NOTE STRATÉGIQUE N° 1

INSTAURER LA CONFIANCE ENVERS LA CYBERSÉCURITÉ EUROPÉENNE

Confiance et cybersécurité

Dans ce document visuel, nous présenterons quelques-uns des concepts essentiels issus des publications interdisciplinaires concernant la confiance et la fiabilité.

Nous montrerons que la cybersécurité forme une condition fondamentale de la confiance dans le numérique. Par ailleurs, nous analyserons un cas où la confiance favorise la cybersécurité et un cas où le manque de confiance nuit à cette dernière.

- Confiance interpersonnelle
- Confiance et fiabilité
- Éléments moraux et amoraux de la confiance et de la fiabilité
- Confiance contre sanctions

Permet :

- Confidentialité
- Intégrité
- Disponibilité
- Absence de liaison
- Possibilité d'intervention
- Transparence

Faire confiance à quelqu'un par opposition à se fier à quelque chose

La confiance et la fiabilité forment des boucles de rétroaction positive

Faire confiance à d'autres (la confiance interpersonnelle) entraîne une relation plus dynamique que de se fier à des mécanismes et des systèmes.

La confiance interpersonnelle (personnes/organisations) est dynamique : les personnes fiables réagissent de manière différente avec les personnes qui leur font confiance (Pettit 1995).

Fiabilité : morale ou non ?

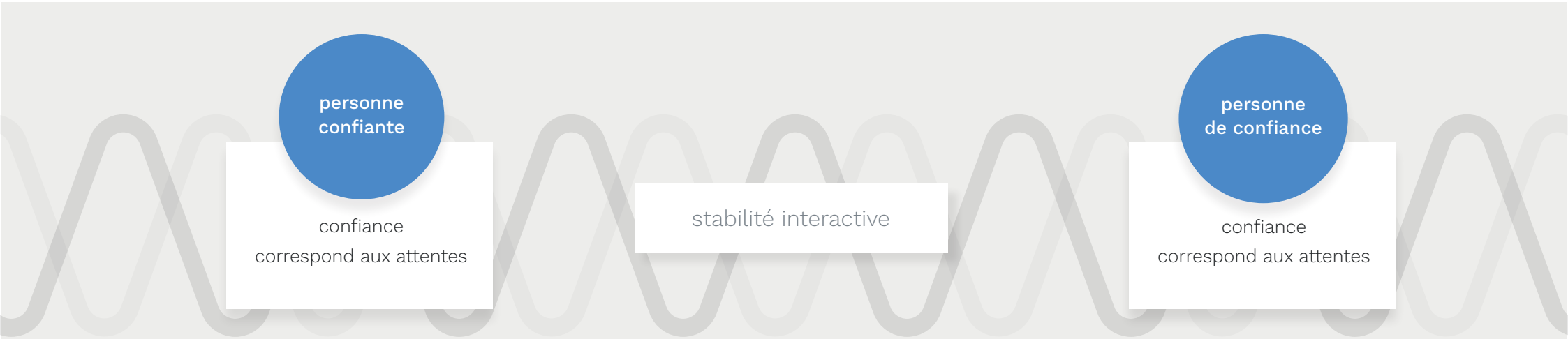
Certaines personnes souhaitent se montrer fiables pour des raisons tant morales qu'amorales.

Confiance et réputation

Certaines personnes veulent être fiables par désir de jouir d'une bonne réputation (Pettit 1995). Cette motivation est amorale (mais non immorale). Plus les relations sociales reposent sur un lien de confiance et plus la réputation devient importante.

Confiance et obligations morales

Certaines personnes s'efforcent d'être fiables en raison de leurs obligations morales, car obtenir la confiance de quelqu'un implique de devoir répondre à des attentes. Ne pas satisfaire ces attentes revient souvent à trahir la confiance de l'autre (Baier 1986).



L’aspect dynamique de la confiance interpersonnelle

La transparence du caractère et des actions des agents (personnes et organisations) influe sur l’instauration d’une « méta-confiance » (Baier 1986), cette confiance interpersonnelle dont nous dépendons pour accomplir d’importants objectifs sociaux.

La confiance mutuelle implique des responsabilités réciproques

En possession d’informations complètes, seuls les agents fiables survivent.

En l’absence de telles informations, les stratégies égoïstes remportent plus de succès que les approches équitables et coopératives.

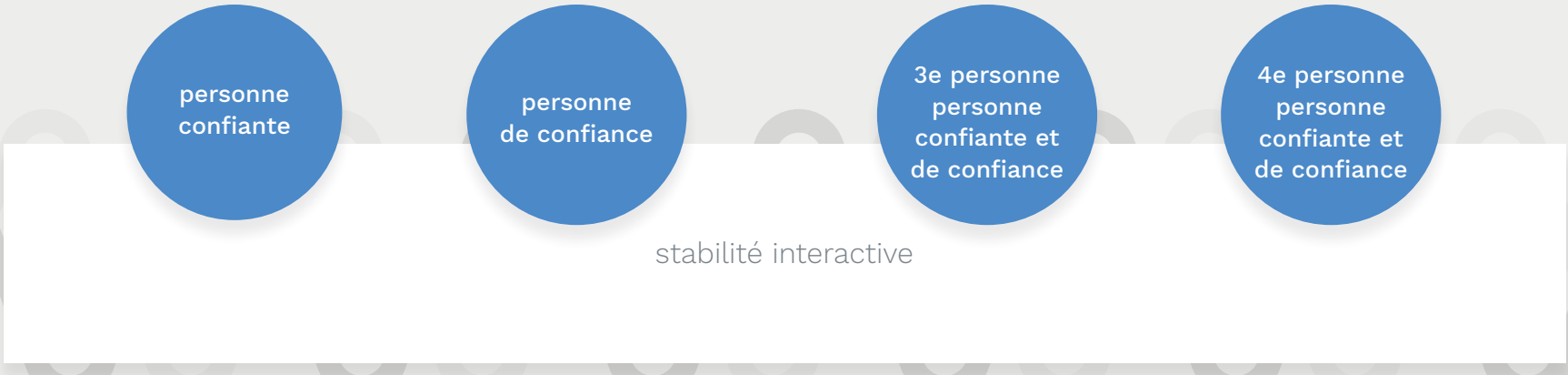
Faire confiance à des agents fiables permet d’établir de vastes réseaux de confiance mutuelle

S’il n’est pas possible de distinguer les agents fiables des autres, nous ne pouvons plus développer de coopération fondée sur la confiance mutuelle (Olson 2000).

Ainsi, la transparence du caractère et des actions des tiers renforce leur fiabilité.

Informations

personne fiable ou non



La confiance suppose de croire aux vertus d'une autre personne

Faire confiance à une autre personne implique de s'en remettre à sa bienveillance, sa diligence, son respect de la réciprocité et son engagement envers la justice (Becker 1996).

La confiance comprend également des aspects non cognitifs :

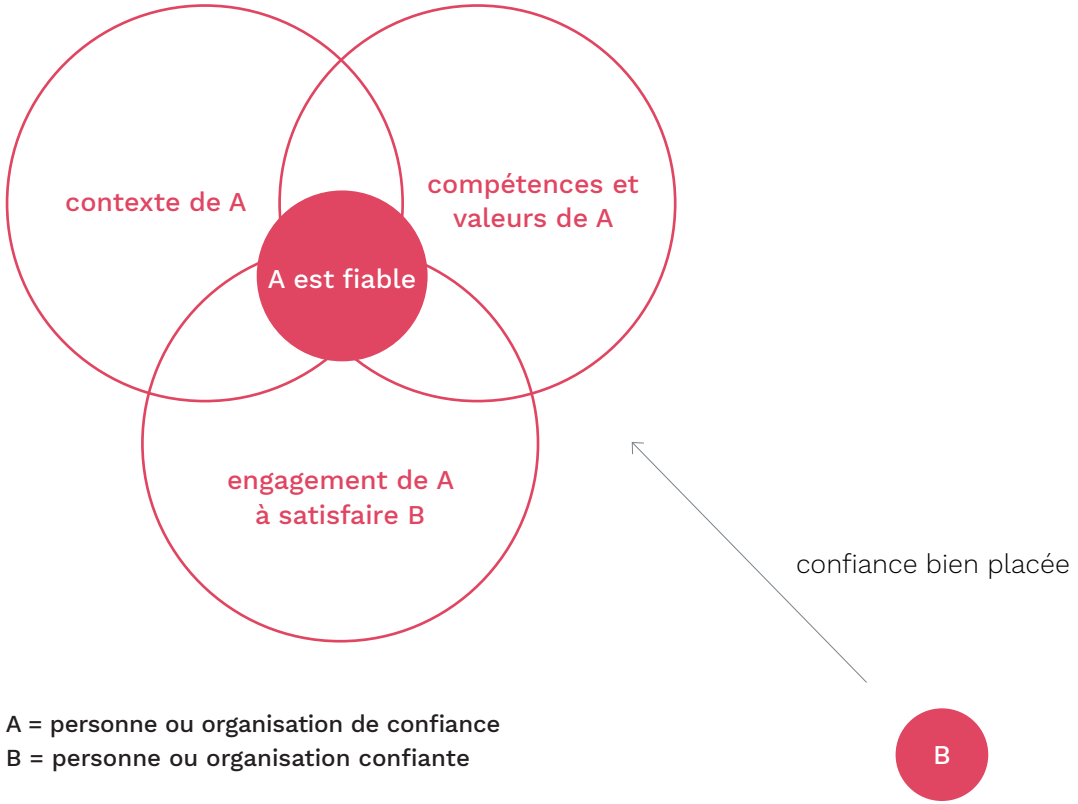
Prendre un risque

Faire confiance à quelqu'un, c'est aussi miser sur le fait que ce dernier se montrera coopératif, alors qu'aucune prédiction fondée sur la rationalité de la « maximisation de son utilité » (maximisation de ses propres intérêts) n'est possible (Held 1968).

Optimisme

Il faut se montrer optimiste quant au fait que la bonne volonté et les compétences d'une autre personne se retrouveront dans notre relation avec celle-ci (Jones 1996), notamment en prévision de futures interactions (Olson 2000).

Cet optimisme n'est pas strictement rationnel, mais il n'est pas non plus insensé. Un nombre colossal d'expériences montrent que les humains peuvent aussi établir des relations de confiance mutuelle dans des situations où la coopération ne semble pas rationnelle pour les intérêts de chacun (Olson 2000).



A = personne ou organisation de confiance
B = personne ou organisation confiante

Confiance contre recours rationnel fondé à la prévention des sanctions

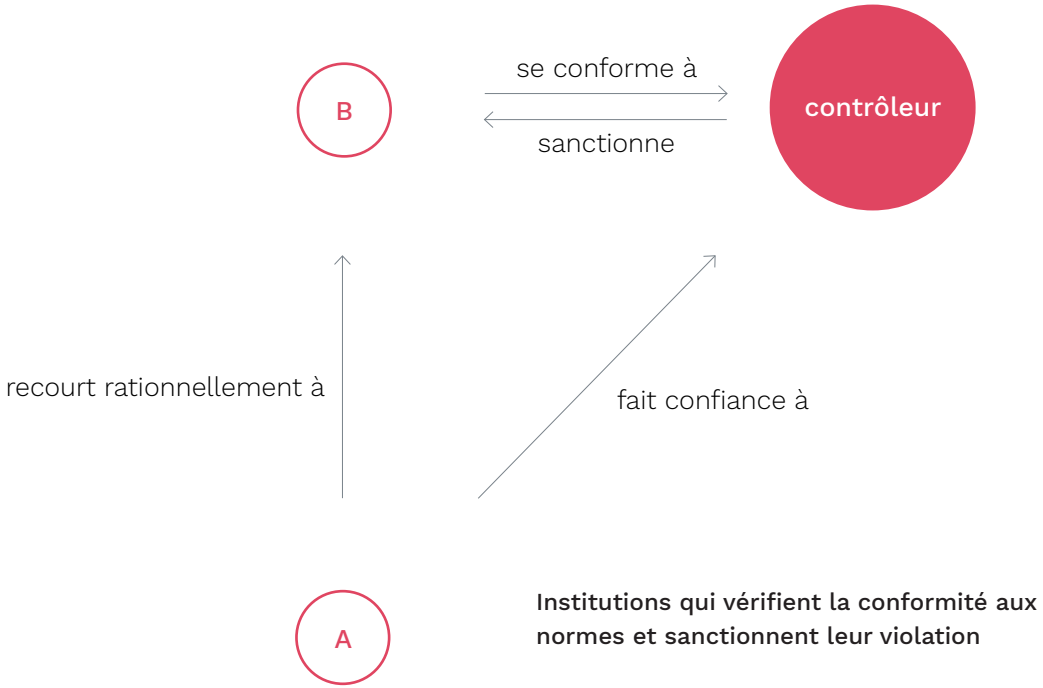
Les institutions juridiques et les incitations économiques produisent un type différent de fiabilité

Il est possible de distinguer les parties fiables des autres lorsque ces dernières sont sanctionnées par des institutions. Ces institutions représentent des mécanismes de responsabilisation externes.

Le recours rationnel réduit les incertitudes et le besoin de se reposer sur la confiance mutuelle.

La confiance et le recours rationnel ne fonctionnent pas toujours bien ensemble.

Cependant, les études empiriques montrent que les sanctions et les incitations économiques pourraient être considérées plus fiables que les motivations sociales et morales (Frey 1994). Les gens peuvent avoir plus de difficulté à établir une relation de confiance mutuelle au renforcement réciproque si ceux qui trahissent la confiance des autres ne sont plus sanctionnés (Frohlich, Norman, et Joe A. Oppenheimer 1996, Ostrom 2000).



La cybersécurité en tant que vecteur de confiance

Les éléments de la cybersécurité

Intégrité
Les données (confidentielles) et les services qui traitent de telles données ne peuvent être modifiés de manière non autorisée ou non détectée.

Disponibilité
L'accès aux données (confidentielles) et aux services qui traitent de telles données est toujours accordé de manière compréhensible, traitable et opportune.

Confidentialité
Les entités non autorisées ne peuvent pas accéder aux données (confidentielles) et aux services qui traitent de telles données.

Mécanismes vecteurs de confiance

Transparence
Les relations fondées sur la confiance mutuelle peuvent s'épanouir lorsqu'il est possible de reconnaître les agents dignes de confiance (personnes et organisations).

Réputation
Les systèmes de réputation offrent des motivations amorales à se montrer fiable.

Sincérité
Il est difficile de faire confiance à un agent face à des signaux incertains concernant sa fiabilité.

Confidentialité (pour des individus et des groupes)
La confiance mutuelle permet et favorise le partage d'informations confidentielles. Mais cela est uniquement durable tant que les informations peuvent être tenues à l'écart des parties non fiables.

Les institutions ont un effet sur la confiance des citoyens envers les acteurs de la cybersécurité

Les lois ainsi que les normes et pratiques sociales efficaces alimentent les attentes rationnelles et les composantes émotionnelles de la confiance

Acteurs impliqués dans la prévention, l'enquête et la répression de la cybercriminalité

Nationaux (exemples)	UE (exemples)
– Autorités compétentes pour SRI (sécurité des réseaux et des systèmes d'information) – CERTs266 – Forces de police – Unités de cybercriminalité – Agences de défense et de sécurité	– ENISA – CERT-UE – EP3R – EC3 (Europol) – CEPOL – Eurojust – SEAE – AED

Pays dotés de mesures législatives nationales relatives à la cybersécurité

– Allemagne (2011)
– Autriche (2013)
– Croatie (2015)
– Espagne (2013)
– Estonie (2014)
– Finlande (2013)
– France (2015)
– Hongrie (2013)
– Italie (2013)
– Lettonie (2013)
– Lituanie (2011)
– Luxembourg (2018)
– Malte (2015)
– Pays-Bas (2014)
– Pologne (2013)
– République de Chypre (2012)
– République slovaque (2015)
– République tchèque (2015)
– Royaume-Uni (2016)

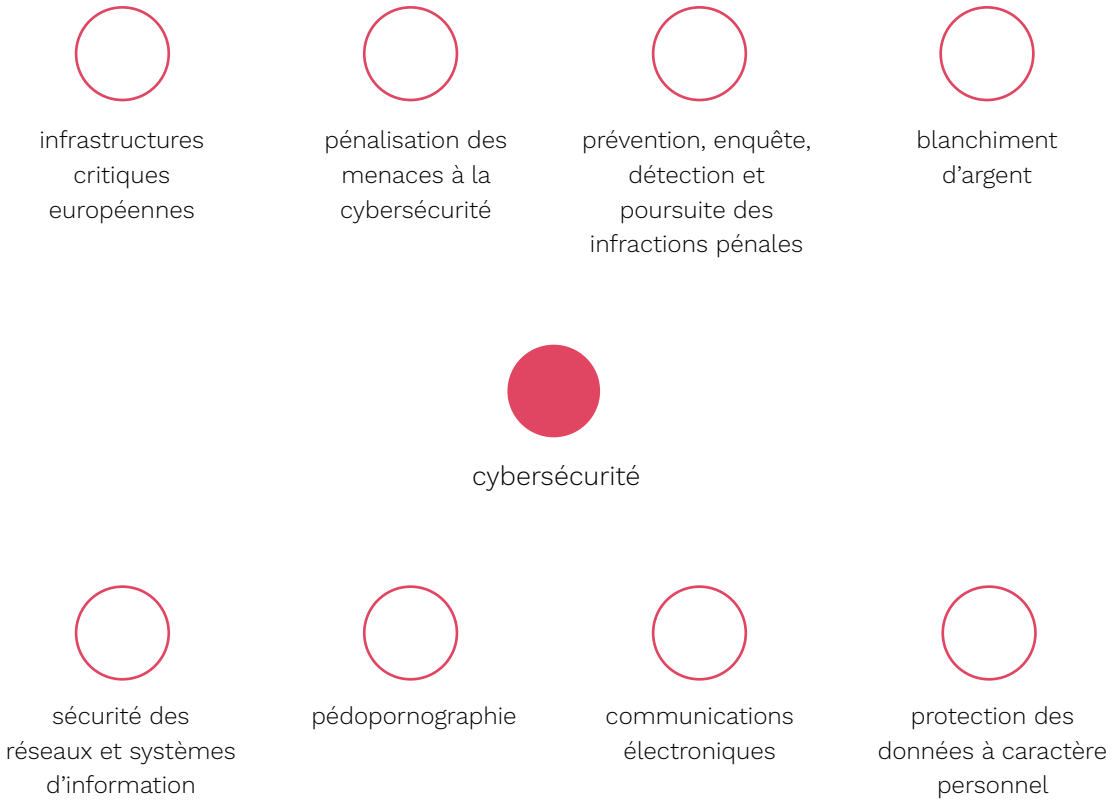
Mesures législatives européennes sur la cybersécurité

– Proposition d'un nouveau règlement de la cybersécurité (12 sept. 2018)
– Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD)
– Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009
– Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011
– Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013
– Directive (UE) 2015/849
– Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016
– Directive 2008/114/CE du Conseil
– Règlement No 611/2013 de la Commission du 24 juin 2013
– Directive (UE) 2016/1148 du Parlement européen et du Conseil

La réglementation en matière de cybersécurité possède plusieurs facettes

Les mesures législatives européennes sur la cybersécurité traitent de différents aspects de cette dernière

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD)
- Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009
- Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011
- Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013
- Directive (UE) 2015/849
- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016
- Directive 2008/114/CE du Conseil
- Règlement No 611/2013 de la Commission du 24 juin 2013
- Directive (UE) 2016/1148 du Parlement européen et du Conseil



Première étude de cas – Piratage éthique et confidentialité des données (1/3)

Bien souvent, la meilleure manière de détecter des vulnérabilités est de faire confiance à un pirate informatique éthique.

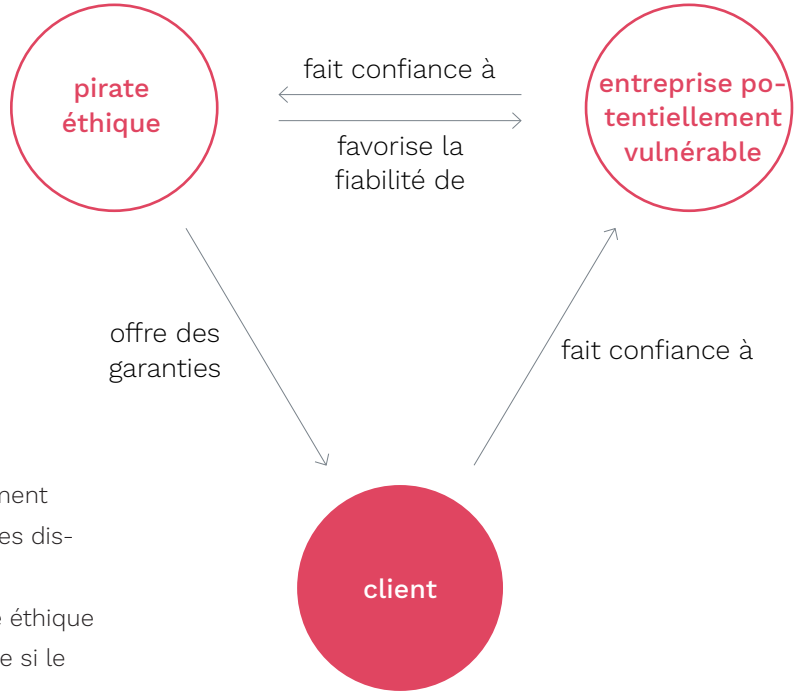
Piratage éthique

Les pirates éthiques (aussi appelés « chapeaux blancs » ou « white hats ») utilisent les mêmes outils et techniques que les pirates malveillants afin de mettre à l'épreuve la cybersécurité d'une entreprise, à la demande et avec la permission de cette dernière.

Un dilemme en matière de confidentialité

Lorsqu'il effectue des tests de pénétration, le pirate éthique obtient l'accès aux données à caractère personnel du client. Aussi, le client prend le risque que le pirate utilise ces informations confidentielles à mauvais escient intentionnellement ou qu'il les divulgue par négligence.

Seul un pirate en qui vous pouvez avoir confiance vous sortira de ce dilemme : un pirate fiable agira avec bienveillance, compétence et de manière consciencieuse.



Un cercle de confiance vicieux ?

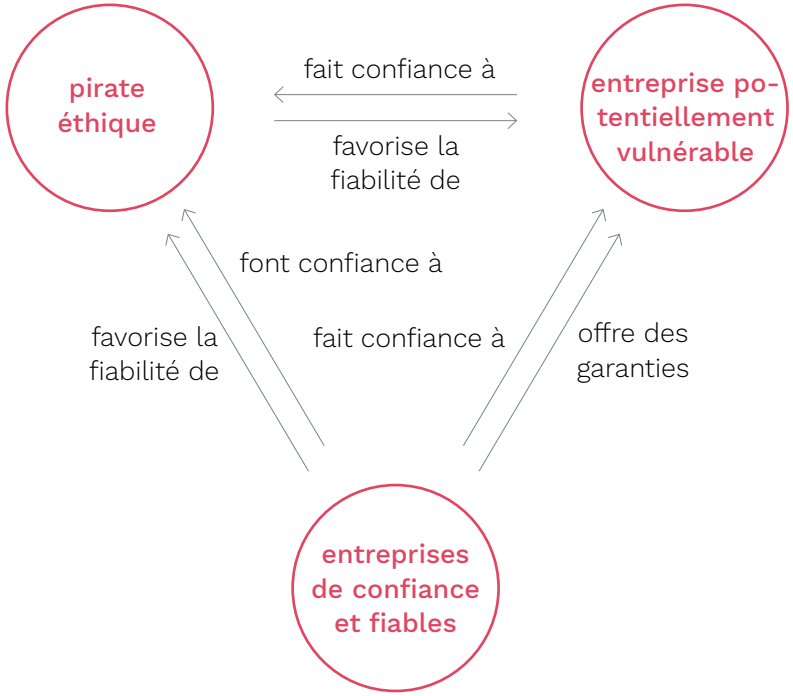
- Une entreprise peut être jugée fiable uniquement après avoir réalisé des tests appropriés sur ses dispositions en matière de cybersécurité.
- Les tests de pénétration menés par un pirate éthique ne contribuent à la fiabilité de l'entreprise que si le pirate est fiable lui-même.
- Comment une entreprise peut-elle identifier les pirates fiables ? Et comment le client peut-il le savoir ?

Première étude de cas – Piratage éthique et confidentialité des données (2/3)

La fiabilité se répercute à travers les réseaux de confiance

Comment peut-on établir la fiabilité d'un pirate éthique ?
Il peut s'avérer compliqué de savoir si un pirate est digne de confiance. En pratique, toutefois, la confiance sera davantage rationnelle si les entreprises ayant des besoins semblables en matière de cybersécurité et entretenant une relation de confiance partagent des informations sur les pirates éthiques. Un groupe d'entreprises se faisant confiance (et étant fiables) peut partager des renseignements indiquant que tel hacker est digne de confiance.

Du point de vue du client :
Les sociétés au courant qu'une certaine entreprise appartient à un groupe d'entreprises entretenant une relation de confiance ont de bonnes raisons de penser que cette entreprise a adopté des pratiques appropriées en matière de cybersécurité (p. ex., en engageant des pirates éthiques fiables), notamment si le groupe est réputé pour partager les meilleures pratiques. D'autres indicateurs de fiabilité peuvent se retrouver dans les certifications, y compris dans les programmes d'auto-certification.



Première étude de cas – Piratage éthique et confidentialité des données (3/3)

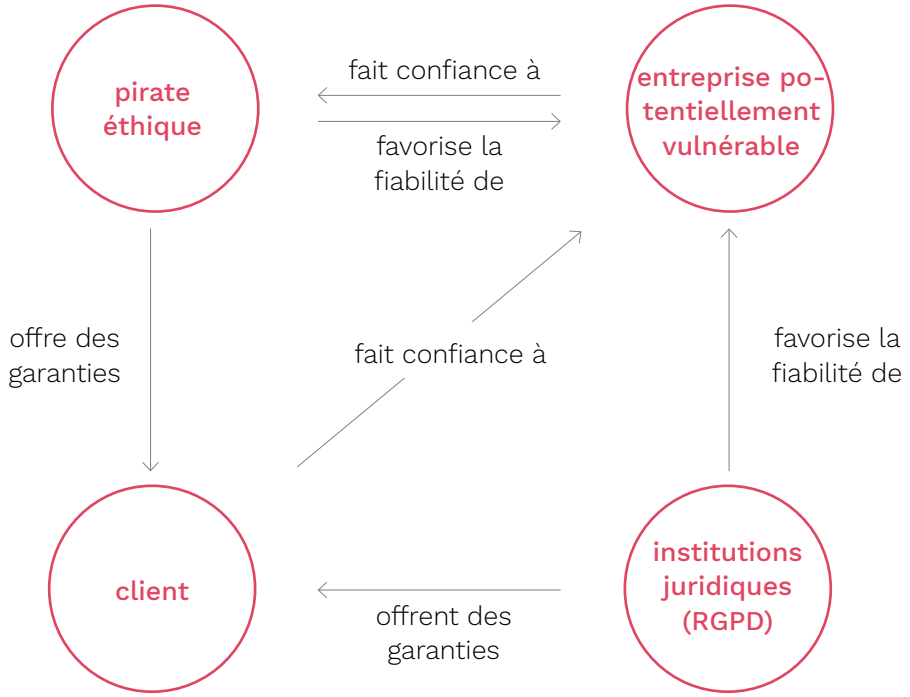
Quel rôle jouent les institutions juridiques ?

Les obligations juridiques contribuent à établir la fiabilité des acteurs

Le RGPD impose aux entreprises de garantir des niveaux appropriés de cybersécurité. Cette obligation motive les entreprises à assurer leur cybersécurité, ce qui participe à améliorer leur fiabilité et, à long terme, la confiance qu'elles reçoivent.

Dans certains contextes (comme les données relatives à la santé), les clients peuvent avoir des attentes précises à propos de la confidentialité de leurs données (p. ex., qu'elles ne soient consultées que par leur médecin traitant). La protection de la confidentialité ne devrait pas être considérée comme un ennemi de la cybersécurité ni comme une excuse pour abandonner cette dernière.

Il convient de répondre aux attentes des clients en matière de confidentialité à l'aide d'une communication efficace. Par exemple, l'accès par un pirate éthique à des données de patients identifiables doit être communiqué (c'est également une obligation juridique prévue dans le RGPD), ainsi que toute technique utilisée pour protéger la confidentialité de ces données au cours du processus.



Deuxième étude de cas – Gouvernements utilisant des exploits « jour-zéro » (2/3)

Une course au cyber-armement où le besoin de sécurité nuit à la confiance

Une nouvelle façon d'attaquer et d'espionner ses ennemis

Les exploits « jour-zéro » (attaques basées sur des failles de sécurité découvertes et utilisées le jour-même avant qu'un remède n'ait été trouvé) représentent une forme d'arme, car ils peuvent perturber les ordinateurs et leur réseau, mais aussi fournir l'accès à des informations importantes. Les gouvernements achètent des exploits « jour-zéro » pour attaquer ou espionner d'autres pays ou ennemis.

Aucune relation dynamique comme celle existant dans la confiance

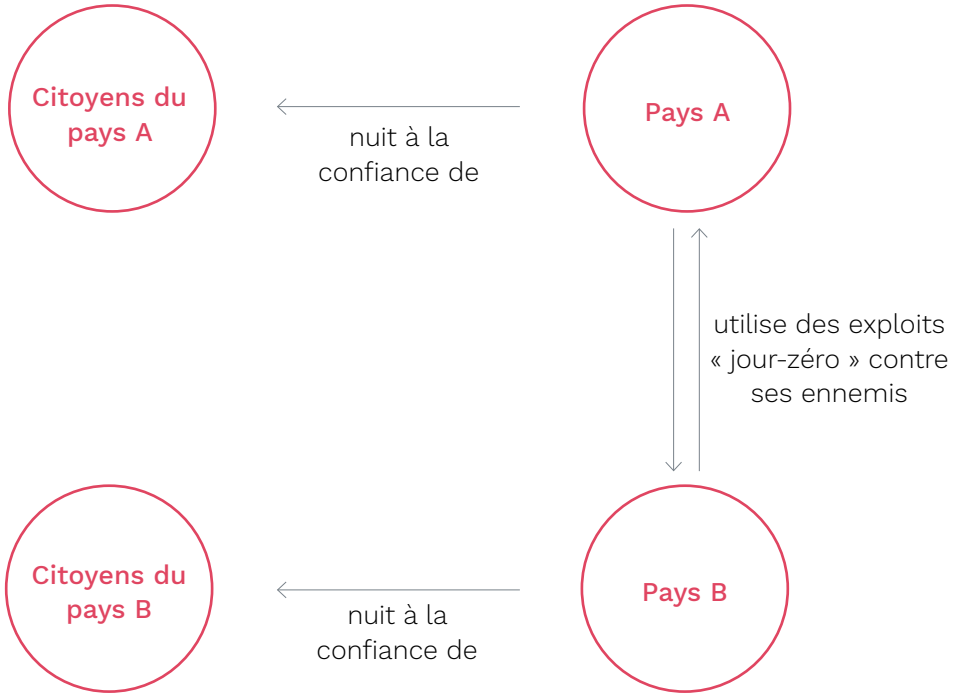
Si chaque gouvernement cherche des vulnérabilités dans les autres pays pour se protéger, cela nuira à la sécurité de tous les pays à long terme. La recherche de « cyber-vulnérabilités » dans les autres pays rend impossibles les relations de confiance entre les pays.

Les chiffres ci-dessous représentent les retombées positives escomptées pour la défense nationale (p. ex., les économies réalisées dans les dépenses traditionnelles, exprimées en millions de dollars).

	Pays B	Utilise des exploits	N'utilise pas d'exploit
Pays A	Utilise des exploits	-100,-100	100,-300
	N'utilise pas d'exploit	-300,100	30,30

Les effets externes de l'utilisation d'exploits « jour-zéro » sur la fiabilité (3/3)

Si les gouvernements ne dévoilent pas les vulnérabilités trouvées à l'aide d'exploits « jour-zéro » dont ils ont connaissance, les citoyens peuvent-ils leur faire confiance ? Les citoyens peuvent-ils être sûrs que les gouvernements ne les utiliseront pas pour les surveiller ?



Garantir la confiance en la cybersécurité : les défis

Compromis commercial (utilité contre sécurité)

- La sécurité et la protection des données constituent des coûts pour les entreprises axées sur les données.
- Course à l'armement pour les stratégies offensives
- Les utilisateurs ne sont pas prêts à accepter les coûts en matière d'utilisation associés à une cybersécurité élevée
- Les systèmes informatiques sur lesquels se reposent les entreprises sont de plus en plus vulnérables

Compromis en matière d'application de la loi (confidentialité contre sécurité)

- Atteinte à la vie privée
- Caractère intrusif des outils de sécurité nuisant au respect de la vie privée
- Les vulnérabilités sont vendues aux gouvernements sur les marchés gris et noirs
- Les exploits informatiques d'accès légal peuvent représenter une faille exploitable pour des parties malveillantes
- De nombreuses mesures de cybersécurité reposent sur la surveillance
- Risque d'utilisation abusive
- Mesures offensives susceptibles d'affaiblir la sécurité de tous

Compromis en matière de réglementation (complexité contre sécurité)

- Identification difficile des intervenants pour les incidents de cybersécurité
- Conditions d'encadrement juridique et factuel souvent obscures
- Technologies qui évoluent rapidement
- La cybersécurité est un problème mondial très complexe
- Conséquences d'événements imprévisibles et variables

Défis étudiés dans Jasmontaite et al. 2017

Où trouver de plus amples informations

Les diapositives sont fondées sur les travaux de recherche menés par le projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs).

L'objectif du projet CANVAS est de réunir les parties prenantes des domaines clés de la stratégie numérique pour l'Europe afin de relever le défi consistant à définir les modalités d'alignement de la cybersécurité sur les valeurs européennes et les droits fondamentaux.

CANVAS fournit notamment les ressources suivantes :

- Documents d'information
- Programme de référence du projet CANVAS
- CANVAS MOOC
- Livre en libre accès
  « L'éthique de la cybersécurité »

La diapositive suivante présente nos livres blancs abordant les détails des défis de la cybersécurité.

Bibliographie : les défis de la cybersécurité (livres blancs de CANVAS)

Défis éthiques

Yaghmaei, Emad, Ibo van de Poel, Markus Christen, Bert Gordijn, Nadine Kleine, Michele Loi, Gwenyth Morgan et Karsten Weber. 2017. “Canvas White Paper 1 – Cybersecurity and Ethics.” Document universitaire SSRN No 3091909. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091909.

Défis juridiques

Jasmontaite, Lina, Gloria González Fuster, Serge Gutwirth, Florent Wenger, David-Olivier Jaquet-Chiffelle et Eva Schlehahn. 2017. “Canvas White Paper 2 – Cybersecurity and Law.” Document universitaire SSRN No 3091939. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091939.

Défis technologiques

Domingo-Ferrer, Josep, Alberto Blanco, Javier Parra Arnau, Dominik Herrmann, Alexey Kirichenko, Sean Sullivan, Andrew Patel, Endre Bangerter et Reto Inversini. 2017. “Canvas White Paper 4 – Technological Challenges in Cybersecurity.” Document universitaire SSRN No 3091942. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091942.

Bibliographie

Confiance (concept général, en philosophie)

- Held, Virginia. 1968. “On the Meaning of Trust.” Ethics 78 (2): 156–59.
- Baier, Annette. 1986. “Trust and Antitrust.” Ethics 96 (2): 231–60.
- Pettit, Philip. 1995. “The Cunning of Trust.” Philosophy & Public Affairs 24 (3): 202–25.
- Becker, Lawrence C. 1996. “Trust as Noncognitive Security about Motives.” Ethics 107 (1): 43–61.

Confiance (concept général, en sciences sociales)

- Frey, Bruno S. 1994. “How Intrinsic Motivation Is Crowded out and In.” Rationality and Society 6 (3): 334–52.
- Ostrom, Elinor. 2000. “Collective Action and the Evolution of Social Norms.” The Journal of Economic Perspectives 14 (3): 137–58.
- Frohlich, Norman, and Joe A. Oppenheimer. 1996. “Experiencing Impartiality to Invoke Fairness in the N-PD: Some Experimental Results.” Public Choice 86 (1): 117–35. https://doi.org/10.1007/BF00114878.

Confiance (en ligne, numérique)

- Erlich, Yaniv, et al. 2014. “Redefining Genomic Privacy: Trust and Empowerment.” PLOS Biology 12 (11): e1001983.
- Etzioni, Amitai. 2017. “Cyber Trust.” Journal of Business Ethics, juillet. https://doi.org/10.1007/s10551-017-3627-y.
- Chakravorti, B., Bhalla, A., Chaturvedi, R.S., 2018. The 4 Dimensions of Digital Trust, Charted Across 42 Countries. Harvard Business Review.

Informations sur le projet

Coordination du projet et contact :
PD Dr. sc. ETH Markus Christen
Université de Zurich (UZH),
Digital Society Initiative
Rämistrasse 66, 8001 Zurich

Version du document visuel :
Version 2.0 octobre 2019

Durée du projet :
sept. 2016 – oct. 2019

Partenaires :
Le consortium CANVAS comprend 11 partenaires (9 établissements universitaires et 2 partenaires extérieurs au monde universitaire) répartis dans 7 pays européens.

Financement :
1,57 million d'euros, dont 1 million financé par la Commission européenne, la partie restante provenant du Secrétariat d'État suisse à la formation, à la recherche et à l'innovation.

Avis de financement pour CANVAS

Cofinancé par le programme Horizon 2020
de l'Union européenne

Le projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs) a bénéficié d'un financement du programme de recherche et d'innovation Horizon 2020 de l'Union européenne au titre de la convention de subvention n° 700540. Ce travail a été financé (en partie) par le Secrétariat d'État suisse à la formation, à la recherche et à l'innovation (SEFRI) sous le numéro de contrat 16.0052-1. Les opinions exprimées et les arguments employés dans le présent document ne reflètent pas nécessairement les points de vue officiels de l'UE et du gouvernement suisse.