NOTE STRATÉGIQUE N° 1

INSTAURER LA CONFIANCE ENVERS LA CYBERSÉCURITÉ EUROPÉENNE

Confiance et fiabilité

Quelle est l'importance de la cybersécurité pour la confiance en ligne ? Et comment instaurer la confiance en la cybersécurité ? Nous exposerons brièvement l'essentiel des nombreux points de vue philosophiques, psychologiques et sociologiques sur le sujet de la confiance. Ensuite, nous en explorerons les implications pour la cybersécurité.

Théories relatives à la confiance

La confiance est souvent associée à des conditions de risque, d'incertitude et de vulnérabilité. Nous sommes vulnérables lorsque nous accordons notre confiance à des tiers sans avoir toutes les informations nécessaires, notamment en ce qui concerne leurs motivations et/ou leur comportement. Des spécialistes ont défini la confiance comme impliquant des engagements essentiellement moraux (Baier 1986 ; Nickel 2007) ou une convergence d'intérêts prévisible (Hardin 1992). D'autres encore invoquent des motivations qui se renforcent mutuellement, en ce sens que, par exemple, les personnes de confiance sont intrinsèquement motivées à être fiables par la confiance qui leur est accordée (Pettit 1995). La confiance est souvent contextuelle : je peux faire confiance à mon comptable pour le dépôt de mes déclarations de revenus, mais pas en tant que conseiller politique.

Une confiance bien placée ou raisonnable concerne la confiance que l'on peut accorder à des fiduciaires fiables : des fiduciaires de confiance. Une confiance bien placée est socialement bénéfique. À l'inverse, accorder sa confiance à des agents qui ne la méritent pas est généralement préjudiciable. Non seulement la confiance est difficile à gagner, mais elle est encore plus difficile à regagner une fois perdue.

La confiance possède des aspects rationnels et non rationnels. L'aspect non rationnel est une sorte d'optimisme quant aux motivations des autres (Jones 1996). Certaines personnes font confiance à des tiers au sujet desquels elles ne disposent que de peu d'informations, voire même à de parfaits étrangers. Cela permet l'émergence de formes de coopération socialement bénéfiques qui, en l'absence de telles attitudes, ne pourraient pas voir le jour (Ostrom 2000). Ces conditions sont plus faciles à mettre en œuvre dans des petits groupes où un comportement non coopératif peut être détecté (Ostrom 2000). Ainsi, il peut s'avérer impossible d'établir une coopération sociale, basée uniquement sur la confiance, dans des sociétés complexes ou sur la scène internationale (Hardin 2009).

Confiance en ligne

Aux débuts d'Internet, il semblait qu'aucune confiance en ligne ne pouvait être instaurée, en raison de l'anonymat d'Internet (Pettit 2004) : comme le disait la fameuse vignette, « *on the Internet, nobody knows you're a dog* (sur Internet, personne ne sait que vous êtes un chien) ». Avec l'Internet 2.0 d'aujourd'hui, cela n'est plus vrai. Les systèmes de commentaires en ligne et les systèmes numériques d'évaluation sociale sont tous basés sur des identités sur Internet, semi-stables et semi-vérifiables (Etzioni 2017). Ces solutions ont permis l'émergence de marchés

en ligne (eBay et Amazon, par exemple) et d'interactions dans l'économie de partage (comme AirBnB et BlaBlaCar).

Confiance interpersonnelle et institutionnelle

Un agent ou une organisation qui se révèle fiable uniquement parce qu'il ou elle craint d'être traduit(e) en justice n'est pas fiable. De nombreuses formes de confiance et de fiabilité voient le jour en l'absence d'incitations économiques directes ou de sanctions juridiques. Pourtant, dans les échanges à enjeux élevés entre de parfaits inconnus, notamment si ces échanges sont ponctuels, il est difficile d'obtenir une confiance interpersonnelle forte, car le risque est trop élevé. Concevoir un environnement et un système de réputation et d'incitations qui permettent et favorisent la confiance n'est pas une tâche facile. Des sanctions légales réellement appliquées contre les comportements malhonnêtes peuvent favoriser les relations basées sur la confiance en atténuant les risques associés à la confiance accordée à des étrangers (Hardin 1992).

Cependant, la confiance à l'égard de sanctions légales présuppose une confiance à l'égard des institutions qui appliquent ces normes.

Cybersécurité et confiance

La cybersécurité est nécessaire à la confiance

Avant d'aborder la confiance à l'égard de la cybersécurité, il est utile de démontrer que la cybersécurité est nécessaire à la confiance. Les objectifs classiques de la cybersécurité – soit la confidentialité, l'intégrité et la disponibilité – sont des conditions prérequises à la confiance dans le domaine du numérique. Du point de vue de la protection des données, l'intégrité est définie comme la propriété selon laquelle les données et les services ne peuvent pas être modifiés de manière non autorisée ou non détectée. Ainsi, l'intégrité représente un élément essentiel pour créer et maintenir la confiance envers l'information. L'intégrité des données, par exemple, est essentielle pour évaluer les services informatiques et justifier la confiance accordée aux entreprises qui fournissent de bons services. L'intégrité et la disponibilité des informations sont également nécessaires afin de vérifier l'identité numérique des personnes avec lesquelles on interagit en ligne. Si quelqu'un peut s'approprier l'identité numérique d'une autre personne en ligne, la réputation de cette dernière peut être utilisée à mauvais escient et réduire à néant la confiance en cette identité numérique.

De plus, la confiance mutuelle se caractérise par la confidentialité. La confiance permet le partage d'informations sensibles. Les personnes qui accordent leur confiance se rendent vulnérables vis-à-vis des personnes auxquelles elles font confiance, car les informations sensibles qu'elles partagent pourraient être utilisées à leur encontre. Cette relation ne peut être raisonnable qu'avec une entité digne de confiance. Par conséquent, la cybersécurité est nécessaire à la confiance en ligne : en cybersécurité, la confidentialité signifie que les données et les services ne sont pas accessibles aux entités non autorisées. La cybersécurité réduit le risque que des informations sensibles deviennent accessibles à des agents non dignes de confiance. En l'absence de cybersécurité, il ne serait pas raisonnable de partager des informations sensibles en ligne, donc de nombreuses transactions en ligne n'auraient pas lieu.

La confiance est nécessaire à la cybersécurité

Si la confiance dépend de la cybersécurité, la cybersécurité dépend également de la confiance. La confiance et la cybersécurité étant interdépendantes, il peut y avoir des cycles tant vertueux que vicieux. L'exemple du piratage éthique illustre un cercle vertueux dans lequel la confiance renforce la cybersécurité, ce qui favorise des niveaux plus élevés de confiance en ligne. Le cas des exploits « jour-zéro » (basés sur des failles gardées secrètes) présente un cercle vicieux dans lequel la méfiance initiale affaiblit la cybersécurité, ce qui sape ensuite davantage encore la confiance.

Piratage éthique

Les hackers éthiques, ou « *white hats* », sont définis ici comme des pirates informatiques qui poursuivent des objectifs légaux, tels que le fait de tester la sécurité des systèmes informatiques contre des attaques malveillantes. Dans ce cadre, ils peuvent utiliser des techniques similaires à celles employées par les pirates informatiques « malveillants », mais les *white hats* n'exploitent pas de manière criminelle les vulnérabilités informatiques ainsi identifiées à leur avantage. Les *white hats* dignes de confiance existent et sont employés par de nombreuses entreprises afin d'identifier leurs vulnérabilités. Cette forme de recherche sur la sécurité n'est possible que parce qu'au départ certaines entreprises ont été disposées à accorder leur confiance à certains hackers éthiques. Le choix d'entreprises plus favorables à la prise de risque initial profite également à d'autres entreprises moins enclines. Il est plus raisonnable de faire confiance à des hackers éthiques dont la réputation est démontrable et garantie par d'autres entreprises. Ainsi, les entreprises qui se font confiance mutuellement disposent de moyens

leur permettant d'identifier les pirates éthiques dignes de confiance. La recommandation d'une entreprise de confiance permet de croire en la fiabilité du hacker éthique. Par ailleurs, pour un pirate informatique, un environnement dans lequel il est payant de jouir d'une bonne réputation permet également d'établir la confiance grâce aux incitations intrinsèques.

La chaîne de confiance s'étend. Grâce à la confiance entre l'entreprise et le hacker éthique, les entreprises deviennent plus sûres, et donc plus fiables pour leurs clients. Les cadres juridiques généraux de la protection des données en Europe et, plus largement, l'ensemble des lois nationales et internationales encourageant la cybersécurité contribuent à la cybersécurité en ligne via la confiance institutionnelle. Les consommateurs peuvent être rassurés par le fait que les entreprises qui ne protègent pas la cybersécurité puissent être sanctionnées, estimant que les entreprises agissent de manière rationnelle afin d'éviter les sanctions. Les entreprises qui se conforment aux obligations de mettre en œuvre des mesures organisationnelles et techniques suffisantes favorisant un niveau élevé de cybersécurité sont donc plus fiables. Les lois sur la protection des données, exigeant une communication transparente avec les personnes concernées en cas de violation des données à caractère personnel, incitent également les entreprises à adopter des niveaux de cybersécurité plus élevés. Les entreprises sont davantage incitées à éviter les violations des données à caractère personnel si elles ne peuvent (légalement) dissimuler ce fait à leurs clients.

La méfiance affaiblit la cybersécurité : L'utilisation des exploits « jour-zéro » (basés sur des failles gardées secrètes)

Les vulnérabilités « jour-zéro » sont des faiblesses liées aux logiciels qui n'ont pas été identifiées avant la distribution de ces derniers. L'exploitation des « jours-zéro » s'apparente à une sorte d'arme, car elle peut perturber les ordinateurs et les réseaux, et permettre aux utilisateurs d'accéder sans autorisation à des informations pertinentes. Les gouvernements peuvent utiliser les « jours-zéro » pour les activités liées au renseignement à l'étranger, en achetant les exploits et en les déployant afin d'attaquer ou d'espionner d'autres pays ou des opposants individuels. Dans ce contexte, on peut dire que la motivation à acheter des exploits « jour-zéro » pour le cyber-espionnage contre des entités nationales découle généralement d'un manque de confiance mutuelle entre les États. Il s'agit d'un mécanisme de méfiance qui s'auto-renforce dans la mesure où entrer dans un marché dans lequel se vendent des exploits « jour-zéro » compromet à son tour la crédibilité des gouvernements qui agissent de la sorte, et ce à plus d'un titre.

Par exemple, si chaque gouvernement cherche des vulnérabilités dans les systèmes des autres pays, cela aura pour effet à long terme que chaque pays sera moins sécurisé. Non seulement cela augmente le risque que de telles vulnérabilités tombent entre les mains de criminels, mais cela peut également être considéré comme un scénario de course aux armements entre États-nations. Dans une telle situation, un pays ne peut se permettre de rester inactif, par crainte que d'autres pays n'obtiennent un avantage susceptible d'être utilisé contre lui. Ainsi, la recherche de « cyber-vulnérabilités » dans les autres pays rend impossibles les relations de confiance entre les pays. Avec la méfiance en arrière-plan, chaque État suppose à juste titre qu'une telle stratégie offensive lui est favorable, par rapport à une stratégie purement défensive, afin de prendre le dessus en matière d'activités d'espionnage ou de cybersabotage à l'étranger. De plus, un gouvernement national qui s'avère vulnérable à certains exploits informatiques peut également sembler moins digne de confiance vis-à-vis des autres pays. Lorsque des communications confidentielles de diplomates et de politiciens sont divulguées ou compromises, cela peut entraîner de graves perturbations dans les relations entre États. Par ailleurs, les gouvernements qui utilisent des exploits seront très probablement redoutés par leurs propres citoyens, au lieu de leur inspirer confiance. Après tout, si les gouvernements disposent de ces armes, leurs citoyens peuvent également devenir la proie du cyber-espionnage et du cybersabotage. Acquérir des exploits « jour-zéro » peut sembler avantageux sur le plan stratégique, voire obligatoire, dans un contexte défavorable de faible confiance internationale. Pourtant, le résultat le plus probable lié au développement ou à l'achat de ces outils est un nivellement par le bas en ce qui concerne la confiance.

Conclusions

En conclusion, la confiance et la cybersécurité se renforcent mutuellement. La confiance est bénéfique (lorsqu'elle est bien placée), mais fragile et difficile à rétablir. Les stratégies individuelles (menées par des personnes, des entreprises et des États) qui peuvent sembler rationnelles et efficaces pour protéger la sécurité nationale devraient toujours être soumises à un examen minutieux afin d'évaluer leurs effets sur la confiance, au risque de se révéler contre-productives. Dans un contexte commercial, la confiance peut être obtenue avec ou sans surveillance et sanctions légales fortes, ainsi qu'avec une combinaison équilibrée de sanctions légales et de systèmes de réputation.

Pour de plus amples informations
Références :

- Baier, Annette. 1986. "Trust and Antitrust." Ethics 96 (2) : 231–60.
- Etzioni, Amitai. 2017. "Cyber Trust." Journal of Business Ethics, juillet. https://doi.org/10.1007/s10551-017-3627-y.
- Hardin, Russell. 1996. "Trustworthiness." Ethics 107 (1) : 26–42.
- Jones, Karen. 1996. "Trust as an Affective Attitude." Ethics 107 (1) : 4–25.
- Nickel, Philip J. 2007. "Trust and Obligation-Ascription." Ethical Theory and Moral Practice 10 (3) : 309–19. https://doi.org/10.1007/s10677-007-9069-3.
- Ostrom, Elinor. 2000. "Collective Action and the Evolution of Social Norms." The Journal of Economic Perspectives 14 (3) : 137–58.
- Pettit, Philip. 1995. "The Cunning of Trust." Philosophy & Public Affairs 24 (3) : 202–25.
- 2004. "Trust, Reliance and the Internet." Analyse & Kritik 26 (1) : 108–121.

Cette note stratégique est basée sur les travaux de recherche réalisés dans le cadre du projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs). Des rapports détaillés sur ces travaux ont été publiés dans quatre livres blancs principaux :

1. Cybersécurité et éthique
2. Cybersécurité et droit
3. Attitudes et opinions concernant la cybersécurité
4. Défis technologiques de la cybersécurité

Tous les livres blancs sont consultables sur notre site Internet, avec toutes nos notes stratégiques (téléchargeables et imprimables), de brèves explications en ligne sur les principaux problèmes en matière de cybersécurité, ainsi que des listes de publications commentées afin d'approfondir le sujet :

canvas-project.eu

Vous trouverez d'autres documents liés au projet CANVAS sur notre site Internet :

Programme de référence du projet CANVAS
(intégration de l'approche prenant en compte les valeurs fondamentales dans la formation et l'éducation en cybersécurité)

CANVAS MOOC
(Cours en ligne ouvert à tous)

Livre en libre accès
« L'éthique de la cybersécurité »

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 du gouvernement suisse.

Objectif de CANVAS :
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.

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

Version et date de publication :
Version 2.0, octobre 2019

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 formaation, à la recherche et à l'innovation.

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

Durée du projet :
septembre 2016 – octobre 2019