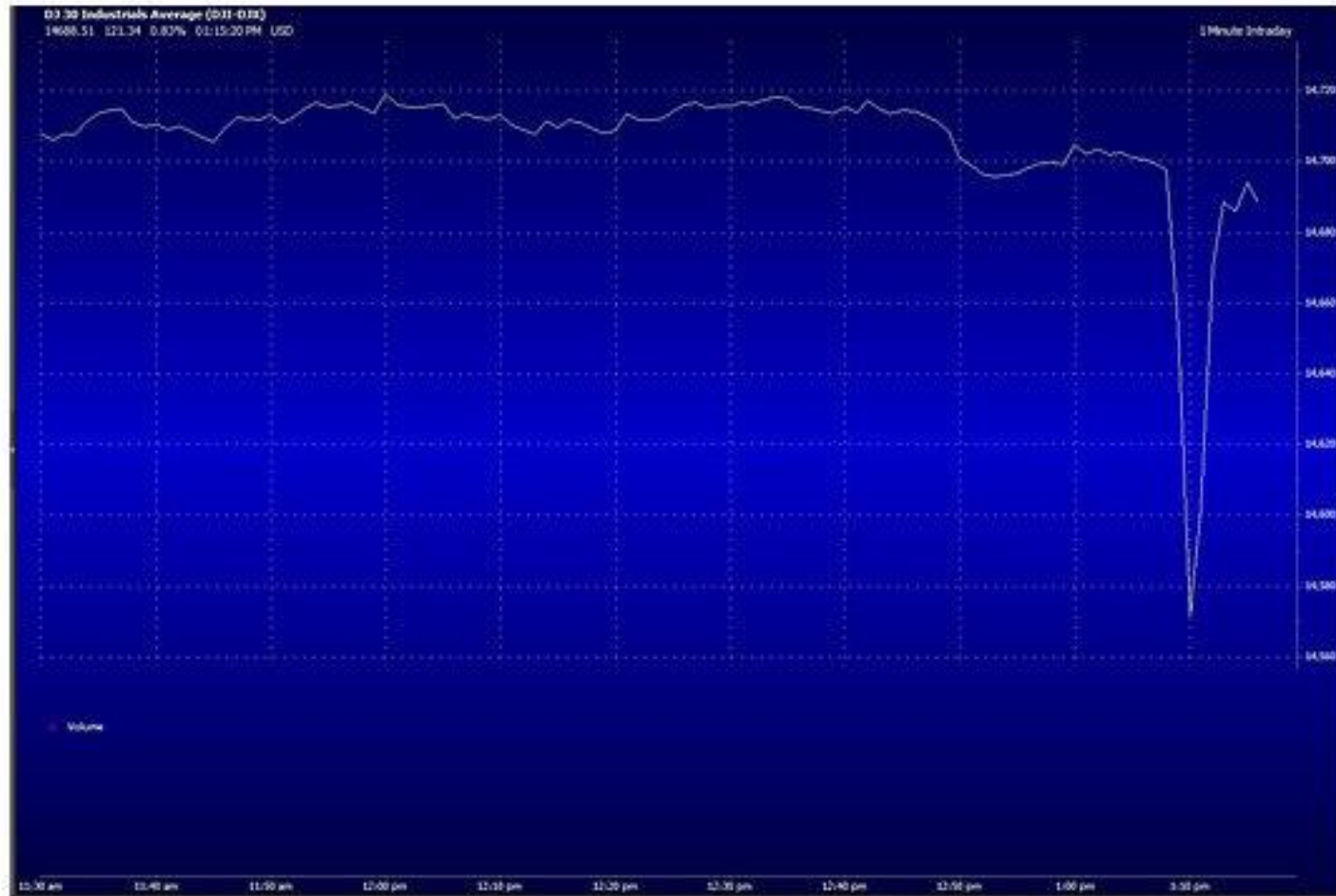


PsyOps via Twitter

(the “Syrian Electronic Army,” a pro-Assad mercenary group, hacked AP’s twitter account and then...)

I Social Media come Campo di Battaglia

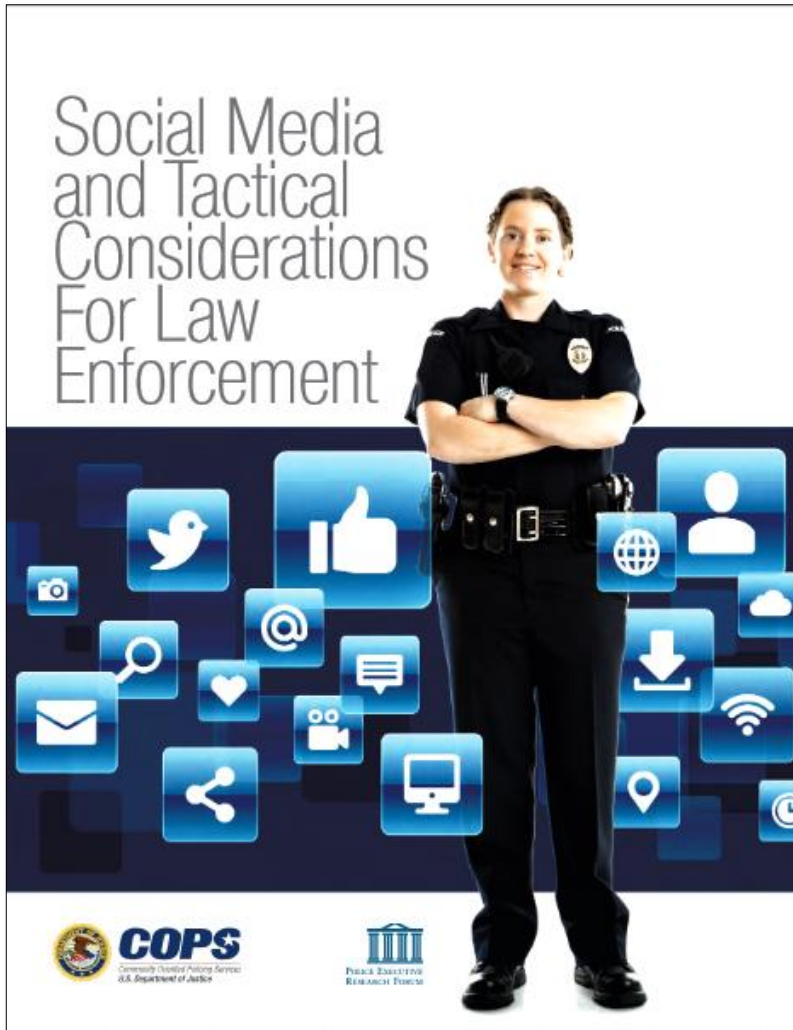
→ Che poteva causare danni molto maggiori...



L'hijacking dell'account Twitter dell'AP ha causato una perdita di **53Md \$** in 5 minuti

I Social Media come Campo di Battaglia

→ Governi: attività ufficiali...



**Privacy Compliance Review
of the
NOC Publicly Available Social Media Monitoring and
Situational Awareness Initiative**

November 8, 2012

**Contact Point
Donald Triner
Director, Operations Coordination Division
Office of Operations Coordination and Planning
202-282-8611**

**Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717**

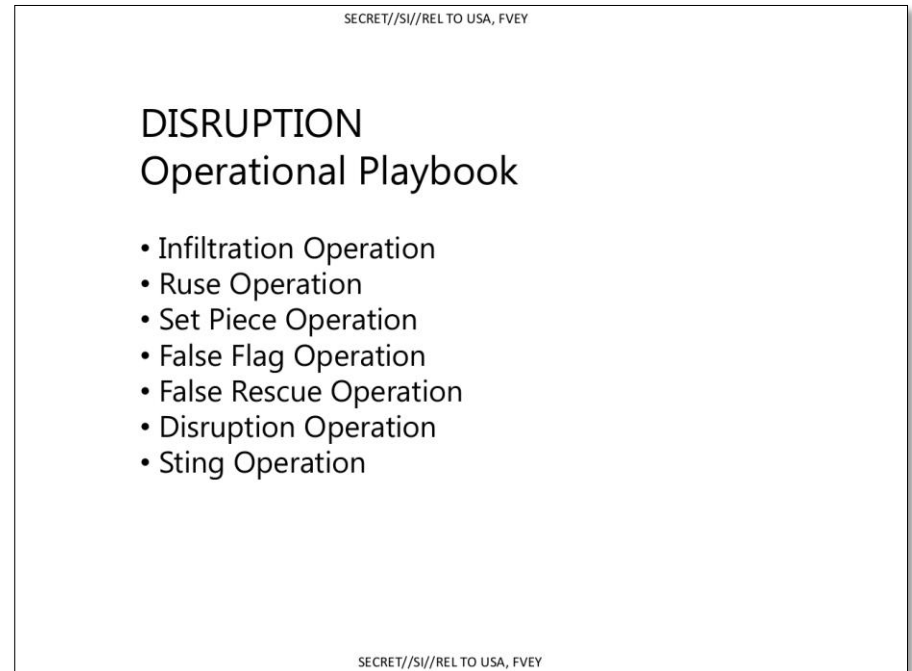
I Social Media come Campo di Battaglia

→ E attività non ufficiali...



Slide tratte da
“The Art of Deception:
Training for Online Covert Operations.”

Documento riservato del GCHQ leaked
da Edward Snowden.



I Social Media come Campo di Battaglia

→ E attività non ufficiali...

SECRET//SI//REL TO USA, FVEY

Gambits for Deception

Attention	Control attention Conspicuity & Expectancies	The big move covers the little move	The Target looks where you look	Attention drops at the perceived end	Repetition reduces vigilance
Perception	Mask/Mimic Eliminate - Blend Recreate - Imitate	Repackage/Invent Modify old cues Create new cues	Dazzle/Decoy Blur old cues Create alternate cues	Make the cue dynamic	Stimulate multiple sensors
Sensemaking	Exploit prior beliefs	Present story fragments	Repetition creates expectancies	Haversack Ruse (The Piece of Bad Luck)	Swap the real for the false, & vice versa
Affect	Create Cognitive Stress	Create Physiological Stress	Create Affective Stress (+/-)	Cialdini+2	Exploit shared affect
Behaviour	Simulate the action	Simulate the outcome	Time-shift perceived behaviour	Divorce behaviour from outcome	Channel behaviour

SECRET//SI//REL TO USA, FVEY

I Social Media come Campo di Battaglia

→ E attività non ufficiali...



Discredit a target

- Set up a honey-trap
- Change their photos on social networking sites
- Write a blog purporting to be one of their victims
- Email/text their colleagues, neighbours, friends etc

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

I Social Media come Campo di Battaglia

→ E attività non ufficiali...



Discredit a company

- Leak confidential information to companies / the press via blogs etc
- Post negative information on appropriate forums
- Stop deals / ruin business relationships

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

I Social Media come Campo di Battaglia

→ E attività non ufficiali...



EFFECTS: Definition



- “Using online techniques to make something happen in the real or cyber world”
- Two broad categories:
 - Information Ops (influence or disruption)
 - Technical disruption
- Known in GCHQ as Online Covert Action
- The 4 D's: Deny / Disrupt / Degrade / Deceive

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

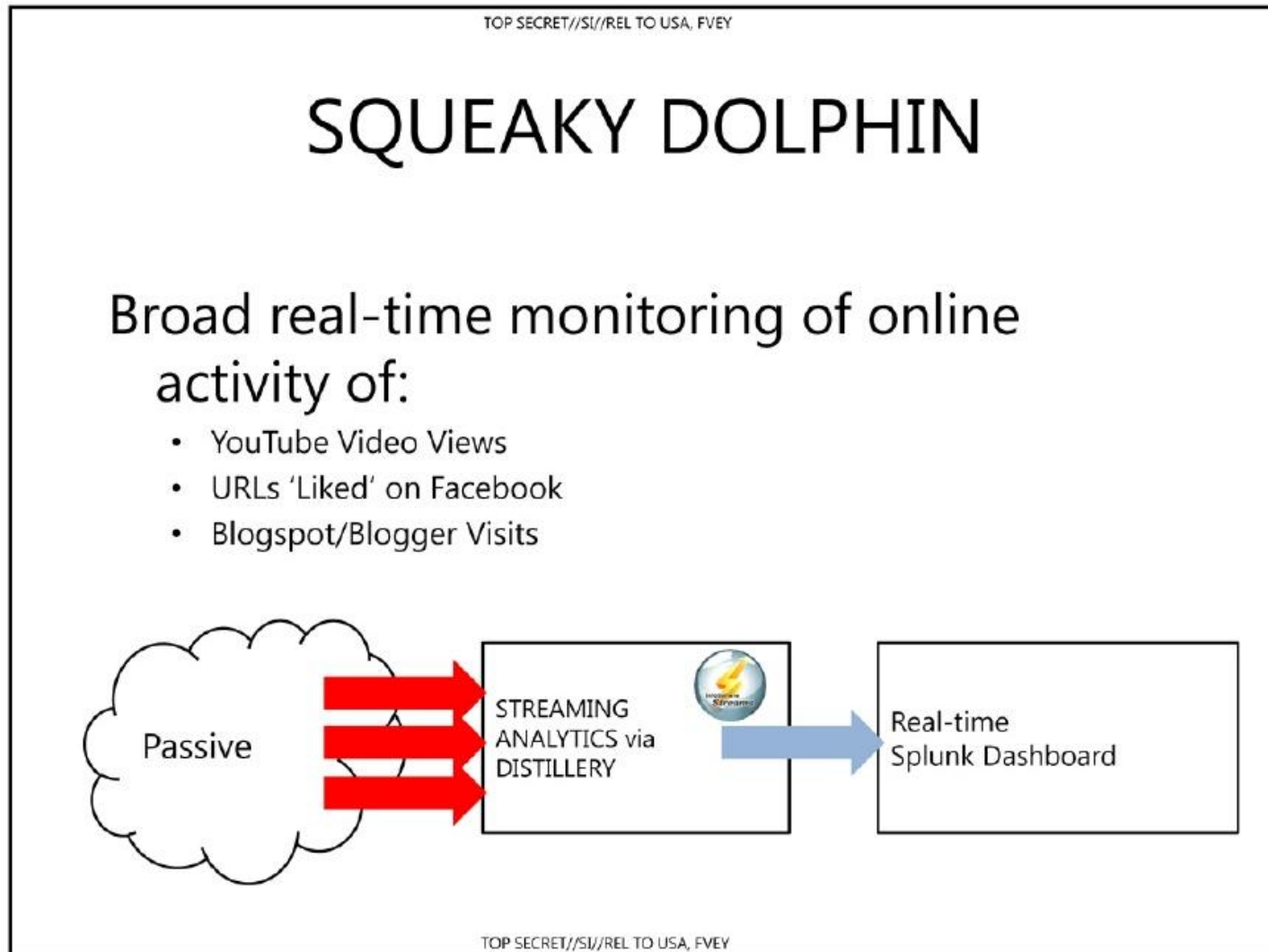
I Social Media come Campo di Battaglia

→ E attività non ufficiali...



I Social Media come Campo di Battaglia

→ E attività non ufficiali...



I Social Media come Campo di Battaglia

→ E attività non ufficiali...

TOP SECRET//COMINT//REL TO USA, FVEY



Golden Nugget!

Perfect Scenario – Target uploading photo to a social media site taken with a mobile device.

What can we get?



TOP SECRET//COMINT//REL TO USA, FVEY

1

I Social Media come Campo di Battaglia

→ Social Drones e la Internet of Bots

L'Italia rappresenta oggi uno dei primi 10 paesi al mondo per utilizzo dei Social Network (ad esempio, ci sono oltre 20 milioni di account Facebook italiani, *in teoria* il 37% della popolazione).

A black rectangular box containing green text that reads: "Wake up Neo", "The Matrix has you...", "Follow the white rabbit...", "Knock knock Neo."

Ma il **30% dei contenuti presenti sui Social sono gestiti da “bot”**, al servizio di aziende ed organizzazioni che li fanno interagire con i membri umani per finalità di **marketing, di intelligence e di social engineering / influence / psyops**.

I migliori tra questi bot sono ormai indistinguibili dagli utenti reali (non che ci voglia molto 😊)

Chi analizza questa enorme quantità di **relazioni**, di **conversazioni** e di **concetti**?

E' possibile **manipolare la percezione e l'interpretazione della realtà** sistematicamente e su larga scala tramite SN, al fine di **influenzare e controllare la popolazione**?

(Risposta: SI, guardatevi intorno)



I Social Media come Campo di Battaglia

→ Thank you!



Andrea Zapparoli Manzoni
a.zmanzoni@idialoghi.com