econocom

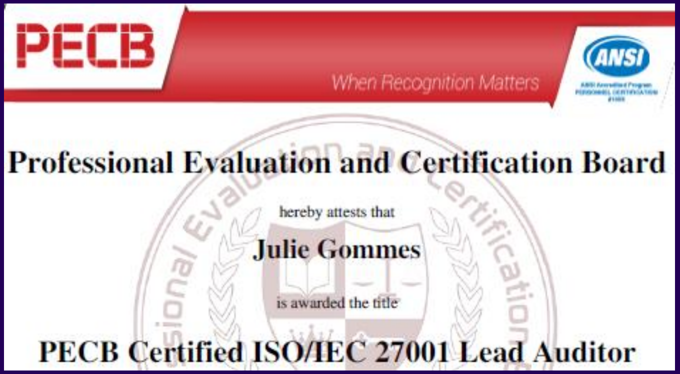
Jihadism and cryptography

From internet to softwares

Julie Gommes

Vienna

November 2015



PECB

When Recognition Matters

ANSI

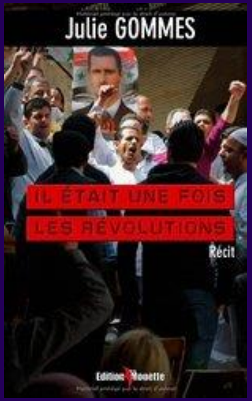
Professional Evaluation and Certification Board

hereby attests that

Julie Gommes

is awarded the title

PECB Certified ISO/IEC 27001 Lead Auditor



Julie Gommes

- IT Security and governance consultant
  - Risk analysis
  - 27001 audits
  - Risk management
- Lived/worked in Egypt, Syria, Soudan, Liban, Tunia…
- Researching on jihadist networks from years
- Find me there :

Jujusete on IRC (freenode, geeknode, europnet…)

@JujuSete on Twitter

https://fr.linkedin.com/in/juliegommes

Previous talks and trainings

How NGOs can encrypt their communication - Ritimo - Paris, Sept. 15

Social networks, practices and issues for NGOs - Ritimo - Paris, may 15

Free softwares, alternatives to Skype, google, Dropbox and others

Ritimo - Paris, may 2015

Information Security for journalists

HITBSecConf – Amsterdam, may 14 / DefCamp – Bucarest, oct. 14 /

MRMCD – Darmstadt, sept. 14 / PSES – Paris, june 14 / NDH (Workshop) – Paris, june 14

Free software and (h)activism - Ritimo – feb. 2014

Social engineering for journalists NDH – Paris, june 13 / Ubuntu party – Paris, may 13

Today ?

First part : starting point of the study

terms and definitions

developpment of websites in french language

developpment of twitter acounts

Second part : Let's talk about Crypto

From Moudjahdin Secret until today

New tools, focused on smartphones

After Paris, what about now ?

Third part : crypto tools

(maybe) Not westerns

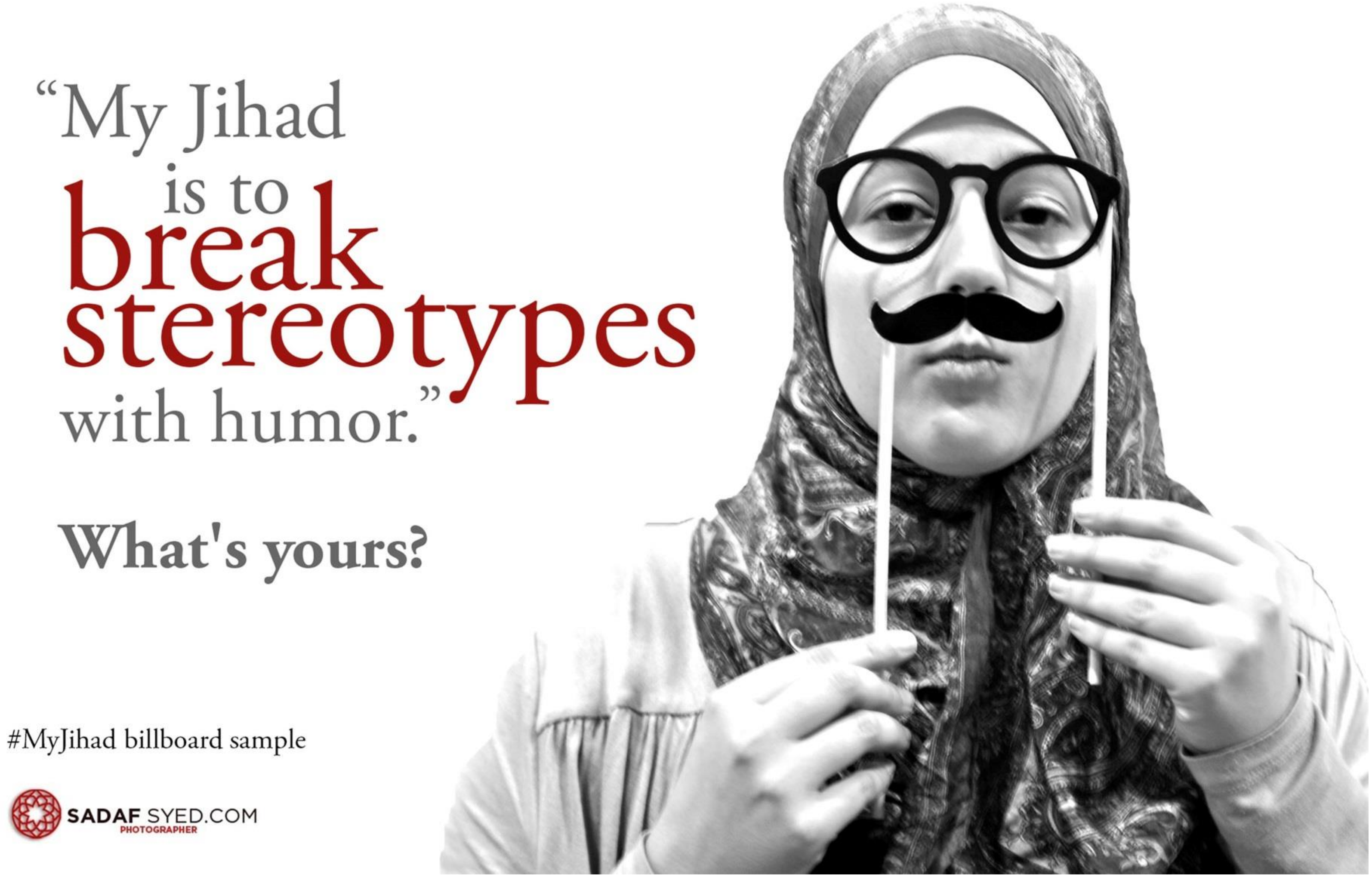
When crypto need religios validating

Terms et définitions

- Jihad
- Cryptojihad
- Terrorism
- Wikiterrorism

Terms and definitions 1/3

- **Jihad**



Terms et definitions 2/3

- **Cryptodjihad**
  - Using encryption / cryptography in order to perform jihad.
- **Terrorism** (not used here)
  - Using fear to put political, religious, idéological presure.
  - So many definitions (109 different according to Wikipedia) they vary on: the use of violence, the technics used, the nature of the subject, the level of organization, etc. In many definitions also involved the criterion of the number of victims.

Terms and definitions 3/3

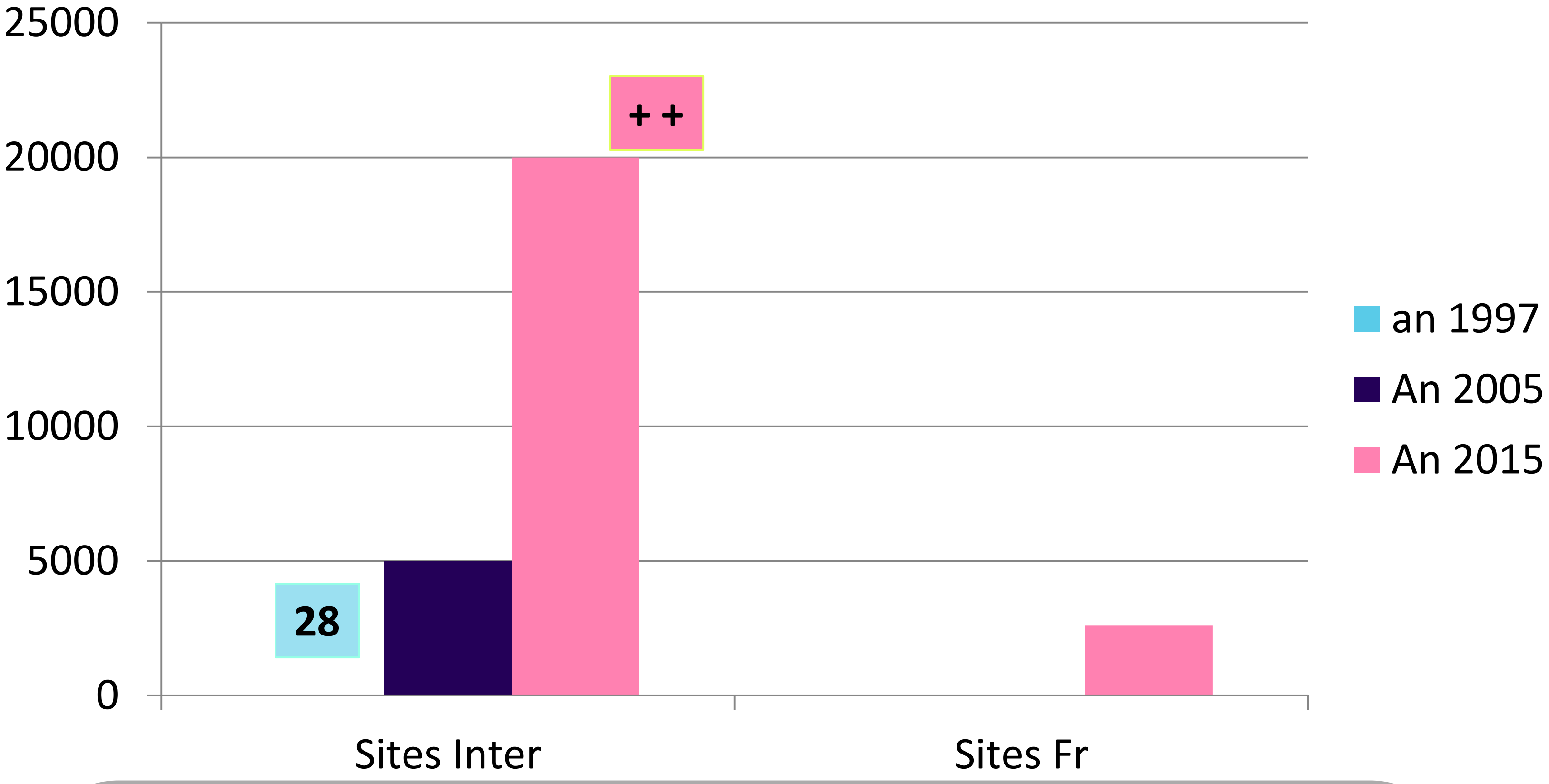
- **Wikiterrorism**
  - Term created by the geopolitical researcher Marc Hecker, working on terrorism and social networks at IFRI. (wich is include in The Three Ages of terrorism)
  - Using/creation of decentralized networks (online, humans, etc.), based on communication and where everyone contributes.
  - This helps to cover their tracks while extending an "ideal" but the other side is that those contributions are very inqual.

Starting point

Evolution

- Number of websites in french languages vs international
- Number of twitter account and what does that mean

Evolution of pro-jihad websites



Sources : http://www.lemonde.fr/proche-orient/article/2015/06/01/l-etat-islamique-compte-2-8-millions-de-francophones-sur-twitter_4645047_3218.html

http://www.lefigaro.fr/actualite-france/2008/11/07/01016-20081107ARTFIG00006-l-inquietante-propagande-islamiste-sur-internet-.php

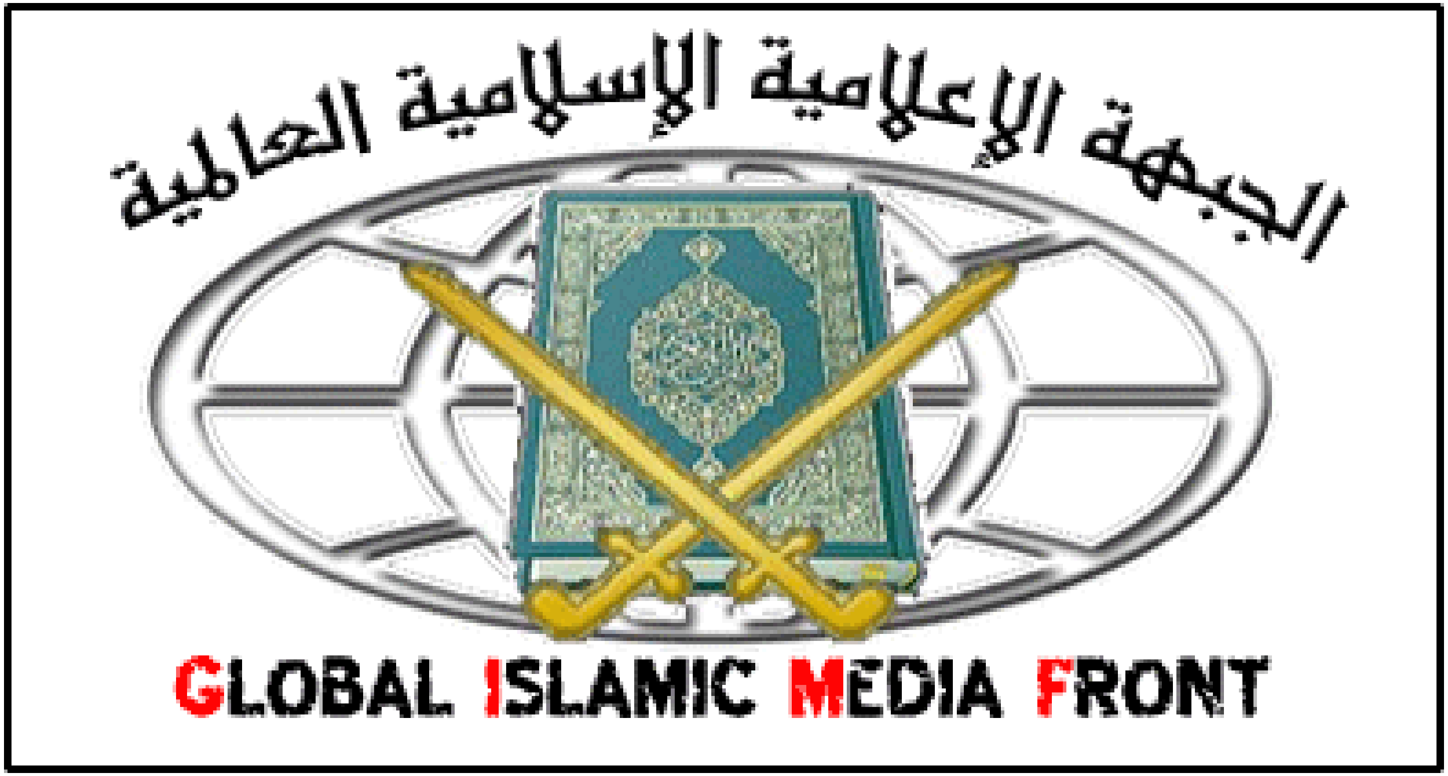
Sites and forums in french language

- Ansar Al Haqq, most famous forum (from december 2006)
  - From 2006 to 2011, 50.000 messages
  - 2010 Some members and the admin where arrested
- Assabyle => ribaat.org
- Le jardin des croyantes (Only for women)
- Nida Al Tawhid

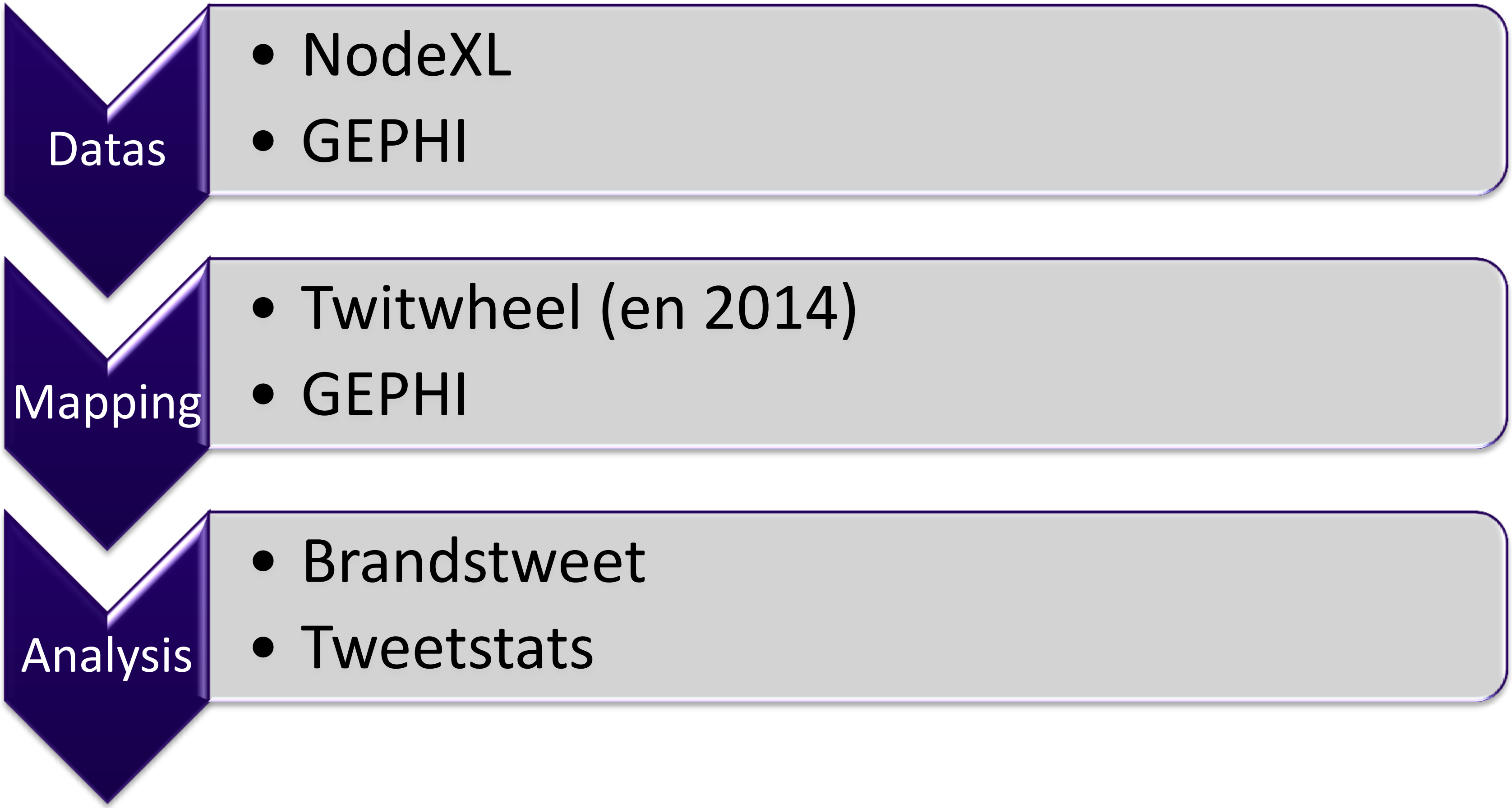
Most famous plateforms are the one wich are supported by ground organizations

Solid tools for communication

- Al Farg Media Center and Global Islamic Media Forum (GIMF)


الجبهة الإعلامية الإسلامية العالمية
GLOBAL ISLAMIC MEDIA FRONT

Tools I used



Datas

- NodeXL
- GEPHI

Mapping

- Twitwheel (en 2014)
- GEPHI

Analysis

- Brandstweet
- Tweetstats

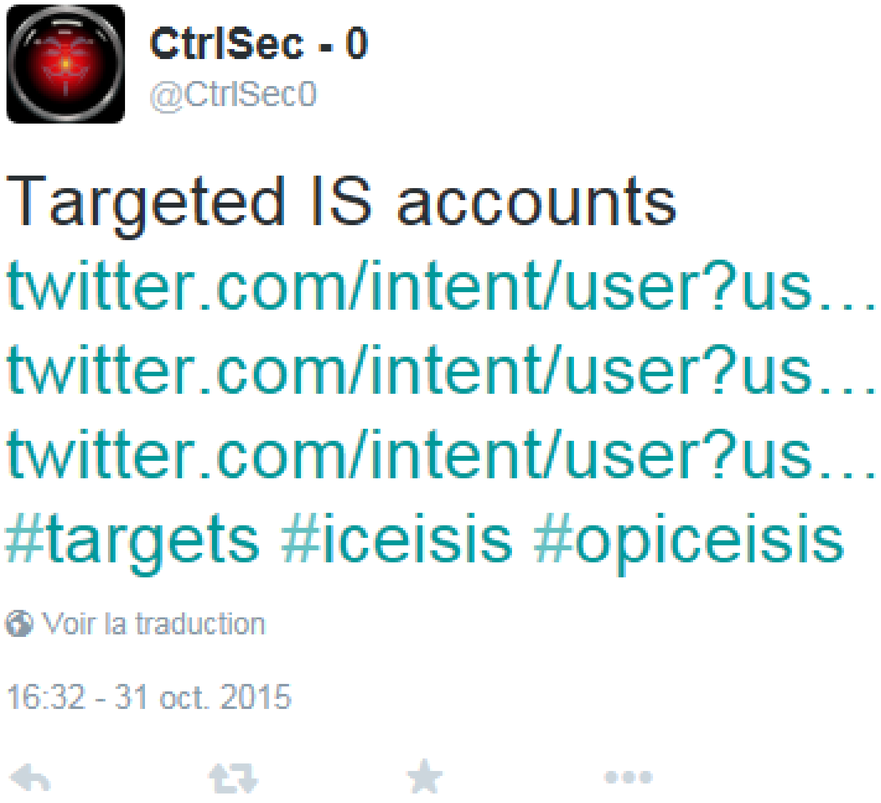
Evolution of twitter accounts 1/2

- September and décember 2014, 46 000 and 90 000 Twitter accounts were used to broadcast ISIS propaganda
- First geolocalisation is **Saoudi Arabia**, before Syria, Iraq, USA, Egypt and Koweït
- **Arabic** is the most used language bi pro-jihad accounts on Twitter (**73 %**), before english (18 %) and french (6 %)
- Every accound is folled by a thousand account

Sources : brookings.edu

Evolution of twitter accounts 2/2

- From mars 2015, « Anonymous » publish on @CtrlSec0 account a list of pro-ISIS accounts
- They've annonced 9200 accounts but new messages are already published



CtrlSec - 0
@CtrlSec0

Targeted IS accounts
twitter.com/intent/user?us…
twitter.com/intent/user?us…
twitter.com/intent/user?us…
#targets #iceisis #opiceisis

Voir la traduction

16:32 - 31 oct. 2015

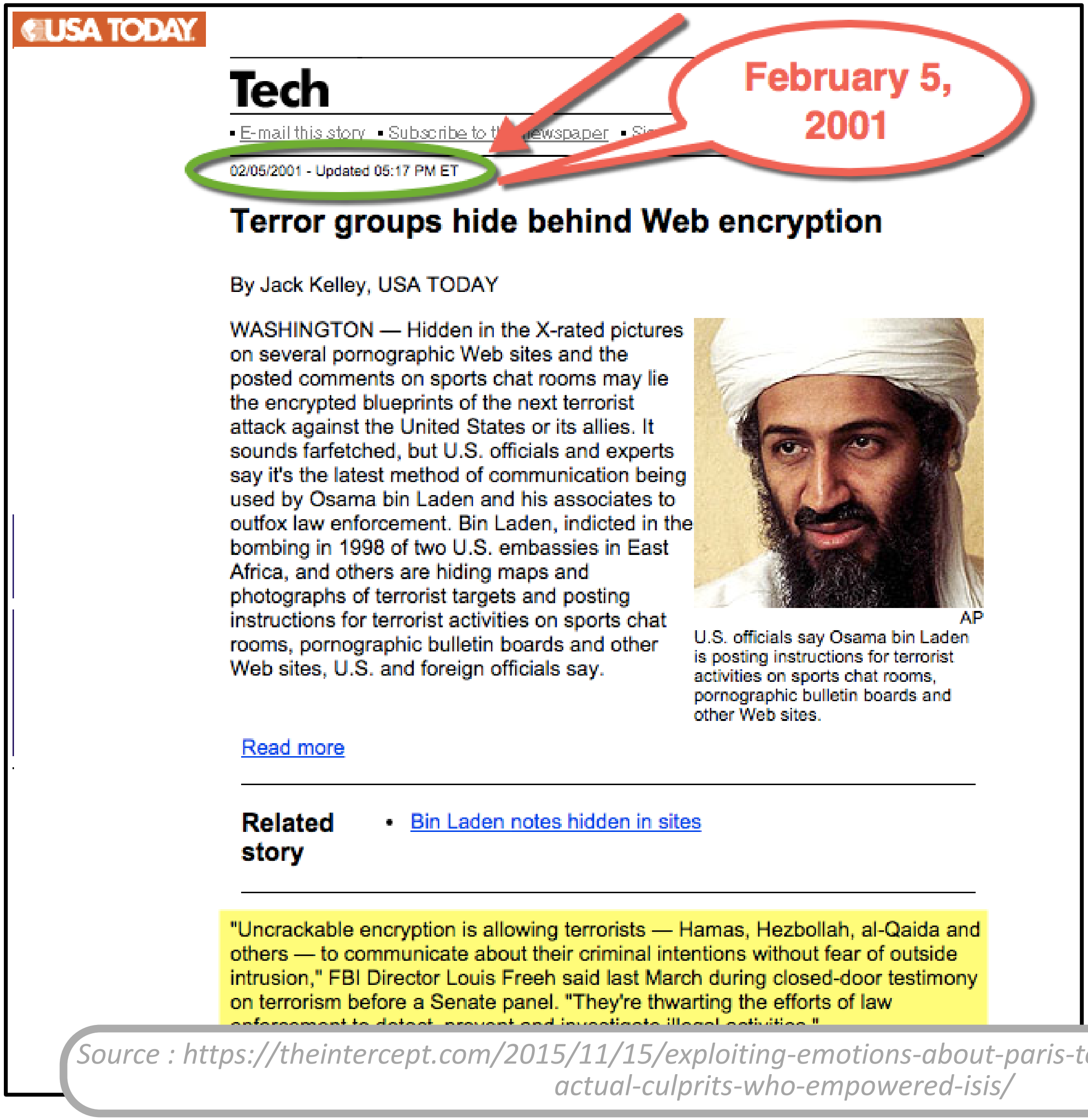
I used those accounts to renew my study

Let’s talk about encryption

- From Moudjahdin secret until today
- More and more smartphone tools
- After Paris, what about now ?

Once upon a time…

The Intercept_



USA TODAY

Tech

▪ E-mail this story ▪ Subscribe to the newspaper ▪ Si

02/05/2001 - Updated 05:17 PM ET

February 5, 2001

Terror groups hide behind Web encryption

By Jack Kelley, USA TODAY

WASHINGTON — Hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may lie the encrypted blueprints of the next terrorist attack against the United States or its allies. It sounds farfetched, but U.S. officials and experts say it's the latest method of communication being used by Osama bin Laden and his associates to outfox law enforcement. Bin Laden, indicted in the bombing in 1998 of two U.S. embassies in East Africa, and others are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites, U.S. and foreign officials say.

AP

U.S. officials say Osama bin Laden is posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites.

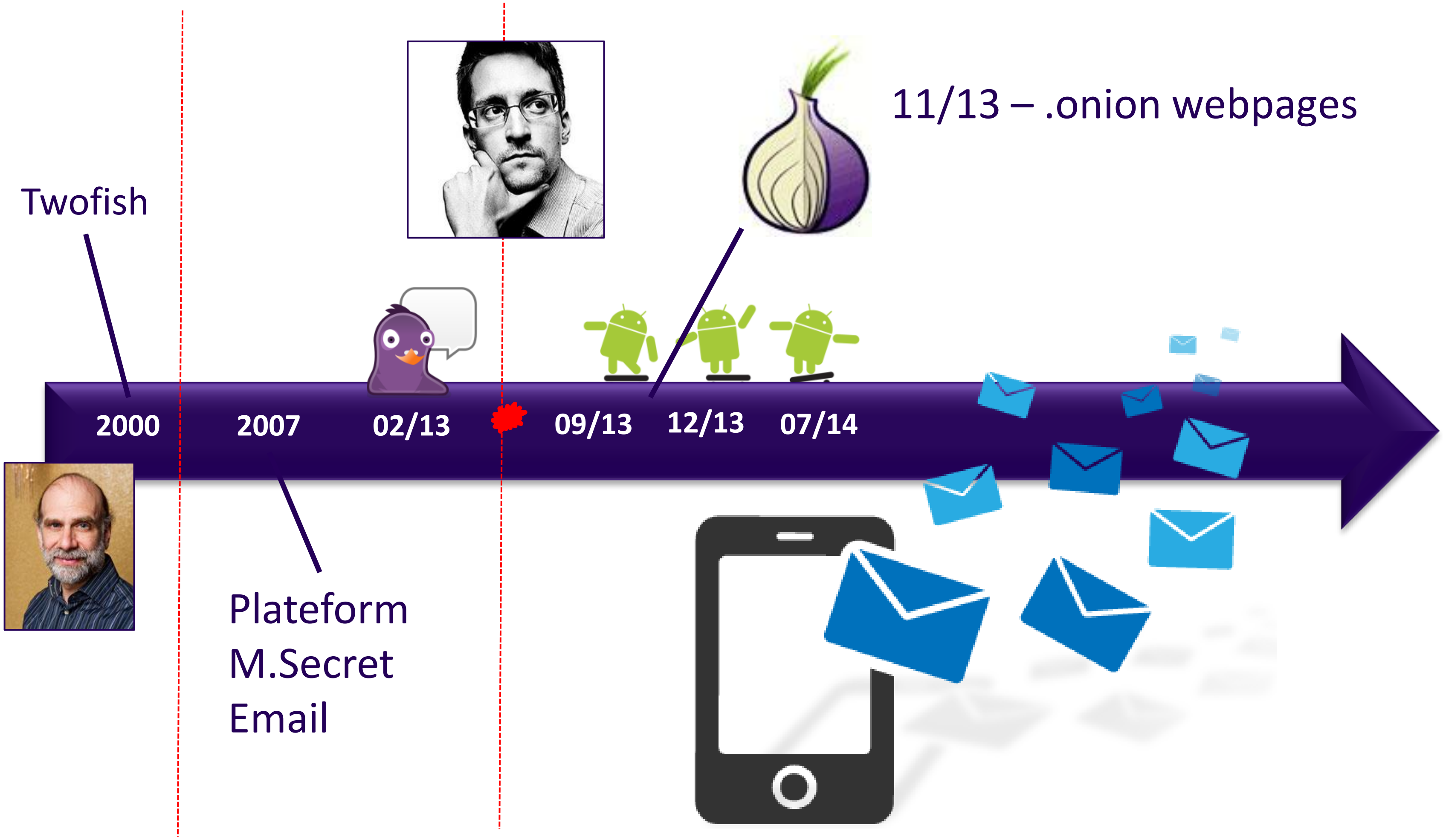
Read more

Related story • Bin Laden notes hidden in sites

"Uncrackable encryption is allowing terrorists — Hamas, Hezbollah, al-Qaida and others — to communicate about their criminal intentions without fear of outside intrusion," FBI Director Louis Freeh said last March during closed-door testimony on terrorism before a Senate panel. "They're thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities."

Source : https://theintercept.com/2015/11/15/exploiting-emotions-about-paris-to-blame-snowden-distract-from-actual-culprits-who-empowered-isis/

From M. Secret to today



Twofish

2000

2007

02/13

09/13

12/13

07/14

11/13 – .onion webpages

Plateform
M.Secret
Email

Sources : études du Middle East Media Research Institute (MEMRI), http://www.lefigaro.fr/international/2007/07/06/01003-20070706ARTFIG90133-secrets_de_moudjahidins_le_programme_de_cryptage_des_terroristes.php

More and more smartphone tools

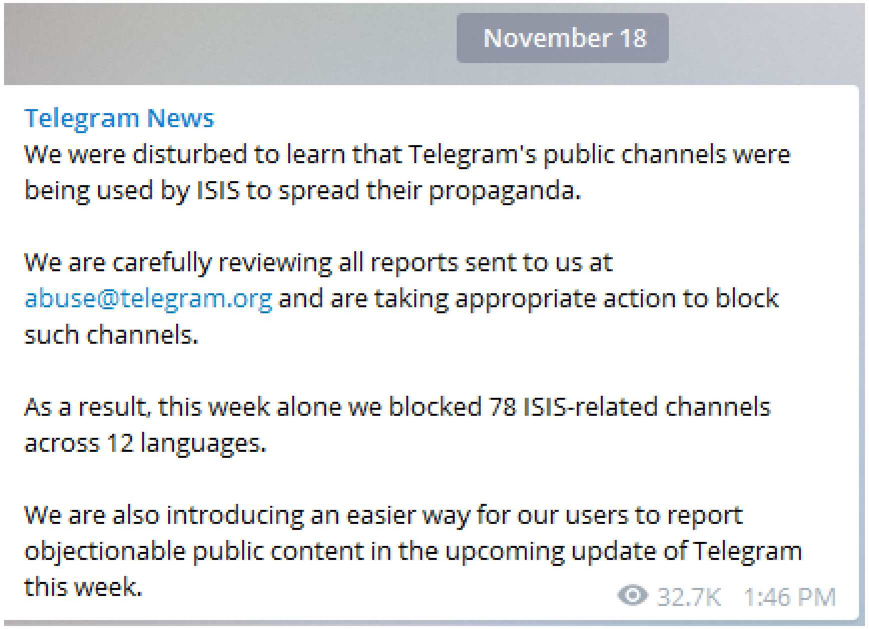
- Some people does not have Internet at home in some countries
- Easyer for instant messaging
- Wikiterrorism => more and more people, younger… (as WhatsApp users in Belgium a few mounths ago)
- Zapping culture

- New security risks for jihadists :
  - geolocalisation
  - Loack of control

After Paris, What about now?

Telegram:
(10 bilion messages daily)

They could still establish private connections, Telegram admitted that it is not able to block communications that happen in private groups, which can include up to 200 users.



November 18

Telegram News

We were disturbed to learn that Telegram's public channels were being used by ISIS to spread their propaganda.

We are carefully reviewing all reports sent to us at abuse@telegram.org and are taking appropriate action to block such channels.

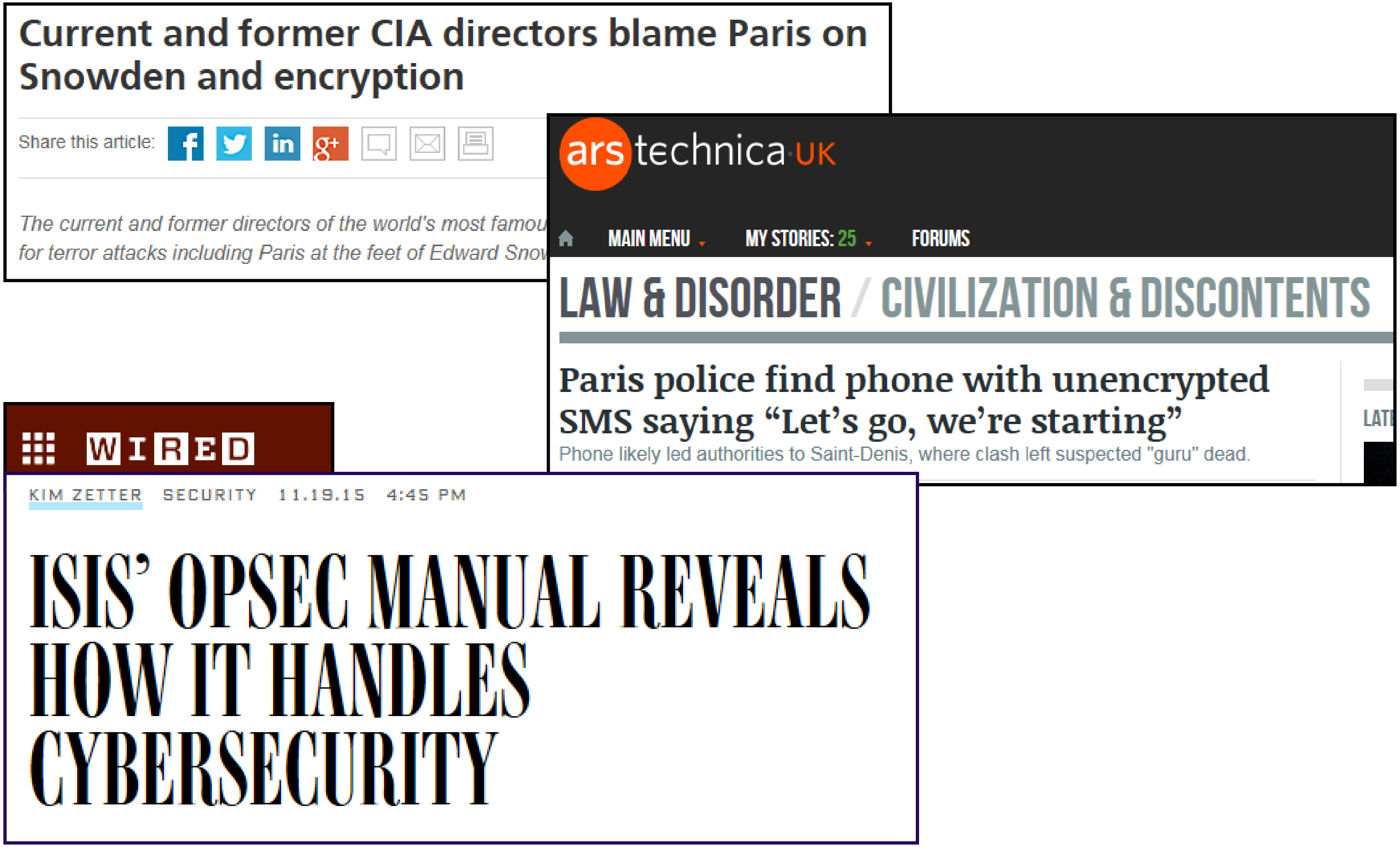
As a result, this week alone we blocked 78 ISIS-related channels across 12 languages.

We are also introducing an easier way for our users to report objectionable public content in the upcoming update of Telegram this week.

"All Telegram *chats and group chats are private amongst their participants," Telegram's spokesperson wrote. "We do not process any requests related to them." (Telegram co-founder - Pavel Durov)*

(securityaffairs.co, yesterday)

After Paris, What about now?



Current and former CIA directors blame Paris on Snowden and encryption

Share this article:

The current and former directors of the world's most famou for terror attacks including Paris at the feet of Edward Snov

ars technica UK

MAIN MENU MY STORIES: 25 FORUMS

LAW & DISORDER / CIVILIZATION & DISCONTENTS

Paris police find phone with unencrypted SMS saying "Let's go, we're starting"

Phone likely led authorities to Saint-Denis, where clash left suspected "guru" dead.

LATE

WIRED

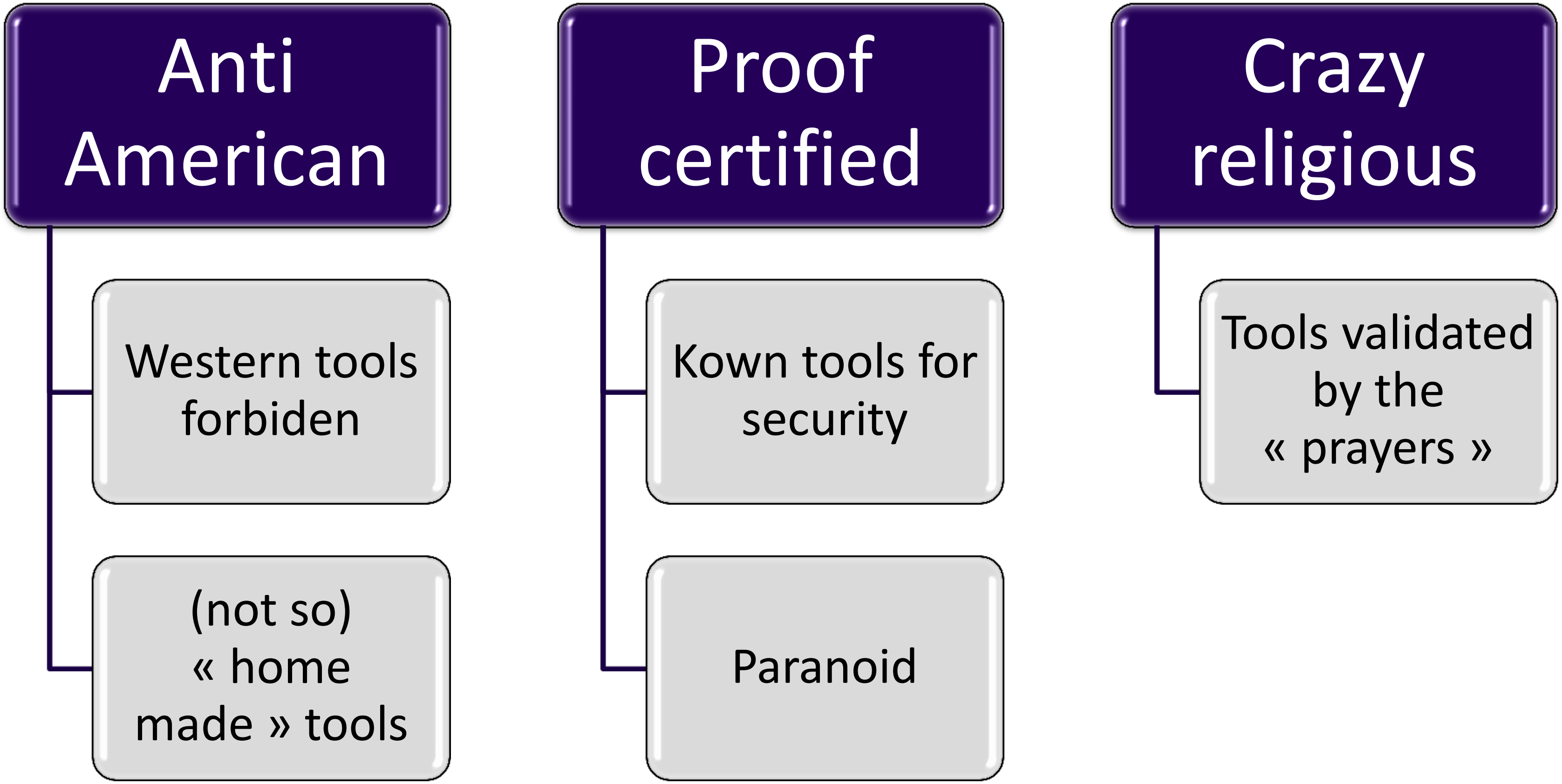
KIM ZETTER SECURITY 11.19.15 4:45 PM

ISIS' OPSEC MANUAL REVEALS HOW IT HANDLES CYBERSECURITY

Tools

- Tools means identity
- (maybe) not western tools
- Home made tools validated by « god »

Groups definitions by tools they're using



Anti American

- Western tools forbiden
- (not so) « home made » tools

Proof certified

- Kown tools for security
- Paranoid

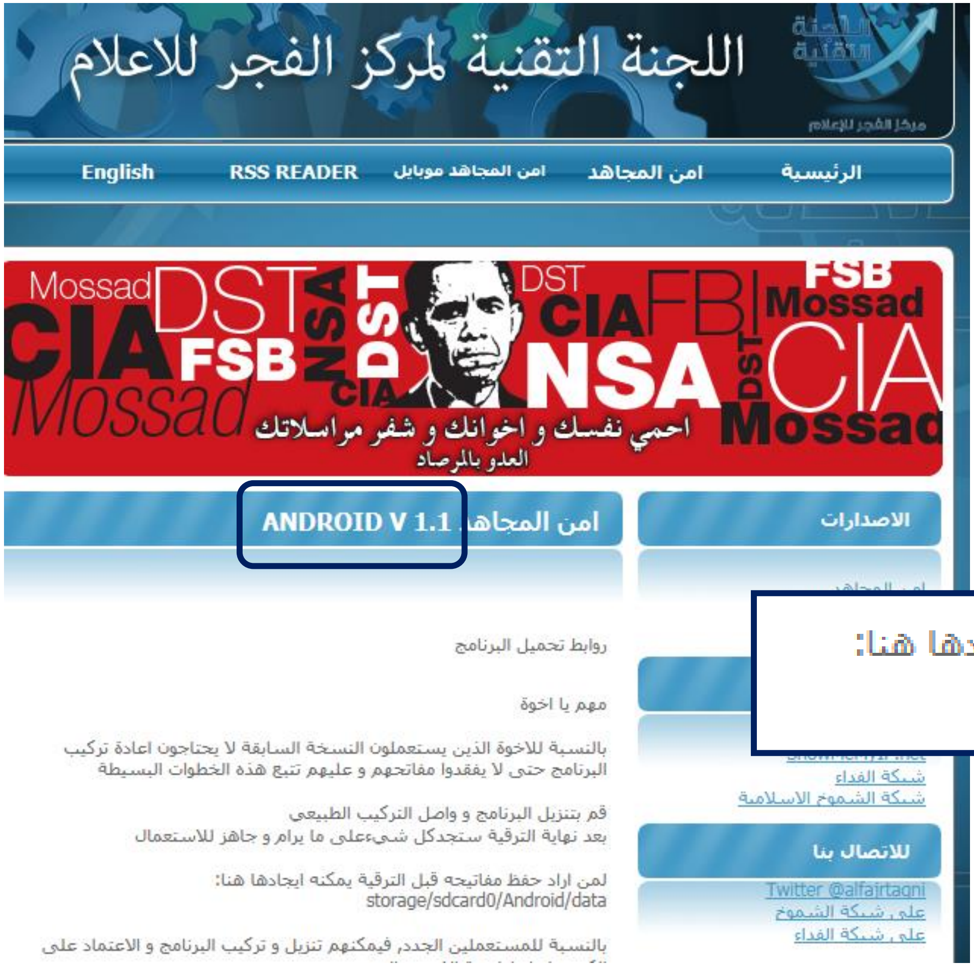
Crazy religious

- Tools validated by the « prayers »

one tool = one group

Dévôts

Outils « validés »



روابط تحميل البرنامج

مهم يا اخوة

بالنسبة للاخوة الذين يستعملون النسخة السابقة لا يحتاجون اعادة تركيب البرنامج حتى لا يفقدوا مفاتحهم و عليهم تتبع هذه الخطوات البسيطة

قم بتنزيل البرنامج و واصل التركيب الطبيعي
بعد نهاية الترقية ستجدكل شيءعلى ما يرام و جاهز للاستعمال

لمن اراد حفظ مفاتيحه قبل الترقية يمكنه ايجادها هنا:
storage/sdcard0/Android/data

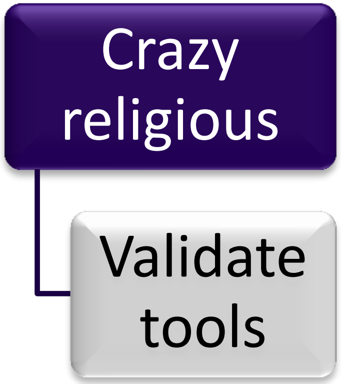
بالنسبة للمستعملين الجدد, فيمكنهم تنزيل و تركيب البرنامج و الاعتماد على

لمن اراد حفظ مفاتيحه قبل الترقية يمكنه ايجادها هنا:
storage/sdcard0/Android/data

Source : http://alfajrtaqni.net/amm.html

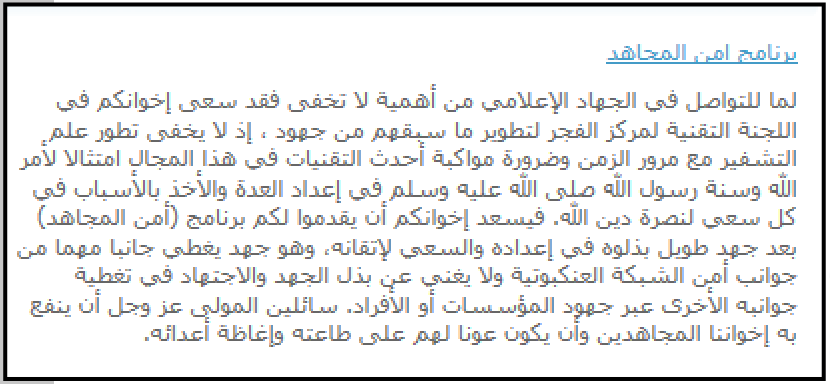
One tool = one group

- "Cryptography is changing, time passes and we must apply the changes in technology in this area with the command of Allah and the Sunnah of the Messenger of Allah peace be upon him"



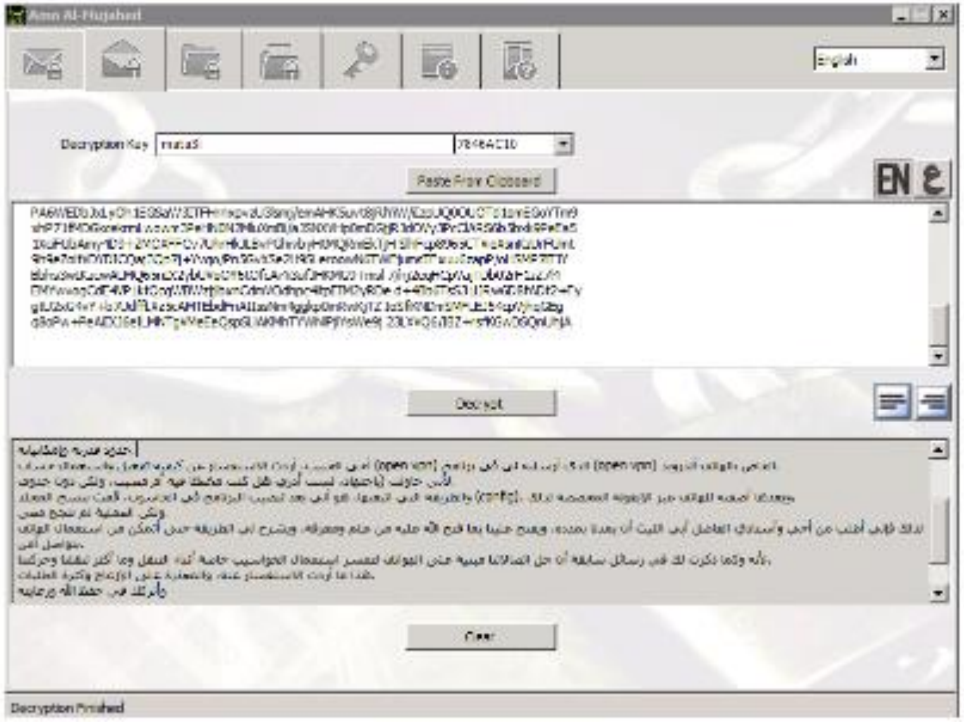
Crazy religious

Validate tools



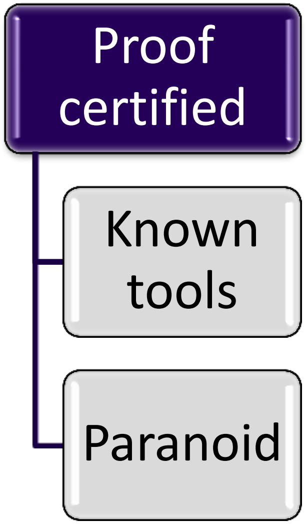
برنامج امن المجاهد

لما للتواصل في الجهاد الإعلامي من أهمية لا تخفى فقد سعى إخوانكم في اللجنة التقنية لمركز الفجر لتطوير ما سبقهم من جهود ، إذ لا يخفى تطور علم التشفير مع مرور الزمن وضرورة مواكبة أحدث التقنيات في هذا المجال امتثالا لأمر الله وسنة رسول الله صلى الله عليه وسلم في إعداد العدة والأخذ بالأسباب في كل سعي لنصرة دين الله. فيسعد إخوانكم أن يقدموا لكم برنامج (أمن المجاهد) بعد جهد طويل بذلوه في إعداده والسعي لإتقانه، وهو جهد يغطي جانبا مهما من جوانب أمن الشبكة العنكبوتية ولا يغني عن بذل الجهد والاجتهاد في تغطية جوانبه الأخرى عبر جهود المؤسسات أو الأفراد. سائلين المولى عز وجل أن ينفع به إخواننا المجاهدين وأن يكون عونا لهم على طاعته وإغاظة أعدائه.



Decryption Finished

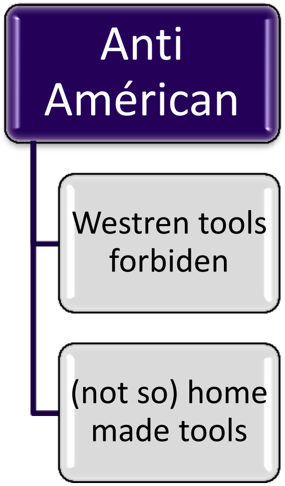
« Proof certified »



- Using TOR, Pigdin, Cryptocat, Wickr, and Telegram encrypted chat tools, ProtonMail , RedPhone…
- Want to be protected of international interligence services
- ISIS support Tails using on his forums
- AQAP created a guide about its well using

Ansar-el-Dardashah, Ansar Al Ghurrabaa

Des outils (presque) pas Occidentaux



Anti Américan

Westren tools forbiden

(not so) home made tools

- « home made » tools
- Twofish algorithm is in (close) every new program since 2013
- They comunicate a lot
- Creating this tools means having a technical hight level they don't have

Amn Al Mujahid par Al-Fajr Technical Committee,

Tashfeer Al Jawal

Conclusion

- Communication: rom a target to a decentralized network
- Encryption is not used just since a few days
- Increase in technical skills (creation of tools and piracy) and new recruits who are not on ground
- A different feeling according to cryptography and existing tools, creating the same separation as on the ground

mercit !

Questions ?

econocom