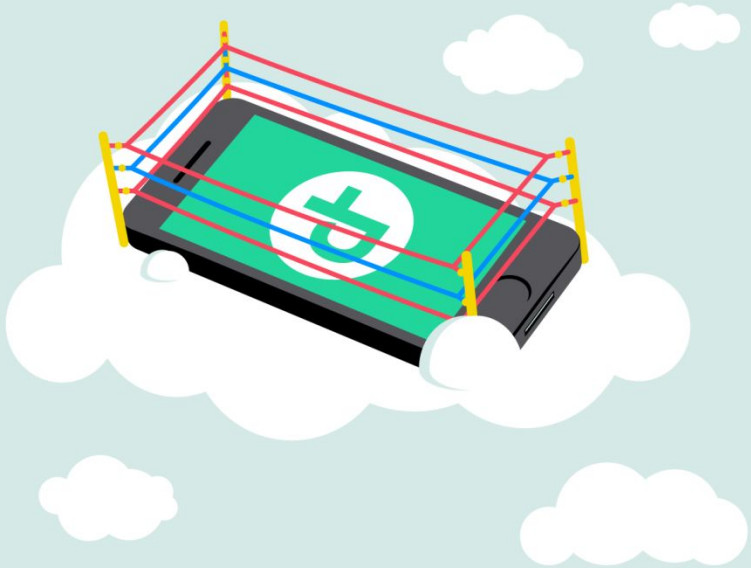
# Jihadism & cryptography

## From Internet to softwares

Overdrive Conference - GERONE



November, 2016

JULIE GOMMES

# Agenda

Introduction

**1.**

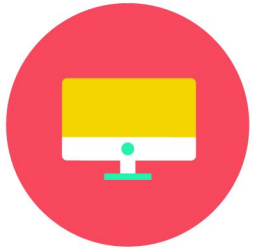
Starting point of the study

**2.**

Let’s talk about crypto!

**3.**

Crypto tools they use and why



**4.**

What can we learn about that?

Q & A

# Who I am 1/2

**Julie GOMMES**

- Senior Information Security Compliance Auditor
  - Iso 27001 compliance Lead Auditor certified
  - Risks analysis
  - Crisis management
- Lived/Worked in Egypt, Syria, Tunisia, Sudan...
- Researching on jihadist networks from years
- Find me there
  - **@Jujusete on twitter**
  - https://fr.linkedin.com/in/juliegommes





devoteam

# Who I am 2/2

Previous talks and trainings

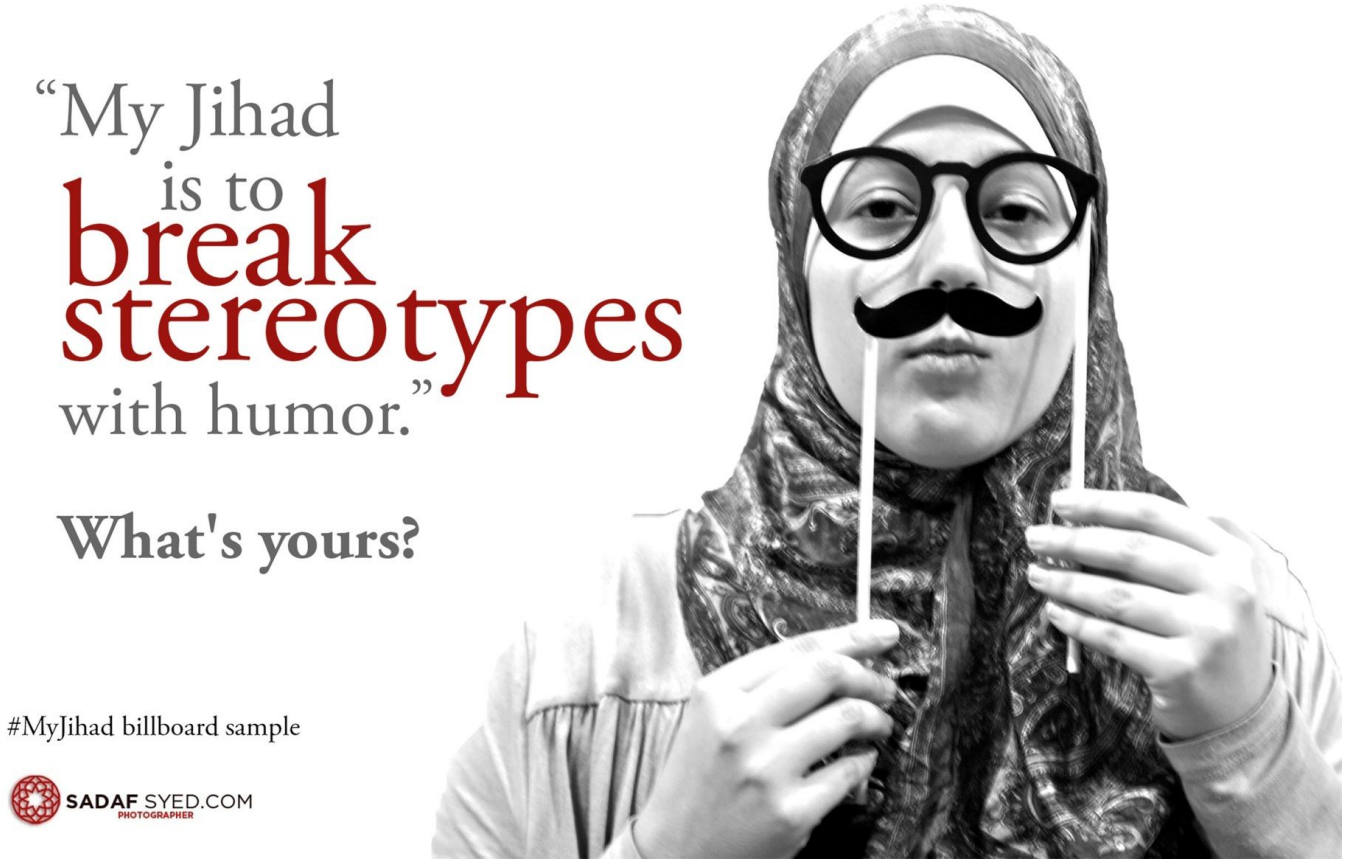
- **Jihadism and cryptography**
  - SecTor.ca, oct. 2016
  - HackFest Quebec, nov. 2015
  - BSides & DeepSec, Vienna, nov. 2015
- **How NGOs can encrypt their communications**
  - Ritimo (workshop), Paris, sept. 2015
- **Information security for journalists**
  - DefCamp, Bucarest, oct. 2014
  - MRMCD, Daarmstadt, sept. 2014
  - NDH2k14 (workshop), Paris, jun. 2014
  - HITBSecConf, Amsterdam, may 2014
- **Social Engineerig, best practices for journalists**
  - NDH2k13, Paris, jun. 2013
  - Ubuntu Party, Paris, may 2013

# 1

Starting point

# Terms and definitions 1/2

## Djihad



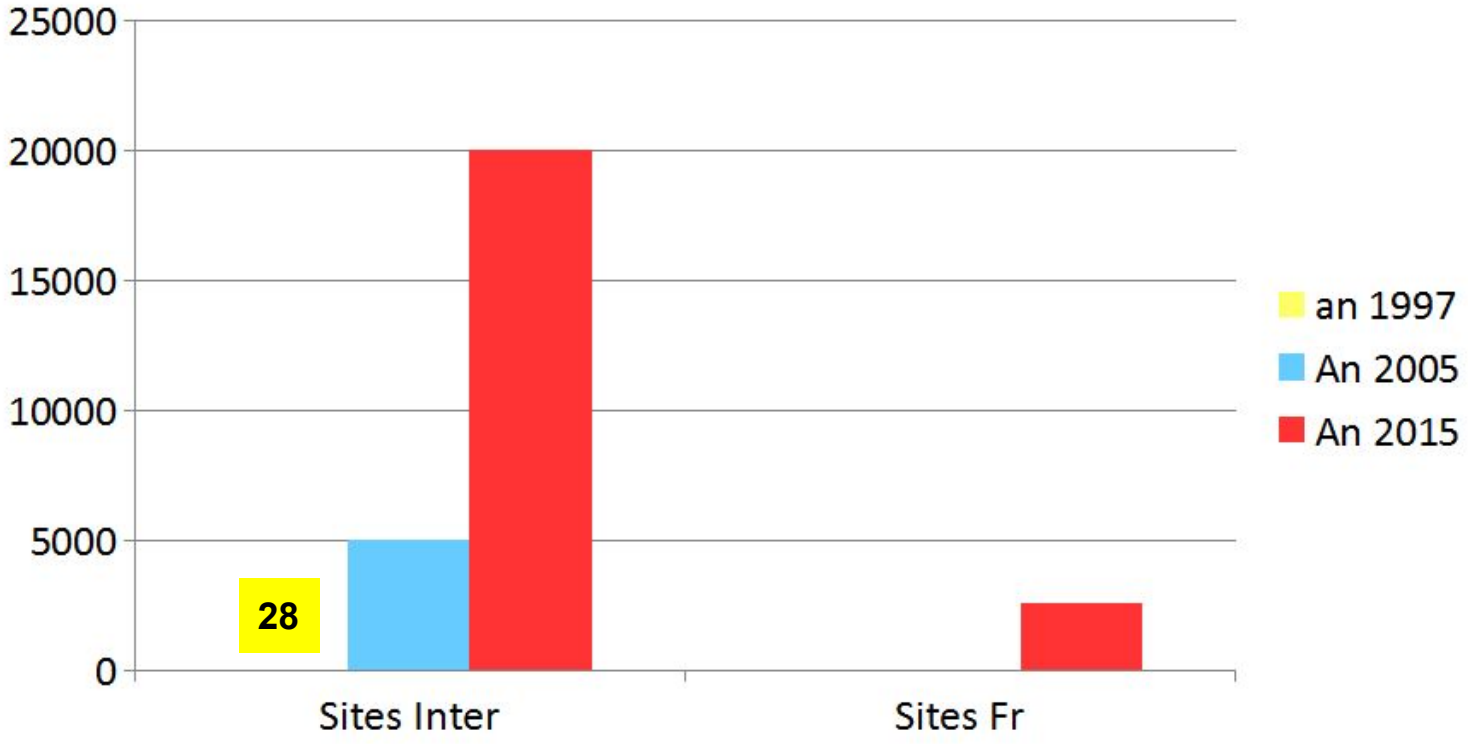
# Terms and definitiions 2/2

- **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.

- **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/creating 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 inequal.

# Evolution of pro-jihad websites




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

# Websites 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

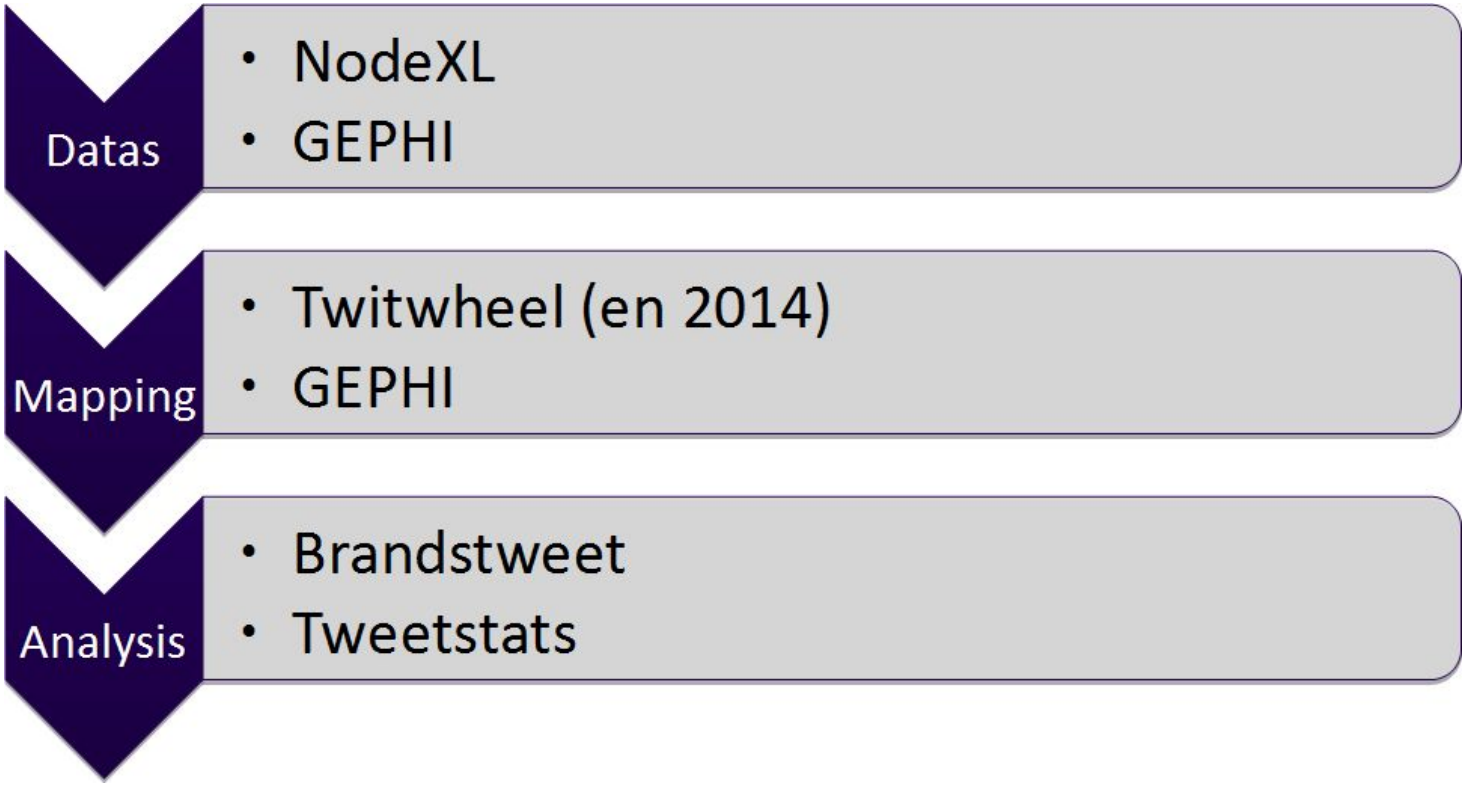
**Most famous platforms are the one wich are supported by ground organizations**

# Solid tools for communication

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

- The GIMF is known by the U.S. Federal Bureau of Investigation (FBI) as an "underground media" organization.
- The GIMF specializes in production of jihadist material for distribution.[1] It is one of several organizations that jihadists use to spread information via the Internet.
- This media organisation was born from the Global Islamic Media Group (GIMG) and Global Islamic Media Centre (GIMC).

# Tools I used


Datas
• NodeXL
• GEPHI
Mapping
• Twitwheel (en 2014)
• GEPHI
Analysis
• Brandstweet
• Tweetstats

# Evolution of twitter accounts

- First geolocalisation is **Saoudi Arabia**, before Syria, Iraq, USA, Egypt and Koweït
- **Arabic** is the most used language on pro-jihad accounts on Twitter (73 %), before english (18 %) and french (6 %)
- Every account is followed by **a thousand accounts**

**Twitter accounts were used to broadcast ISIS propaganda***

| Sept. 14 | Dec.14 |
|---|---|
| 46.000 | 90.000 |

- From march 15, « Anonymous » published on @CtrlSec0 account a list of pro-ISIS accounts to help to close them
  - They've annonced 9200 accounts but new messages are already published
  - I used those accounts and the informations they published to renew my study


*Booking.edu

# 2

Let’s talk
About
Crypto !

# Once upon a time...

… encryption

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

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

# From Moujahdeen Secret until today

11/13 - onion websites

Twoofish

2000

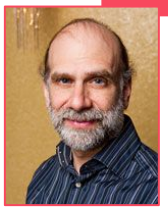
2007

02/13

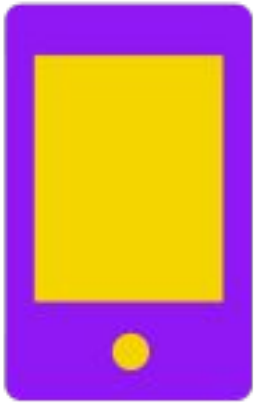
09/13

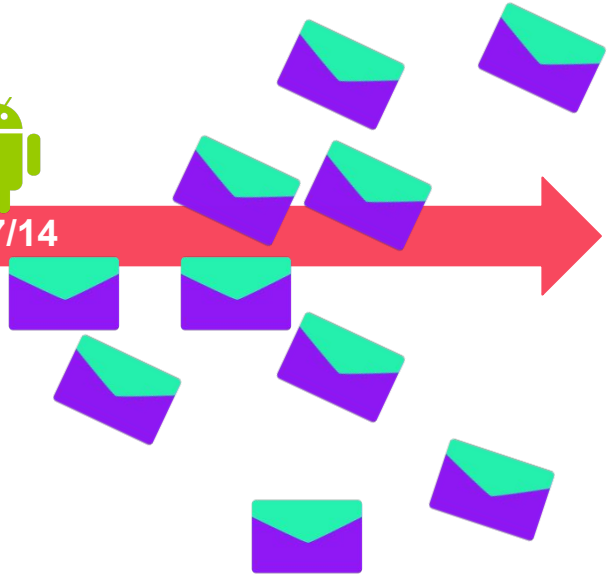
12/13

07/14



M. Secret
Email
Platform





MEMRI
http://www.lefigaro.fr/international/2007/07/06/01003-20070706ARTFIG90133-secrets_de_moudjahidins_le_programme_de_cryptage_des_terroristes.php

# Mojahedeen Secrets platform

- It encrypts email as well as file transfers using RSA public/private encryption systems. Sort of PGP alternative.
- Symetric cryptography.
- Users create their own private keys.
- The application supports a file shredder feature to delete files safely.

# From Moujahdeen Secret until today

11/13 - onion websites

Twoofish

2000

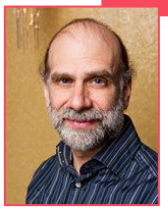
2007

02/13

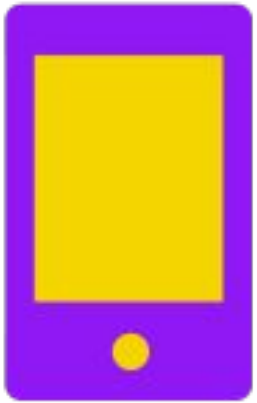
09/13

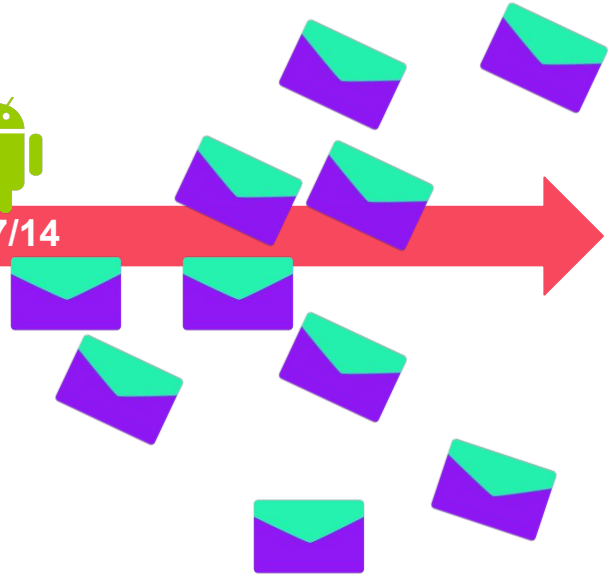
12/13

07/14



M. Secret
Email
Platform





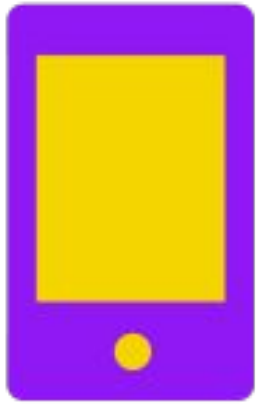
MEMRI
http://www.lefigaro.fr/international/2007/07/06/01003-20070706ARTFIG90133-secrets_de_moudjahidins_le_programme_de_cryptage_des_terroristes.php

# More and more smartphone tools

Sub-title

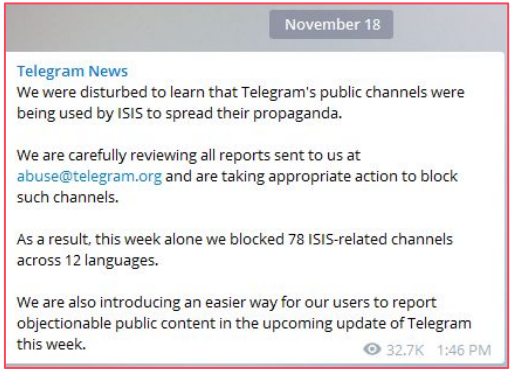
- Some people does not have Internet at home in some countries
- Easyer for instant messaging
- Wikiterrorism => more and more people, younger… (as WhatsApp users in Belgium last year)
- Zapping culture

**New security risks for them**
Geolocalisation
Lack of cotrol (wikiterrorism)

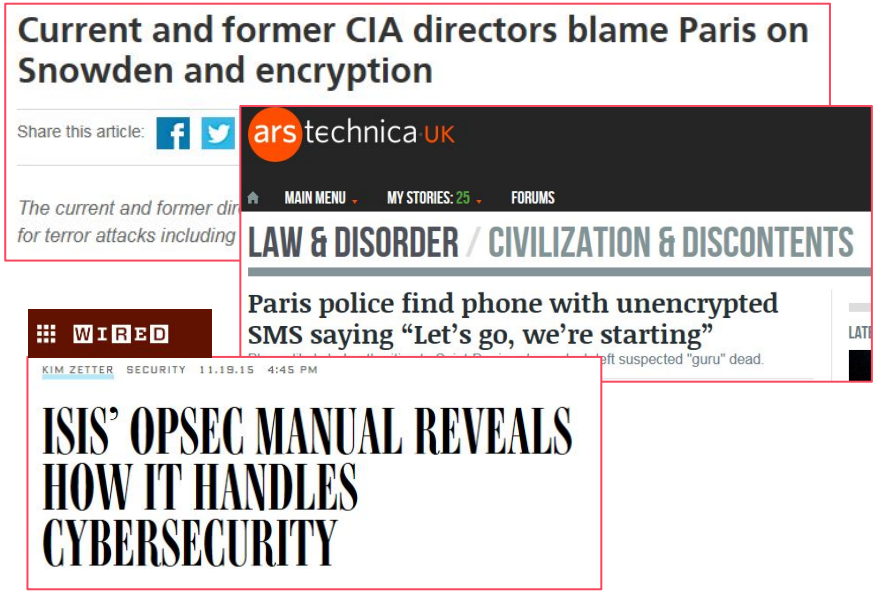


# After Paris, what about now ?

Telegram - 10 billion 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.
- "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 - november 15

Paris terrorists used burner phones, not encryption, to evade detectionhttp://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/

# Telegram and breach

Telegram. In the OS X version, text that was copied-and-pasted into the app was also written to the file /var/log/system.log

Secure messaging app Telegram leaks anything pasted in to it

01 AUG 2016 0

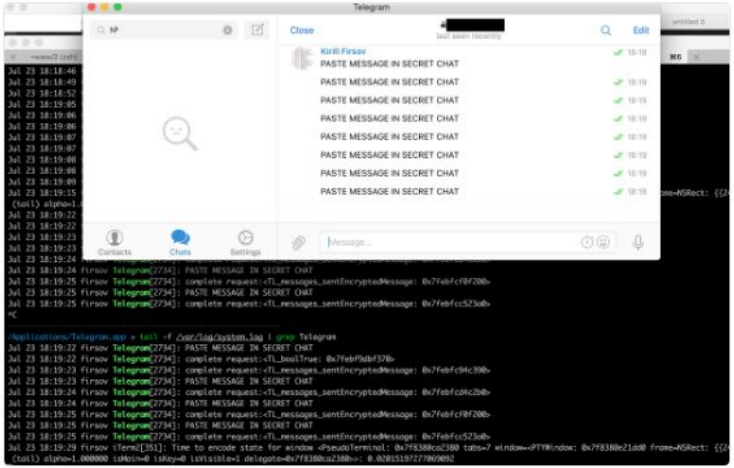
Privacy, Vulnerability


Previous: Facebook ordered to refund parents for accide... Next: Disney's "Playdom" games forum breached, passw...

Kirill Firsov
@k_firsov

Suivre

Official #Telegram for MacOS logs every pasted message to syslog, even in secret chats. @durov what's going on?






devoteam

# 3

Tools (finaly)

# Groups definition according to the tools they’re using

3 big cathegories

**Crazy religious**

**Proof certified**

**Home made tools**

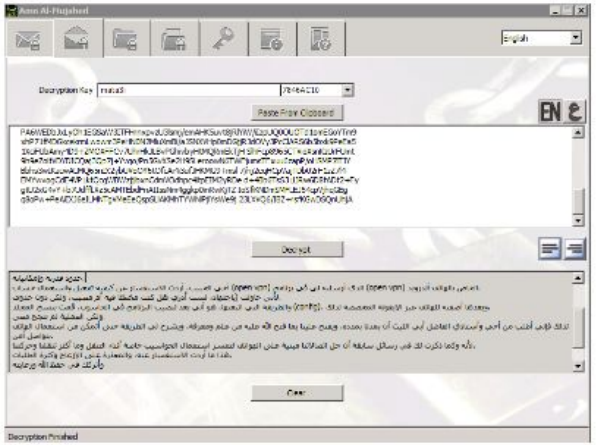
# Crazy religious 1/2


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

# Crazy religious 2/2

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.




"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"

# “Proof certified” 1/2

- Using TOR, Pigdin, Cryptocat, Wickr, and Telegram encrypted chat tools, ProtonMail, RedPhone…
- Ansar-el-Dardashah, Ansar Al Ghurrabaa
- December 2015, al-Aqsa IT Team (from Al Quaeda) distributed the manual “Tor Browser Security Guidelines” for ensuring online anonymity while using Tor software.
- "Militants and extremists don't seem to find the Tor hidden services infrastructure very useful. So there are few jihadis and militants in the darknet, it's used for criminal services, fraud, extreme, illegal pornography, cyber attacks and computer crime."*
- Want to be protected of international intelligence services
- ISIS support Tails using on his forums
- AQAP created a guide about its well using
- They download hacking tools from publicly available sources. Those program may contain custom malwares

*Thomas Rid, professor of Security Studies at King's College, Cryptopolitik and the darknet, http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

# “Proof certified” 2/2

O متصفح Tor او Orfox باندرويد لا يحتويان علي بروتوكول WEB RTC

Firefox متوفر له اضافة Web Rtc Block لكنها لا تعمل بكفاءة فالافضل استخدام متصفح

Safari على نظام los لا يحتوي على بروتوكول WEB RTC لكن تنصح باستخدام Firefox بدلا

---

اهم الإضافات الأمنية للمتصفحات

محرك البحث Disconnect انشاء مطورين بعام 2011 كانوا يعملون بشركة جوجل سابقا , محرك البحث آمن ومفتوح المصدر ويمنحك مزيدا من الخصوصية اثناء التصفح

أداة ublock Origin اداة خفيفة وفعالة جدا في حظر الاعلانات لا تستهلك نسبة كبيرة من المعالج او الذاكرة العشوائية والاداة تتفوق على Adblock في انها لا تظهر اعلانات مطلقا لكن Adblock تظهر بعض الاعلانات المقبولة Acceptable Ads

اي موقع تتصفحه يجمع عنك معلومات اساسية منها مانوع المتصفح الذي تستخدمه ورقم الاصدار ونظام التشغيل الذي تستخدمه هذه المعلومات حساسة جدا وقد يستخدمها البعض في استهدافك لكن اداة Random Agent Spoofer تسمح لك بتضليل هذه المواقع التي تجمع عنك معلومات عن طريق السماح لك باختيار نوع المتصفح الذي تريده ان يظهر الى المواقع التي تتصفحها

مثال : انا استخدم متصفح فايرفوكس لكن لا اريد المواقع التي اتصفحها ان تعرف اني استخدم متصفح فايرفوكس فاداة Random Agent Spoofer تسمح لك باختيار المتصفح الذي تريده لتضليل هذه المواقع

الكوكيز عبارة عن ملفات تخزنها المواقع التي تتصفحها على جهازك هذه الملفات تحتوي على بيانات حساسة مثل كلمات المرور والبريد الالكتروني لكن اداة self-Destructing Cookies تقوم بحذف هذه البيانات بشكل تلقائي بعد غلقك للموقع الذي تتصفحه

اداة HTTPS Everywhere اداة طورتها منظمة الحدود الالكترونية EFF حيث تجبر جميع المواقع التي تتصفحها على استخدام بروتوكول التشفير HTTPS بدلا عن HTTP

اداة NO SCRIPT

O متصفح Tor او Orfox باندرويد لا يحتويان علي بروتوكول WEB RTC

الكوكيز عبارة عن ملفات تخزنها المواقع التي تتصفحها علي جهازك هذه الملفات تحتوي علي بيانات حساسة مثل كلمات المرور والبريد الالكتروني لكن اداة self-Destructing Cookies تقوم بحذف هذه البيانات بشكل تلقائي بعد غلقك للموقع الذي تتصفحه

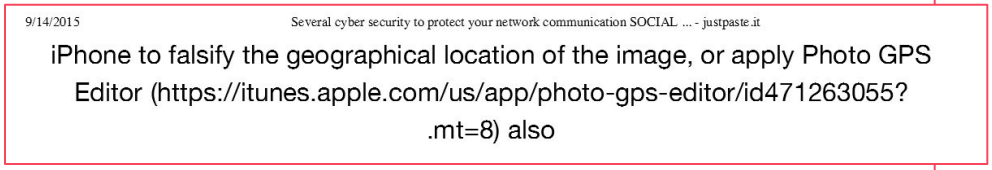
اداة HTTPS Everywhere اداة طورتها منظمة الحدود الالكترونية EFF حيث تجبر جميع المواقع التي تتصفحها علي استخدام بروتوكول التشفير HTTPS بدلا عن HTTP



devoteam

# “Proof certified” 3/3

Some extract from **guidebook**


9/14/2015 Several cyber security to protect your network communication SOCIAL ... - justpaste.it

iPhone to falsify the geographical location of the image, or apply Photo GPS Editor (https://itunes.apple.com/us/app/photo-gps-editor/id471263055? .mt=8) also

Use the service Freedome (http://www.f- .2 secure.com/en/web/home_global/freedome) of VPN phones for the iPhone from here (https://itunes.apple.com/us/app/f-secure-freedome-vpn/id771791010?mt=8) and for Android from (https://play.google.com/store/apps/details? id=com.fsecure.freedome.vpn.security.privacy.android&hl=en)here, a service of the Finnish security company F-Secure which is not free, but a quick control and protect you from spyware and fraudulent websites and so .on

use an application The Serval Project for Android .7 (https://play.google.com/store/apps/details? id=org.servalproject&hl=en)devices, which makes your application is a station to communicate with other parties using the same application in the vicinity of 200 meters and the more the number of users increases, the more the vicinity of the application work, communication is done by internal numbers such as "Operator" system

**Note: The** download version (7.1) of the TrueCrypt program only and do not download new versions (7.2) for the existence of the changes and stop the .encryption properties by developers for unknown reasons

**SpiderOak service:** cloud storage service encrypted very high encryption keep confidential files where no one can not company employees see the contents of your files

**Hushmail service:** safe and free e-mail service through which to open an **-1** account and start correspondence which ensures service encrypts messages without user intervention lies Service servers in Canada, which is .one of the most secure mail services

# (not so) home made tools

- Twofish algorithm is in (close) every new program since 2013
- They communicate a lot
- Creating this tools means having a technical hight level they don’t have
  In french language, we say “that is coded with feet
- Amn Al Mujahid par Al-Fajr Technical Committee, Tashfeer Al Jawal

# 4

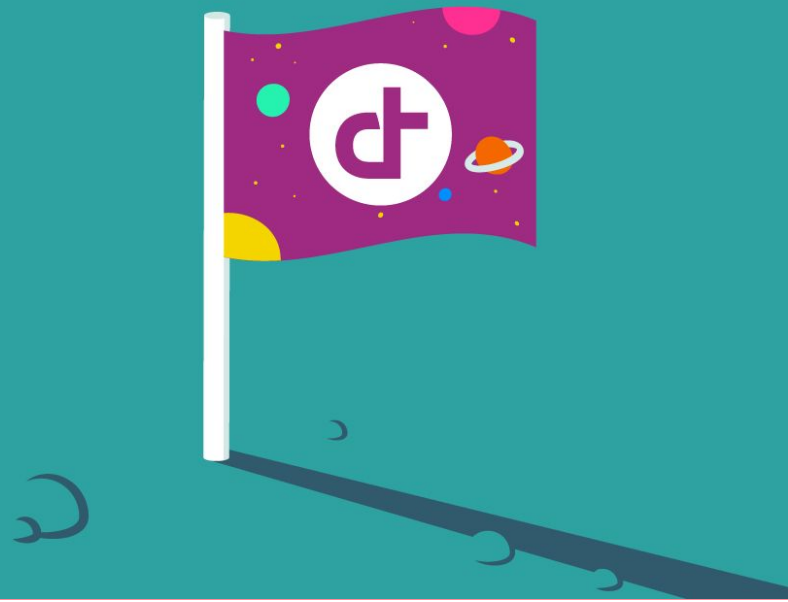
So what can
We learn
About that ?

# Conclusion

- Communication: from 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

# Thank you !

# Questions ?



https://twitter.com/jujusete

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

Julie GOMMES

*Information Security Compliance auditor*

julie.gommes@devoteam.com

devoteam