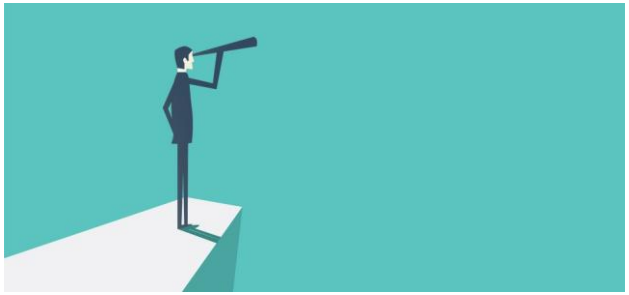
Project CyberSouth
Cooperation on cybercrime in the Southern Neighbourhood

Session 5 – How the judiciary evaluates the number of cases

09 April 2019 / 14:30 – 17:30

Cybercrime, statistics and gathering data : how to break the curse ?

Jacques MARTINON
Magistrate, head of mission against cybercrime
French Ministry of Justice



Overview

- *Questions : how data are collected and analysed ? The use of statistics for judiciary ?*

- **Introduction : triple curse on cybercrime** (the so-called « dark figure » of cybercrime ; the fog of statistics ; the « going dark » phenomena) ;
- **1. Fog of statistics** (needles in a haystack ; attemps to categorize ; inappropriate statistical tools)
- **2. Workarounds** (offense committed in cyberspace ; new databases PERCEVAL, THESEE and ACYMA)
- **3. New leads for future** (ONRDP, SMSSI, update of CASSIOPEE)
- **4. Our contribution to the « global threat » report** (DMISC)

Introduction
Triple curse on cybercrime

- the so-called « dark figure » of cybercrime ;
- the fog of statistics ;
- the « going dark » phenomena

1. Fog of statistics

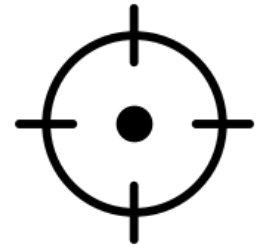
- 1.1 Needles in a haystack
- 1.2 Attemps to categorize
- 1.3 Inappropriate statistical tools

1.1 Needles in a haystack

• Mismatch between traditional statistics of offenses and cybercrimes

•Example : offenses against a computer system -> Too broad approach (ransomware, cryptojacking, cyberespionage, cybersabotage, jackpotting…)

Wide scope of cybercrime



- The scope of cybercrime may cover:
- Certainly, the computer offenses defined by articles 323-1 and following of the penal code;
- a number of common offenses specifically aggravated by the circumstance of using an electronic communications network;
- several data privacy violations resulting from abuse of data gathering or data processing;
- a large number of common offenses committed with a cybercrime dimension, like the way of approaching the victim (concealment, fraud, scam)

1.2 Attemps to categorize

- CLASSIFICATION : Cybercrime and Cyber enabled crime ?
- TABLE PHENOMENA (*extract*) : more than 40 phenomena identified… And growing ! (EN version WIP)

TABLE 1: Phénomènes cyberdélinquants ayant pour objet un système de traitement automatisé de données

Phénomène	Intensité	Préjudice	Auteur	Victime	Qualification pénale
Attaque par déni de service (et variantes)	Variable	Pécuniaire, variable en fonction de la cible	Individu isolé, organisation criminelle et menace persistante avancée (MPA)	Ciblée : tout service en ligne	Entrave au fonctionnement d'un STAD : 323-2 C. pén. et possiblement extorsion simple ou en bande organisée : 312-1 et 312-6-1 C. pén.
Braquage 3.0	Faible	Pécuniaire, matériel importants, image et réputation	Organisation criminelle ou individu isolé	Ciblée : banques, stations services, plateformes d'échanges de cryptomonnaies etc.	Altération du fonctionnement d'un STAD : 323-1 C. pén. et vol simple en bande organisée : 311-9 et suiv. C. pén.
Compromission d'un STAD (recrutement dans un réseau de machines zombies)	Haute	Matériel	Organisation criminelle	Indiscriminée et en nombre important	Accès, maintien et altération du fonctionnement d'un STAD : 323-1 C. pén.
Cryptojacking	Basse	Pécuniaire	Individu isolé, organisation criminelle ou MPA	Ciblée ou indiscriminée et en nombre important	Atteintes aux STAD : 323-1 à 323-4-1 C. pén.
Cyber-espionnage économique ne portant pas atteinte aux intérêts fondamentaux de la Nation	Haute	Patrimonial, image et réputation	Individu isolé, organisation criminelle ou MPA	Ciblée : entreprise privée ou publique, possiblement OIV et OSE	Atteintes aux STAD : 323-1 à 323-4-1 C. pén.
Cyber-espionnage portant atteinte aux intérêts fondamentaux de la Nation	Haute	Patrimonial, image et réputation	Individu isolé, organisation criminelle ou MPA	Ciblée : État, opérateur d'importance vitale ou opérateur de service essentiel	Livraison d'informations à une puissance étrangère : 411-6 à 411-8 Code pénal (C. pén.) et atteintes aux STAD : 323-1 à 323-4-1 C. pén.
Cyber-extorsion (données privées)	Variable	Pécuniaire, matériel, image, réputation et moral	Organisation criminelle ou individu isolé	Ciblée : particuliers, organisations ou indiscriminée et en nombre important	Accès frauduleux et extraction de données d'un STAD : 323-1 et 323-3 C. pén., extorsion simple ou en bande organisée : 312-1 et 312-6-1 C. pén.
Cyber-sabotage	Haute	Matériel et possiblement humain	Individu isolé ou MPA	Ciblée mais en nombre important si existance de victimes collatérales	Sabotage : 411-9 C. pén. et atteintes aux STAD : 323-1 à 323-4-1 C. pén.
Cyber-terrorisme	Haute	Matériel et moral	Individu isolé, organisation criminelle ou MPA	Ciblée	Actes de terrorisme : 421-1 C. pén. et atteintes aux STAD : 323-1 à 323-4-1 C. pén.

1.3 Inappropriate statistical tools

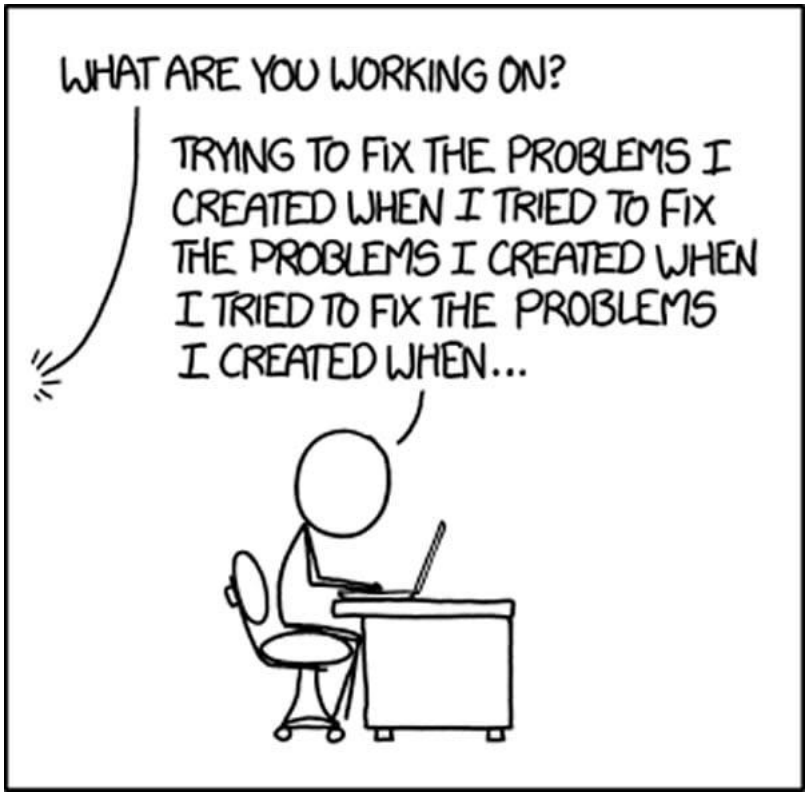
- 2 mains sources :
- NATAFF (Nature of Case) : recorded at the first reception by prosecutor's office (« Bureau d'ordre », « Order's Office ») ; based on generic type of offenses but actually incomplete on cybercrimes. Extract from software CASSIOPEE (SID, *Système d'information décisionnelle*). Statistics are the flow of cases recorded by the prosecutor's office.
- NATINF (Nature of Offense) : recorded after analysis of a prosecutor (more precise, but still inapproprite sometimes because NATINF are based on specific offense). Tables with the national criminal record (CJN). The statistics are the sentences pronounced by the courts.

Limitations

- The statistical system of the Ministry of Justice does not make it possible to determine operating mode variables, and thus isolate within the very broad set of common offenses, those that may be cybercrime-related ;
- The only possible figures are related to specific offenses, such as computer offenses (Article 323-1 Penal Code), those with a special aggravating circumstance or offenses related to privacy (database)

2. Workarounds

- 2.1 Offense committed in « cyberspace » ?
- 2.2 New databases (PERCEVAL, THESEE and ACYMA)



2.1 Offense committed in « cyberspace » ?

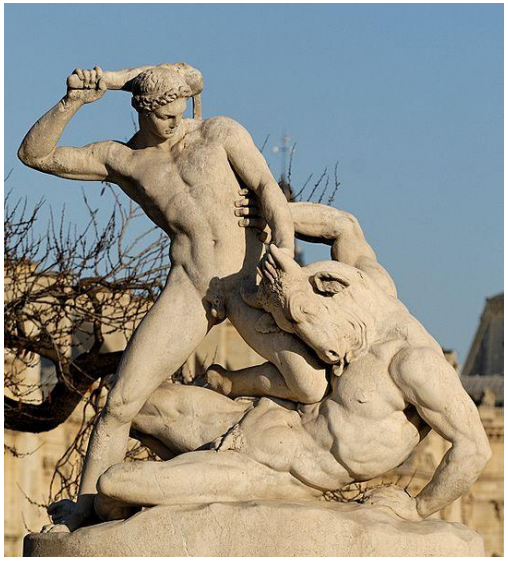
- A solution for « gendarmerie & police » software : tick a box « cyberspace » for the location of offenses.

2.2 New databases on cybercrime

- **PERCEVAL** : already open to public (june 2018) -> misuse of credit card on Internet
- **THESEE** : should be deployed this year

  -> scams on Internet (Sextorsion, mailbox hacking, ransomware, fake website…)
- **ACYMA** (https://cybermalveillance.gouv.fr) : real-time feedback of new phenomena (ex: tech support scam)

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique



3. New leads for future

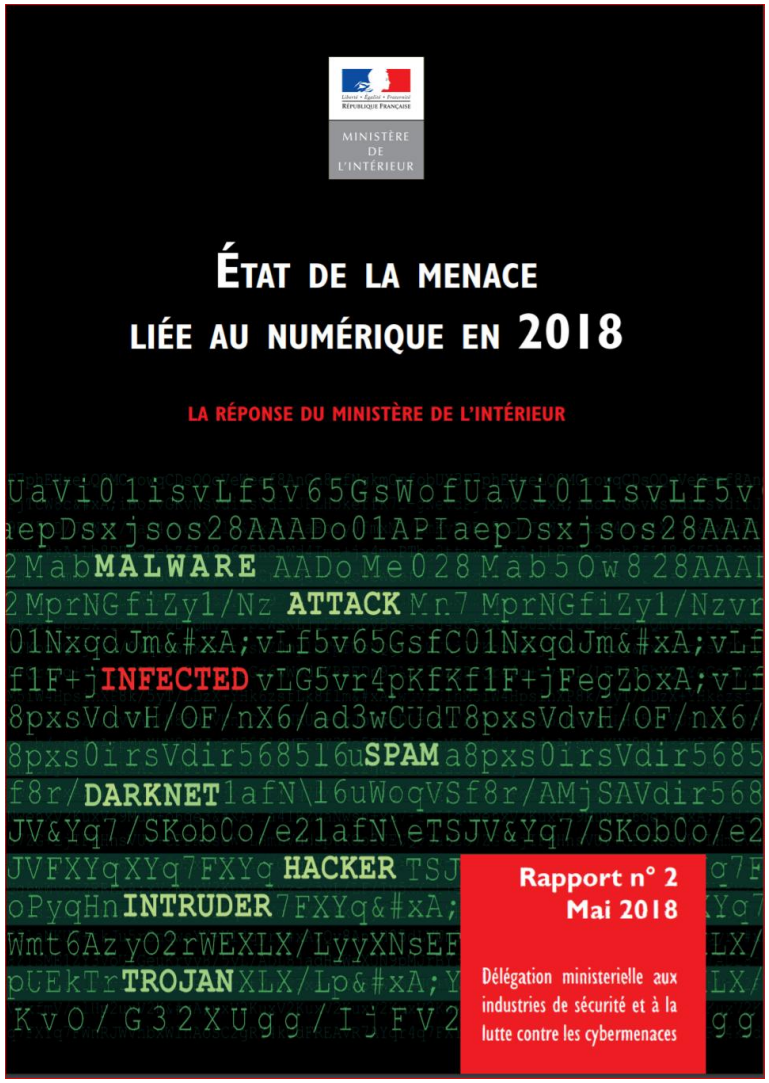
- New joint ministerial report : specific recommandations on statistics ! A prerequisite before the allocation of additional resources ?

- ONRDP (National Observatory of Delinquency and Criminal Responses), attached to the National Institute of Higher Studies of Security and Justice (INHESJ) ;

- SMSSI (French Ministerial Statistical Department for Internal Security) : the Ministerial Statistical Department for Internal Security (SSMSI) was established in 2014 in the administration of the French Ministry of the Interior.
  - The missions of the department are to:
  - Provide independent and evidence-based analyses, policy evaluations and recommendations to help the national police and the national gendarmerie in the performance of their duties, as well as the minister's office in the design of its public policies for internal security.
  - Produce and disseminate official statistics and analysis on internal security and crime to the public and to the research community, respecting the public statistics standards of reliability and of impartiality.

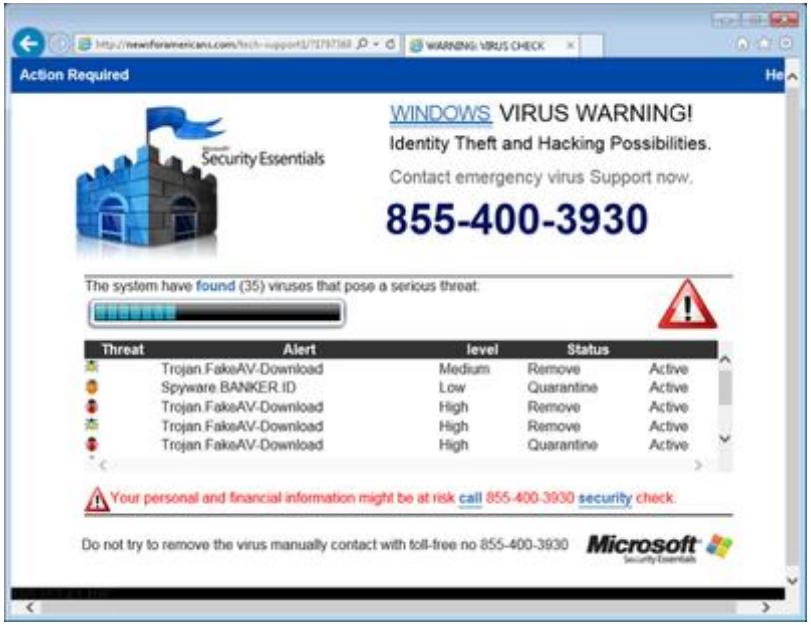
- update of CASSIOPEE (*Chaine Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants*) : long term solution ?

4. Our contribution to the 2019 « global threat » report (DMISC)



Previous statistics & Data from cybercrime Section of Paris (F1)

- Previous statistics shown ;
- New trends of cases treated by Section F1 of Paris Prosecutor's Office : Ex Tech Support Scam & Sextorsion « Cryptoporno » ;
- When it's done, we can send you the 2019 Report (FR)



Conclusion

- “Facts are stubborn things, but statistics are pliable.”
  — **Mark Twain**
- Statistics on cybercrime have to be improved, but can it be really a prerequisite for additional ressources ?
- Contact : jacques.martinon@justice.gouv.fr