Cyber code éthique

Éthique et cybersécurité

Inti Rossenbach

JSSI - 10 mai 2022

cryptosec@jssi:~$ whoami

Inti Rossenbach
Divague dans la cyber depuis 1998
RSSI
Cours à Nanterre et Sorbonne Paris Nord
iro@cryptosec.org
@secucrypt

#include <exemples.h>

Où il sera question d’éthique dans le domaine de la cybersécurité

Un hack back light

Un *defacement,* impact limité
Un proxy vulnérable
… accès aux logs
L’attaquant a commis beaucoup d’erreurs
Nous trouvons son identité
Nous sommes certains

Que faire ?

Surveiller et punir

Logiciel de surveillance et interception

Eagle

Des gens bien, sans doute

Révélations en 2011

2021, des gens mis en examen pour « complicité d’actes de torture »

Embûche à l’embauche

Vous êtes analyste sécurité, accès au SIEM

Il est tard, vous êtes seul

DG arrive, votre N+3/4

« Quels sites a consulté M. Louche ? »

Votre responsable, M. Rossenbach, est injoignable, au bistrot, en mer ou à la JSSI

Que faites-vous ?

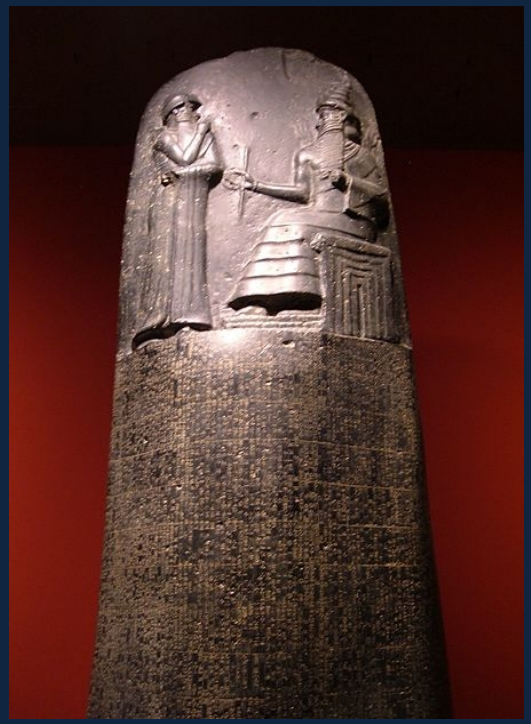
cryptosec@jssi:~$ man éthique

De quoi parle-t-on exactement ?

Quelles sont les différences entre morale, légalité et éthique ?

Morale – Légalité – Éthique

Nudistes bibliques



Hammurabi, Babylone, 1750 av. J.-C.

Éthique : questionnement qui précède. Je suis ce que je peux. Déterminer la conduite et l'action.

Impératif catégorique kantien :
« Agis de telle sorte que la maxime de ton action puisse être érigée par ta volonté en une loi universelle »
(*in Critique de la raison pratique, 1788*)

Utilitarisme (Bentham, Mill – XIXe) : focus sur les conséquences

Morale – Légalité – Éthique

Propres à un milieu, une culture, une époque, à des mœurs, à des groupes

Aristote : l’attitude éthique ne vient pas du jugement, mais de la pratique, par l’exercice, l’habitude et l’apprentissage (!= Platon)

S’arrache au cours des choses, à la nature et à ses lois. Il ne s’agit pas que de sa propre liberté, mais aussi de celle d’autrui (*inanité des libertariens*)

Spécificités de la question éthique en cybersécurité ?

« La technique est la mise en œuvre d’un savoir, distinct de celui-ci, et qui ne prend pas en considération les fins ultimes de l’activité dont il s’agit » (C. Castoriadis)

Détachement de l’outil et de de son usage.

« Avec un grand pouvoir vient une grande responsabilité » (Spider-man, 1962)

- ~~La sécurité, c’est bien, le risque, c’est mal~~
- Accès à des données sensibles
- Collecte, surveillance, contrôle, investigation
- Simulation d’offensif
- Le face-à-face avec des *bad guys*
- Conséquences IRL
- Juridictions différentes
- Zones grises
- Effet tunnel de l’intérêt technique
- Domaine très profitable

Ethical Blue screen error

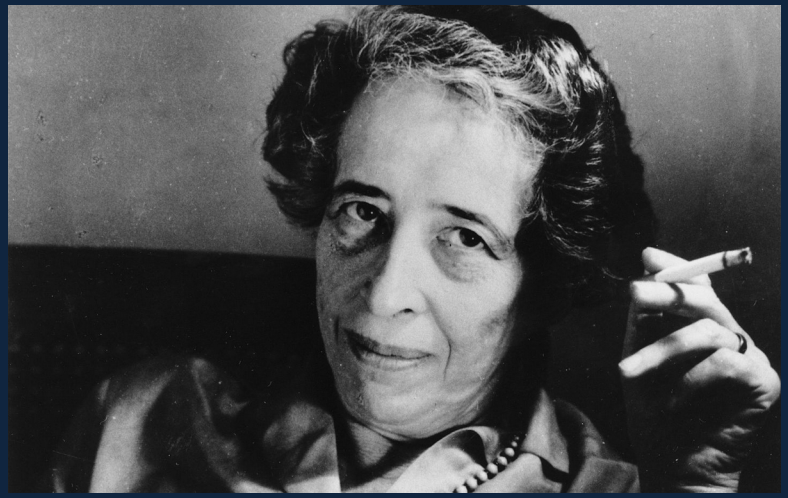
Qu’est-ce qu’un problème éthique, dans notre domaine ?
Comment le caractériser ?

Problème éthique ?

- Écarts entre finalités et principes
- Dépassement de nos limites, principes
- Accepter d’être un rouage passif
- Outrepasser nos droits et pouvoirs
- Contrainte du groupe, de la hiérarchie
- Garder le silence quand il faudrait parler
- Adaptation aux moyens de l’adversaire
- Contournement de la légalité
- Actions illégales
- Inflexibilité de l’application des normes juridiques

Faillite éthique ?

- Amoralité, psychopathie : rares
- Intérêt (argent, ambition)
- Solitude
- Obéissance, respect aveugle de la hiérarchie
- Déresponsabilisation
- Ne pas se poser de questions, cesser de réfléchir



Concept de *banalité du mal* mis en lumière par Hannah Arendt

Le renoncement éthique est très souvent... médiocre

$ find . -type f -exec grep -Il 'Pire exemple médiatique récent' {} \;

```
114   numSyms = 0;
115   nRefSegs_1 = nRefSegs;
116   refSegs_1 = (int *)refSegs;
117   v28 = nRefSegs;
118   do
119   {
120     Segment = (JBIG2SymbolDict *)JBIG2Stream::findSegment(this, *refSegs_1);
121     if ( !Segment )
122     {
123       v47 = (*(__int64 (__fastcall **)(JBIG2Stream *))(*(_QWORD *)this + 40LL))(this);
124       error(v47, "Invalid segment reference in JBIG2 text region");
125       j__free(*(void **)v106);
126       operator delete(v106);
127       return;
128     }
129     v30 = Segment;
130     if ( Segment->vfptr->getType(Segment) == jbig2SegSymbolDict )
131     {
132       numSyms += v30->size;
133     }
134     else if ( v30->vfptr->getType(v30) == jbig2SegCodeTable )
135     {
136       GList::append(v106, v30);
137     }
138     ++refSegs_1;
139     --v28;
140   }
141   while ( v28 );
142   v89 = v12;
143   v91 = v14;
144   v31 = 0;
145   if...
146   syms = (_QWORD *)gmallocn(numSyms, 8u);
147   i_1 = 0LL;
148   k = 0LL;
149   do
150   {
151     seg = (JBIG2SymbolDict *)JBIG2Stream::findSegment(this, refSegs[i_1]);
152     if ( seg
153       && (symbolDict = seg, seg->vfptr->getType(seg) == jbig2SegSymbolDict)
154       && (size = symbolDict->size, (_DWORD)size) )
155     {
156       bitmaps = symbolDict->bitmaps;
157       do
158       {
159         v40 = (__int64)*bitmaps++;
160         kk = (unsigned int)(k + 1);
161         syms[(unsigned int)k] = v40;          // crash here !!!
162         LODWORD(k) = k + 1;
163         --size;
164       }
165       while ( size );
166     }
167     else
168     {
169       kk = k;
170     }
171     ++i_1;
172     k = kk;
173   }
174   while ( i_1 != nRefSegs_1 );

00085228 __ZN11JBIG2Stream17readTextRegionSegEjiijPjj:161 (181D6E228)
```

Pegasus – NSO Group

- Framework offensif iOS et Android
- Depuis 2014. Forbidden Stories, juillet 2021 / Citizen Lab - Amnesty International
- Liens malveillants, SMS, WhatsApp, iMessages – exploits zero-click, accès au terminal…
- Au moins 45 pays clients, dont des démocraties
- L’exportation nécessite l’accord de l’État israélien
- Sensé n’être utilisé que contre des délinquants et des terroristes, dans un cadre légal. Mais sert à espionner des journalistes, opposition, politiques, avocats, activistes...
- Serait lié à au moins 300 actes de violences physiques. Dont des meurtres.

L’essentiel des informations provient de l’excellente enquête du New Yorker, 18 avril 2022:
https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

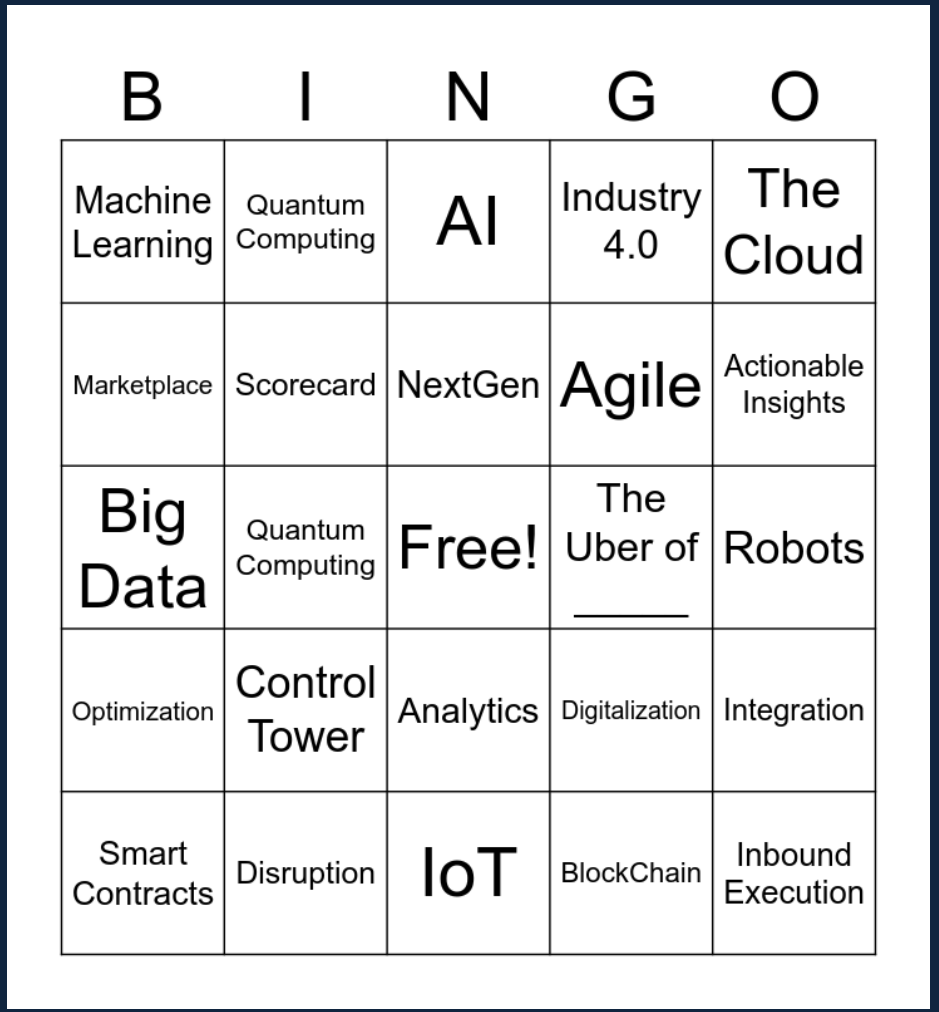
Leur défense ?

- La légalité, absence de régulation
- Autorisation d’exportation. Mais : “*Israeli export control was not dealing with ethics. It was dealing with two things. One, Israeli national interest. Two, reputation.”*

Comment a réagi le personnel ?

- *“The company has a very strong narrative that it tries to sell internally to the employees”*
- Des démissions, mais d’autres ont réaffirmé leur loyauté à l’entreprise et leur conviction que leur outil était utile pour attraper des criminels
- Le meurtre de Jamal Khashoggi en octobre 2018 a permis à certains employés de se réveiller et de comprendre ce qui se passait : idée de seuil intolérable.

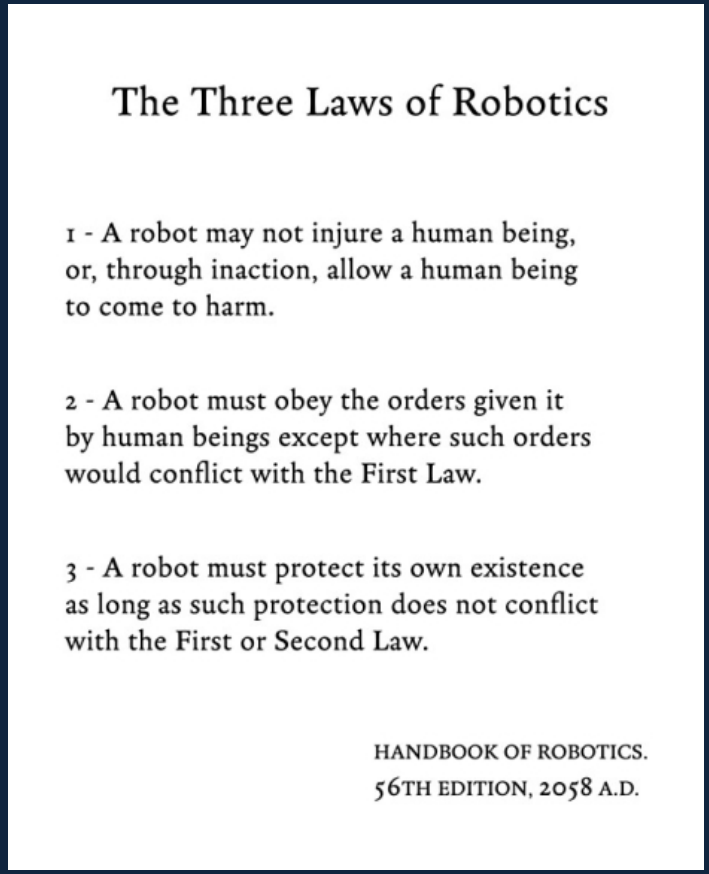
Ailleurs



B	I	N	G	O
Machine Learning	Quantum Computing	AI	Industry 4.0	The Cloud
Marketplace	Scorecard	NextGen	Agile	Actionable Insights
Big Data	Quantum Computing	Free!	The Uber of _____	Robots
Optimization	Control Tower	Analytics	Digitalization	Integration
Smart Contracts	Disruption	IoT	BlockChain	Inbound Execution

Surveillance, *smart contracts,* IA, collecte de données...

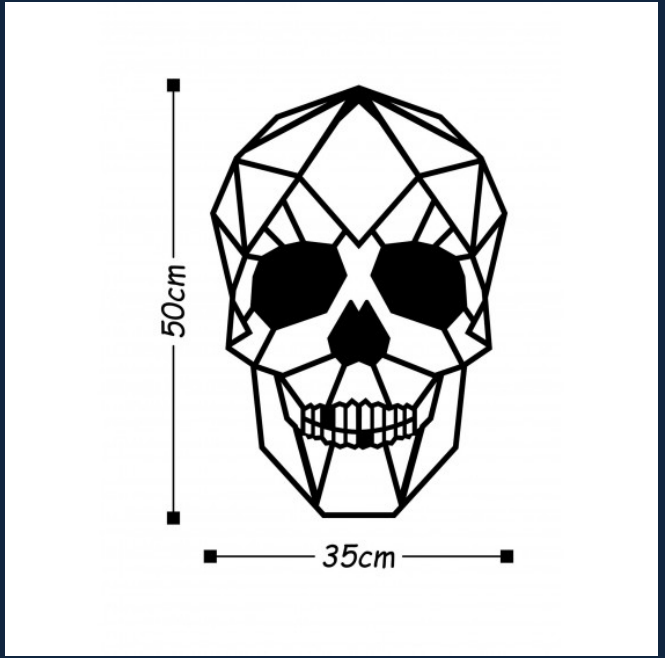
- Société de la surveillance, privée et étatique
- Commercialisation de données : est-il éthiquement raisonnable de laisser faire des entreprises dont le *business* est de vendre nos données ?
- *smart contracts* : déclencher des actions automatiques : perte de la liberté de ne pas faire
- IA : les décisions importantes ne devraient jamais être laissées aux ordinateurs, car ils manqueront toujours de qualités humaines telles que la compassion et la sagesse (Joseph Weizenbaum)



Isaac Asimov, 1942

Retour sur Pegasus - NSO

« One solution was to expand the product line. The company demonstrated for me an artificial-intelligence tool, called Maestro, that scrutinizes surveillance data, builds models of individuals' relationships and schedules, and alerts law enforcement to variations of routine that might be harbingers of crime. "I'm sure this will be the next big thing coming out of NSO […] Turning every life pattern into a mathematical vector. »



$ gcc -Wall -o programme_ethique -c code_ethique.c

Peut-on imaginer un code cyberéthique ?

« Science de la morale » ?

Un vrai code, pour nous aider ?

L’éthique renvoie au libre arbitre, qui, du point de vue cognitif, consiste à maximiser, optimiser une satisfaction entre des valeurs auxquelles nous croyons

Différence essentielle entre décider et choisir
(Joseph Weizenbaum, *in Puissance de l'Ordinateur et Raison de l'Homme, 1976*)

- Décider = calcul
- choisir = jugement, facteurs non exacts, comme les émotions

Donc, non

Use case éthiques

Penser des cas éthiques, comme on pense des *use case* pour développer :

Les cas simples : je fais des choses contraires à mes principes essentiels / je suis en totale adéquation avec mes principes

Les cas compliqués sont ceux de l’entre-deux

Quand le travail au quotidien est OK, mais que la finalité, ou le produit final de ce sur quoi je travaille est *dirty*

Notion de *distance éthique*

https://app.sli.do # 234 732

Retour sur l’*embûche à l’embauche*

Vous êtes analyste sécurité, dans mon équipe ; seul au bureau ; vous avez accès au SIEM, qui contient les traces de l’activité de tous les utilisateurs ; une charte informatique décrit précisément les conditions d’accès aux traces : il doit y avoir une demande écrite, signée par DRH / RSSI / DPO ; arrive un directeur général, votre N+3 ou 4, qui vous demande de lui montrer les sites visités la veille par un utilisateur ; vous essayez de me contacter, mais sans succès ; le directeur s’impatiente, rappelle qu’il est le chef du DRH, du RSSI et du DPO ; vous êtes seul, vous devez décider.

Que faites-vous ?

https://app.sli.do
234 732

Question d’environnement

Vous êtes *pentester ;* vous avez de fortes convictions concernant les questions environnementales. Votre employeur vous propose une mission d’audit au sein d’une entreprise dont l’activité à un impact environnemental très nocif. Vous lui expliquez que vous préférez ne pas le faire. Il vous explique qu’il a besoin de vous, et, d’ailleurs, que ça fait longtemps qu’il ne vous a pas augmenté, ce sera +15 % après la mission.

Que faites-vous ?

https://app.sli.do
234 732

Contrôle fiscal

Vous êtes responsable sécurité d'une entreprise. Au cours de vos contrôles, vous détectez les actions d'un collaborateur qui collecte des données sensibles de façon suspecte. Vous investiguez. Certains de ses messages indiquent clairement qu'il s'apprête à révéler la couverture, par des cadres de l'entreprise, d'une vaste fraude fiscale.

Que faites-vous ?

https://app.sli.do
234 732

Quelles *stratégies* face aux questions éthiques ?

En évitant l'*ethicalwhashing*

Gestion des *fails* éthiques

Les neurosciences semblent montrer qu'en cas de désaccord entre la pensée et les actes

→ mal être

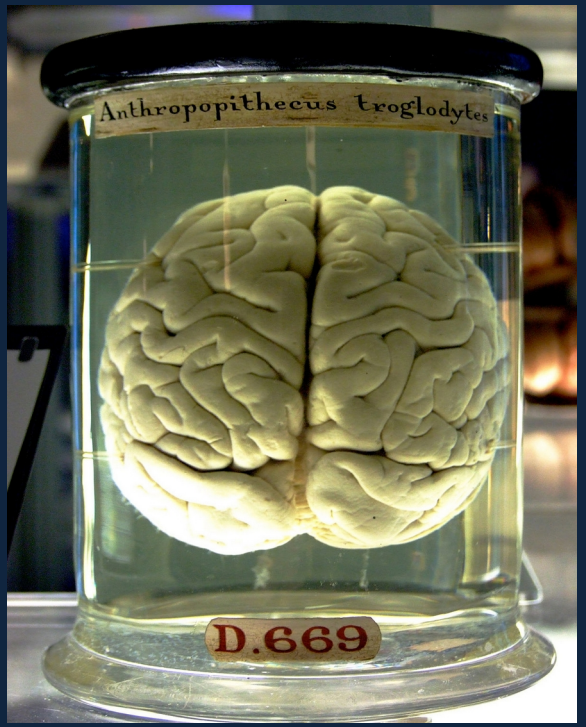
→ modification des actes ou de la pensée

Modifier la façon de penser est plus simple

Processus souvent inconscient

Ce qui peut expliquer la cécité flagrante d'esprits brillants

Alternative : vivre avec de hauts degrés de contradictions, par exemple en remettant à *plus tard* leur résolution



Gestion des *fails* éthiques

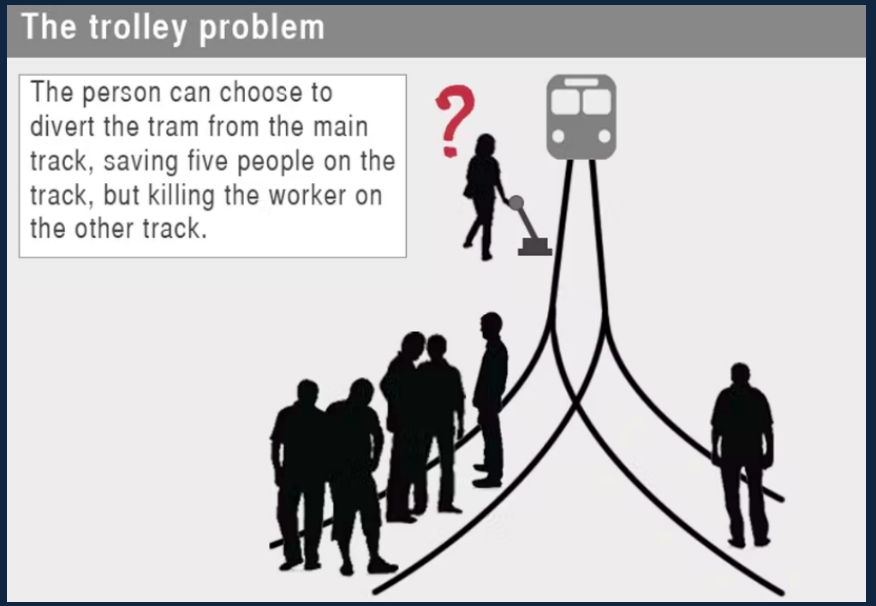
- Je nie la contradiction, je déclare qu'elle est fausse, inexistante
- Je n'en vois pas, c'est-à-dire que je ne la saisis pas
- Je la perçois, mais ne veux pas me poser de questions, je n'en fais rien
- Je la vois, mais je mens - *ethicalwashing*
- Je compense (je fais du *dirty*, mais, par ailleurs, je soulage ma conscience), ou je remets à plus tard leur résolution
- Je ne la vois pas mais on me la fait voir
- Je la vois et je modifie ma façon de penser
- Je la vois et je modifie ma façon d'agir

Conclusion

Valeurs évidentes dans le cyber : dextérité technique, économie / gains, culture / reconnaissance, sécurité *en soi*...

Empathie, fraternité, sororité, égalité, liberté, solidarité, dignité humaine, tolérance, non-violence, libre consentement, protection des données personnelles, utilité sociale, biens communs, protection de l'environnement, régulation...

Boussole uniquement technique et économique : peu de problèmes éthiques



Conclusion

L’éthique ressemble à la confiance : elle se pratique, elle se vérifie

Peut-on imaginer une sorte de *Common decency* ? Une sorte de CyberNethiquette (RFC 1855) ? Des comités de cyberéthique ?

- **Toujours penser par soi même**
- **Se fixer des seuils, des limites *a priori***
- **Être prêt à désobéir**
- **Empathie, i.e se mettre à la place d’autrui**

JSSI - 10 mai 2022

¡ Merci !

¿ Questions ?

iro@cryptosec.org | @secucrypt