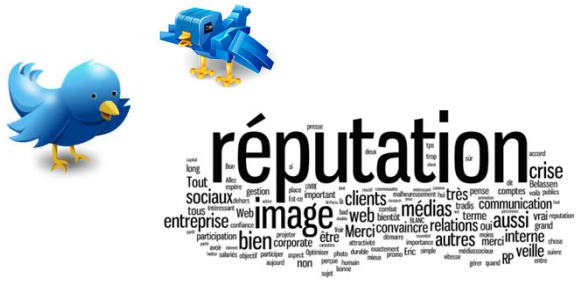
LES ATTEINTES A LA REPUTATION

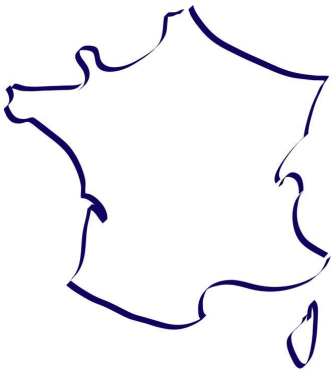


Les *"bots"* sociaux malveillants : une nouvelle menace sérieuse

par M. Daniel GUINIER

Expert en cybercriminalité près la Cour Pénale Internationale de La Haye
Colonel (RC) de la gendarmerie nationale

LES UTILISATEURS DES RESEAUX SOCIAUX



33 millions

Messages : 10 milliards/jour

2 milliards

29 millions

1,5 milliard

16 millions

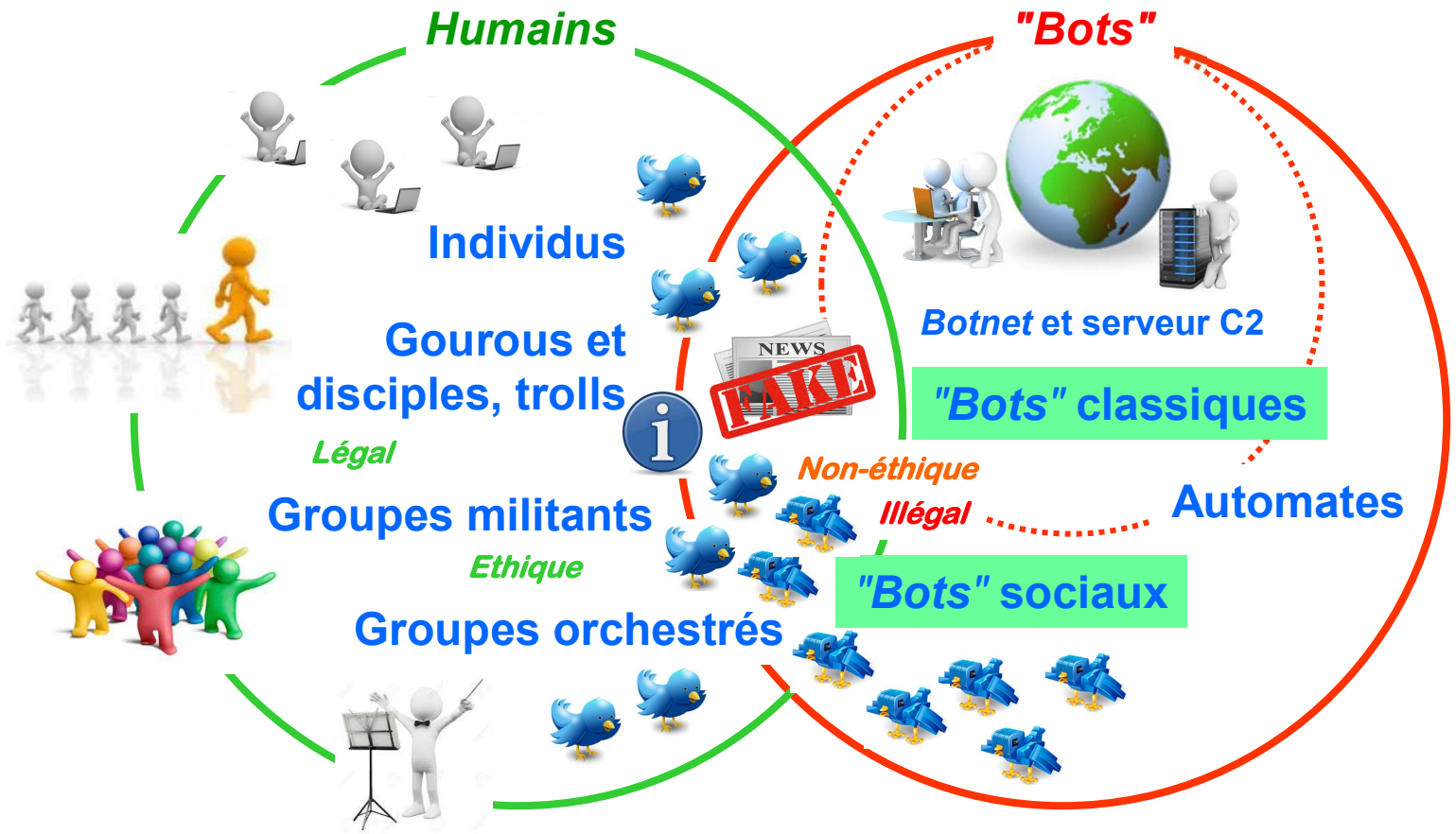
330 millions

Tweets : 500 millions/jour

Twitter permet l'envoi spontané de brefs messages (140 car. max), **les *tweets***, par messagerie instantanée sur Internet ou par SMS, **en réaction immédiate**.

Le nombre d'utilisateurs actifs des trois principaux réseaux sociaux, indique qu'ils sont de très bon candidats pour les *"bots"* en servant de vecteurs.

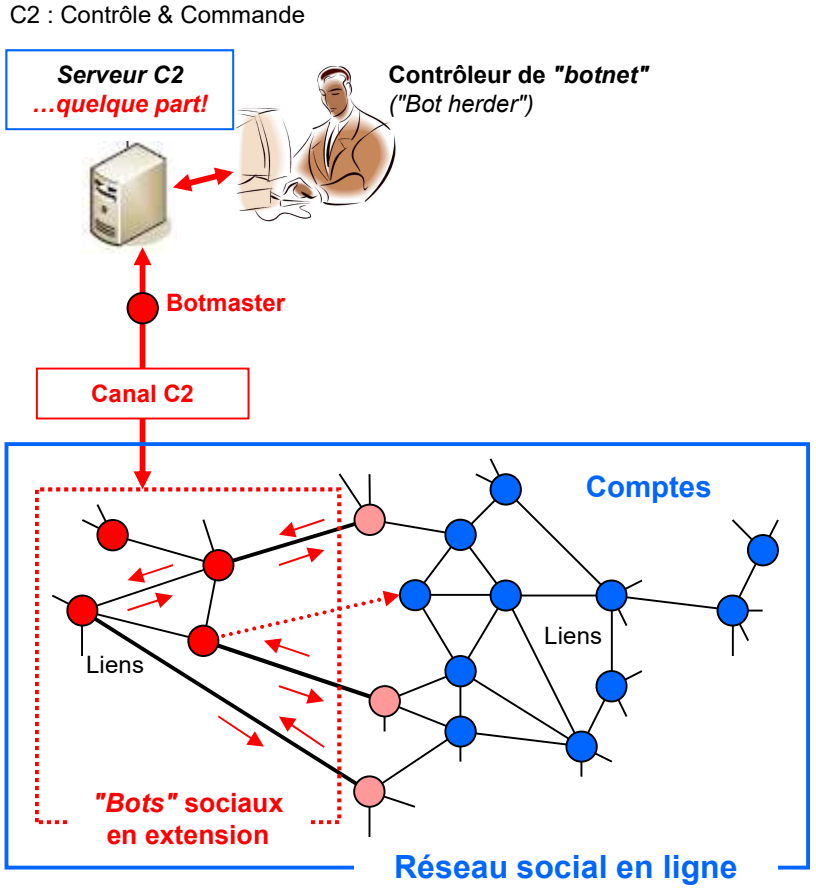
L'ECOSYSTEME DE L'INFLUENCE EN LIGNE



"False news" : Informations inexactes
"Fake news" : Fausses informations

Cet écosystème d'influence permet ainsi l'interférence et l'amplification des messages des différentes sphères, avec l'appui d'outils et de services légaux ou illégaux pour obtenir et diffuser des informations, vraies, inexactes ou fausses.

LES *"BOTS"* SOCIAUX



Les *"bots"* sociaux sont destinés à interagir en temps réel avec des humains sur les réseaux sociaux en produisant automatiquement du contenu de façon coordonnée mais incontrôlée par les plateformes, *telles que Facebook ou Twitter*.

En simulant le comportement humain ils peuvent créer et diffuser de fausses informations de façon massive, visant à atteindre la réputation.

Un *"bot"* social est lié à un compte d'appartenance à un réseau social, tandis qu'un *"bot"* classique se rapporte à une machine compromise d'adresse IP.

APPEL AUX SCIENCES COGNITIVES

Réseaux

sociaux humains

et "bots" sociaux

d'influence

Modélisation
Perception
Langage
Mémoire
Connaissances
Raisonnement
Émotions

Simulation
Acquisition
Transmission
Utilisation

Système d'IA
Algorithmes

"Bots" sociaux

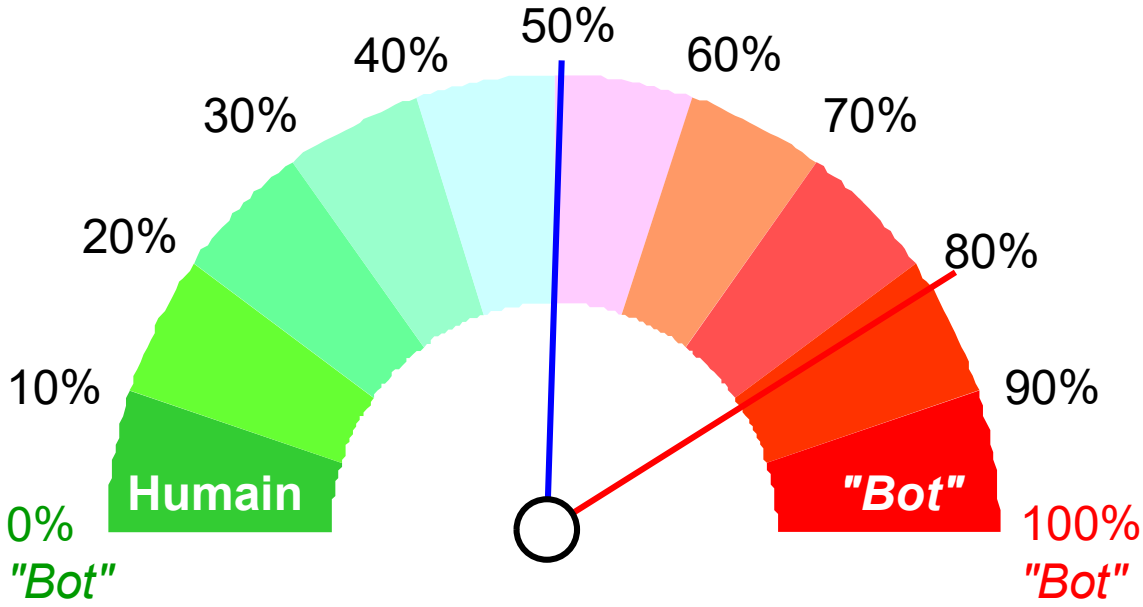
Action
Comptes sociaux :
Infiltration
Création, etc.
Informations :
Elaboration
Diffusion, etc.

Manipulations : leviers d'influence, biais cognitifs ; alimentées par des rumeurs.

IA : Intelligence Artificielle

Les sciences cognitives : *neurosciences, linguistique, psychologie, philosophie, anthropologie, et IA,* seront requises en traitant conjointement leurs données pour réaliser les *"bots"* évolués visant à simuler la pensée humaine.

DETECTION *Tweet* HUMAIN *versus "BOT"*



82%

40% : Réseau
45% : Temps

85% : Utilisateur
83% : Contacts
71% : Contenu
54% : Sentiments

Exemple

Après acquisition de l'historique, scores obtenus avec le système *BotOrNot* pour un compte *Twitter* @..... ; déterminant clairement un *"bot" social.*

ATTAQUES AVANCEES SUR LA REPUTATION

Préparation

Renseignements par tous moyens

Conception de stratégies

Experts en techniques d'influence pour bâtir des scénarii
Elaboration de fausses informations cohérentes et peu vérifiables

Exploitation de failles humaines et techniques

Moyens légaux ***Moyens illégaux***

Corruption Espionnage

Ingénierie sociale

Intrusion : furtivité, *"botnet"*

Experts

Cyberattaque

Exfiltration de fichiers et **accès en ligne à des comptes sociaux compromis**

Exécution

Choix en fonction des **circonstances** et du **but**
Diffusion de fausses informations
Relais : réseaux et *"bots"* sociaux, communautés, etc.

Points particuliers

Groupes d'influence, ***identités et comptes multiples*** *pour* ***amplifier la portée*** *;* ***détournements*** *d'hashtag impliquant la victime : spams, défiguration ;* ***invasion*** *: retweets, reposts, etc.*

Réaction de la victime

Plainte, préservation des preuves, enquête
Informations mêlées pour disqualifier l'attaque
Relais : réseaux sociaux, sympathisants

Points particuliers

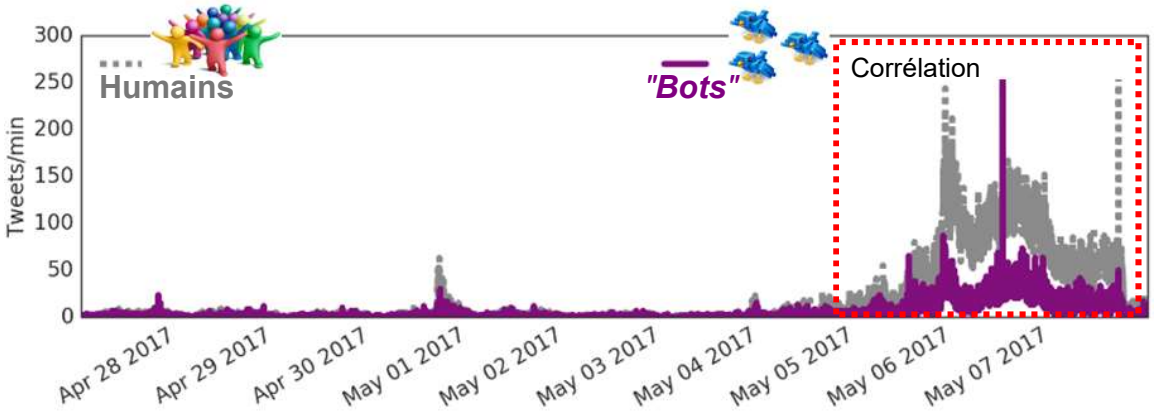
Compartimentation, chiffrement, messageries et protocoles ***sécurisés*** *;* ***détection précoce*** *:"honeypot" - "cloud" ;* ***veille active*** *:* ***réseaux et "bots" sociaux*** *;* ***PSI - plan d'action****, etc.*

La diffusion de fausses informations mêlées à d'autres, réelles, donneront de la crédibilité ou jetteront le doute, selon le cas de chacun : *attaquant ou victime*.

MacronLeaks : LES *"BOTS"* EN MARCHE …

Réf. : Ferrara E. (2017)

La campagne de déstabilisation débute le 5 mai 2017, **quelques heures avant l'entrée dans la période de réserve électorale** avec **un pic important de *tweets* dus à des *"bots"* le dimanche 7 mai**.



Les *tweets* de désinformation de *"bots"* sociaux précèdent les cascades de *tweets* humains qui sont suscités par un **phénomène d'induction** permettant l'**amplification de la portée de l'influence**.

L'élection présidentielle française de 2017 a été liée aux *MacronLeaks*, par leur diffusion importante via *Twitter*.

Origine *"bots"* sociaux de la campagne : 18%

Origine anglophone de la campagne > 50%

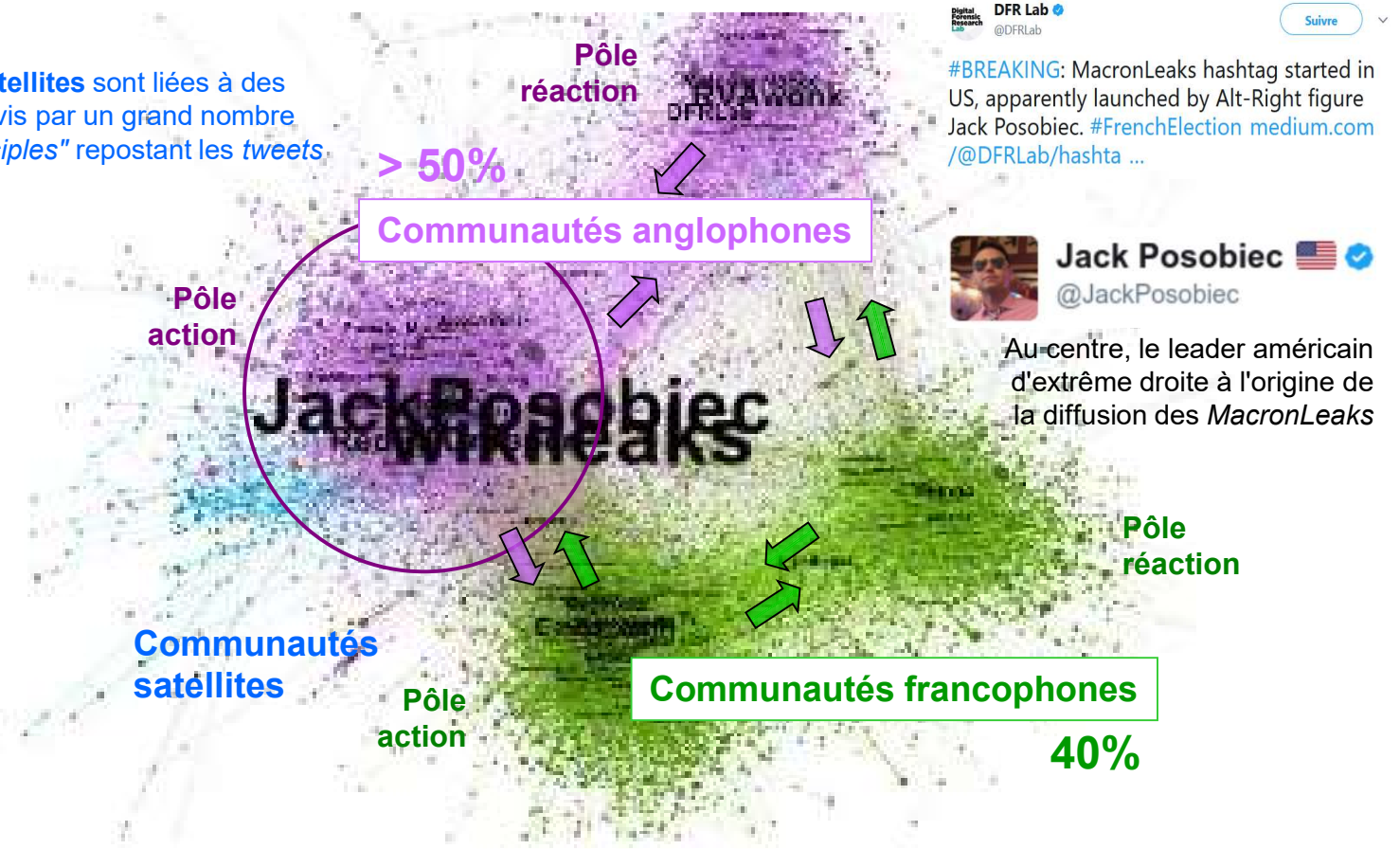
Langue majoritaire : l'Anglais
Vocabulaire anglais et français

Il faut s'attendre à voir apparaître sur les *"darknets"* un marché de *"bots"* sociaux, sinon d'automatismes de désinformation, réutilisables à diverses fins.

LES RESEAUX DE COMMUNAUTES

Réf. : Gu L. et al. (2017)

Les **communautés satellites** sont liées à des comptes *"gourous"* suivis par un grand nombre de comptes actifs *"disciples"* repostant les *tweets* de leur *"gourou"*.



Le diagramme du réseau du *hashtag #MacronLeaks* permet d'observer les interactions entre les communautés de comptes ou de *"bots"* sociaux utilisés pour amplifier le trafic de propagande ou pour diffuser les *MacronLeaks*.

CONCLUSION SUR LES *"BOTS"* SOCIAUX

- Les réseaux sociaux sont aussi un lieu de désinformation
- Les campagnes menées sont un risque pour la réputation
- Des *"bots"* sociaux ont d'ores et déjà été engagés
- D'autres seront plus sophistiqués et offerts sur les *"darknets"*
- Des actions de plus grande ampleur sont attendues
- Elles seront le fait d'organisations structurées ou d'États

Les *"bots"* sociaux sont de nouveaux vecteurs de menaces sérieuses

Les autorités ont à anticiper l'ampleur du phénomène et de ses conséquences, aux fins de prévoir des contremesures efficaces jusqu'au niveau international.