LES PUBLICATIONS

[EN CLAIR]

CYBERSÉCURITÉ VS SOBRIÉTÉ NUMÉRIQUE : UN CHOIX CORNÉLIEN

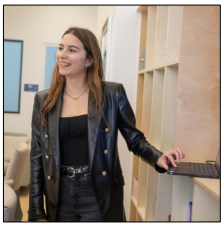
Par Noaïma HENRY avec l'aide de Thierry HORTIN

LES JEUNES IHEDN

À PROPOS DE L'ARTICLE

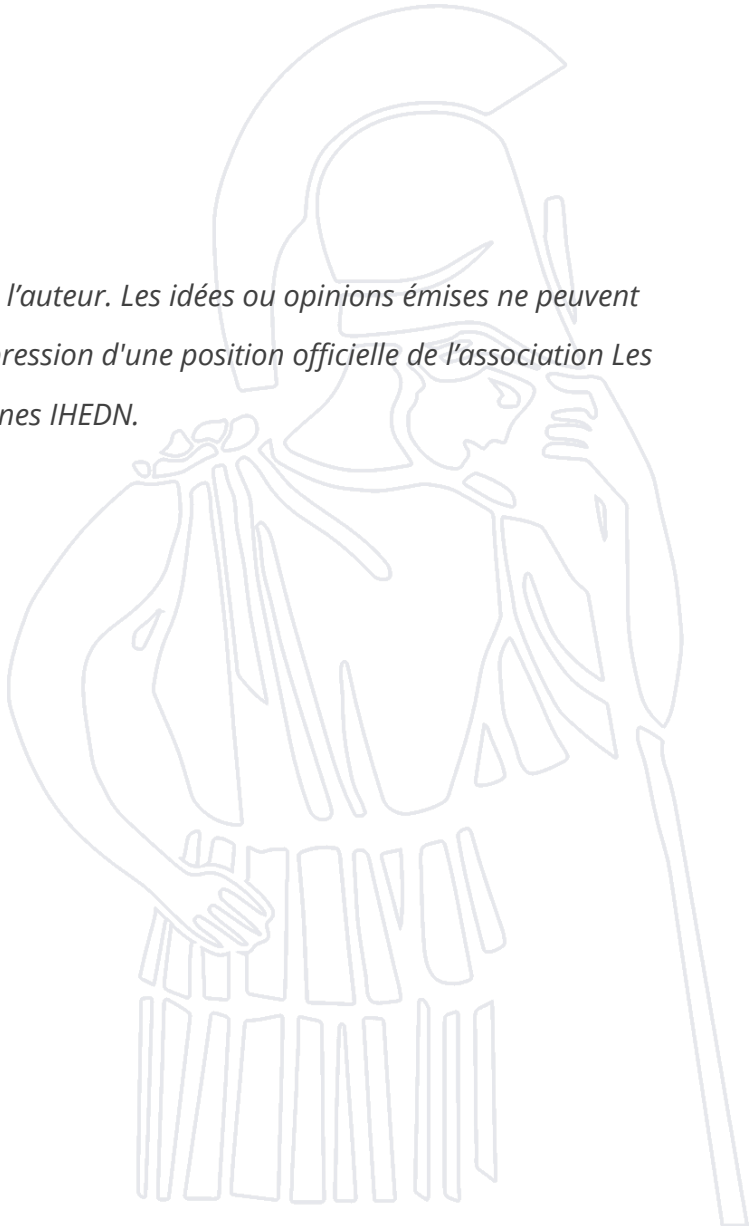
Le numérique est sans cesse en transformation. Intelligence artificielle, métavers, cyber-guerres : le numérique est porteur d'enjeux nouveaux. Parmi ces enjeux, certains sont incontournables pour les organisations, mais aussi parfois contradictoires. Ainsi, les principes de la cybersécurité et de la sobriété numérique que sont aujourd'hui contraintes de mettre en place les entreprises et organisations, semblent bien souvent être en contradiction. Cet article explore les liens qui existent entre sobriété numérique et sécurité informatique et propose une première approche pour allier les deux au sein de tout type d'organisation.

À PROPOS DE L'AUTEUR



Noaïma HENRY est consultante senior en cybersécurité et responsable de la RSE chez VONA Consulting. Membre du Comité Cyber depuis un an, elle a à cœur d'intégrer les enjeux du numérique responsable dans ses activités de cybersécurité.

Ce texte n'engage que la responsabilité de l'auteur. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle de l'association Les Jeunes IHEDN.



Cybersécurité vs sobriété numérique : un choix cornélien

Cybersécurité et sobriété numérique : deux notions incontournables pour les entreprises et les organisations

Selon une enquête du cabinet PwC, 75% des dirigeant.e.s interrogé.e.s se sentent exposé.e.s à des risques « préoccupants » en matière de cybersécurité. Dans le même temps, l'urgence climatique oblige ces mêmes organisations à se soucier de leur sobriété numérique. La Confédération des PME précise que « *si le numérique permet de maîtriser notre consommation énergétique, notamment par la diminution de nos déplacements, il n'est pas neutre énergétiquement* ». Le numérique français représente en effet 10,3% de la consommation électrique du pays et a d'autres impacts sur l'environnement, notamment sur les ressources en eau. L'empreinte carbone du numérique pourrait augmenter de 60% en 2040 si rien n'est fait pour la limiter.

Ces deux sujets sont très dynamiques, indépendamment l'un de l'autre. Au niveau de l'Union européenne (UE) par exemple, la directive européenne EcoDesign établit des exigences d'écoconception applicables aux serveurs et tout produit de stockage de données et salles serveurs d'une entreprise privée afin de limiter leur impact sur l'environnement. D'un point de vue de la cybersécurité les directives NIS et NIS 2 de l'UE établissent des obligations en matière de sécurité informatique pour les opérateurs dans des secteurs stratégiques .

Par contrainte réglementaire, financière, *business* ou encore par conviction, les entreprises et organisation sont aujourd'hui contraintes ou *a minima* incitées à mettre en place des mesures de cybersécurité ainsi que des mesures de sobriété numérique. Pour cela, elles peuvent suivre différents référentiels : ISO 27001 et 27002 pour la cybersécurité et les 74 bonnes pratiques clés pour un numérique plus responsable de GreenIT.fr.

Néanmoins, il n'existe aujourd'hui pas de croisement entre ces référentiels qui présentent des mesures qui sont parfois en contradiction les unes avec les autres. Il n'existe pas encore non plus à notre connaissance d'expert.e.s formé.e.s sur les deux sujets au sein des entreprises et organisations, qui soient capable de les accompagner sur les deux sujets en parallèle.

Cybersécurité et sobriété numérique : des principes de base identiques

La cybersécurité et la sobriété numérique partagent des principes communs. Tout d'abord, la cybersécurité est d'abord un problème de sobriété. De fait, certaines mesures de sécurité informatique s'appliquent pleinement à la sobriété numérique. Parmi eux, le principe de minimisation des données. Ce principe de conception de systèmes d'information consiste à collecter et à stocker le minimum de données nécessaires pour remplir une fonction ou un objectif spécifique. Il répond à la fois à des enjeux de protection des données car moins de données exploitables sont alors disponibles pour les hackers, mais aussi écologiques. En effet, limiter le nombre de données stockées par nos systèmes d'information permet le juste dimensionnement des équipements informatiques comme les *data centers*, qui représentent 16% de l'empreinte carbone du numérique française[1]. Les enjeux d'archivage et de destruction des données s'inscrivent dans la même logique. Des données ayant un besoin en disponibilité moins important ou n'existant tout simplement plus ont un impact environnemental moindre et représentent moins de risque de sécurité. Plus encore que la minimisation des données, il est essentiel d'adopter une posture de sobriété dans le développement des outils afin de les sécuriser[2] au mieux plutôt que de multiplier les outils souvent énergivores, parfois sous utilisés et souvent vecteurs de vulnérabilités. Les bénéfices de l'application de ces principes sont parfois là où on ne les attend pas. À l'heure de la flambée des prix de l'énergie, réduire sa

[1] ADEME et ARCEP, Évaluation de l'impact environnemental du numérique en France et analyse prospective [en ligne], 19 Janvier 2022 [28 Avril 2023]. Disponibilité et accès : https://www.arcep.fr/uploads/tx_gspublication/etude-numerique-environnement-ademe-arcep-note-synthese_janv2022.pdf.

[2] ESILV, Cybersécurité, une question de sobriété numérique et management [en ligne], 01 Août 2022 [28 Avril 2023]. Disponibilité et accès : https://www.esilv.fr/cybersecurite-une-question-de-sobriete-numerique-et-management/.

facture en utilisant mieux le numérique est une voie à mettre en œuvre dans les entreprises… Un double bénéfice, puisque cela permet aussi de mieux respecter l'environnement.

Des exigences parfois contradictoires

Néanmoins, les exigences de cybersécurité et de sobriété numérique ne vont pas toujours de pair. Plusieurs exemples sont assez parlants. Un premier exemple serait l'utilisation de matériel reconditionné. Les terminaux représentent 79% de l'impact environnemental du numérique[3] et 73% de leur impact provient de leur fabrication[4] (73% pour les ordinateurs et 80% pour les smartphones). Une des actions prioritaires du *Green IT* est donc de limiter la production de nouveaux terminaux. Ainsi, le reconditionné est présenté comme étant une des mesures les plus impactantes du *Green IT*. Néanmoins, le reconditionné présente plusieurs risques de sécurité informatique. Dans un premier temps, l'origine précise de l'appareil reconditionné acheté est bien souvent inconnue. Il est possible que le produit ait été compromis ou qu'il contienne des logiciels malveillants qui pourraient être utilisés pour accéder compromettre les données du terminal. Deuxièmement, comme le présente L'ADN dans son article « *Télécoms : faut-il vraiment choisir entre sécurité et sobriété ?* », la sobriété numérique « *favorise l'apparition d'un marché de mieux en mieux structuré et globalisé de la seconde main, ce qui aura mécaniquement pour conséquence de réduire les ventes de futurs nouveaux modèles mieux sécurisés* [5] ». En effet, les appareils reconditionnés peuvent ne pas supporter les dernières mises à jour de sécurité de leur constructeur et donc être plus susceptibles aux failles de sécurité.

Enfin, lorsque l'on se débarrasse d'un terminal en fin de vie afin qu'il soit reconditionné, les données contenues dans l'appareil, si elles ne sont pas effacées au préalable, pourraient ne pas être supprimées correctement par le reconditionneur. Des

[3] Voir note 1.

[4] ECOTOPIE, Pollution d'un ordinateur : anatomie d'un désastre écologique et social [en ligne], [28 Avril 2023]. Disponibilité et accès : https://ecotopie.fr/numerique-responsable/pollution-dun-ordinateur-anatomie-dun-desastre-ecologique-et-social/.

[5] PAGES Arnaud, « Télécoms : faut-il vraiment choisir entre sécurité et sobriété ? » [en ligne]. L'AND, 02 Janvier 2023 [28 Avril 2023]. Disponibilité et accès : https://www.ladn.eu/tech-a-suivre/telecoms-faut-il-vraiment-choisir-entre-securite-et-sobriete/.

informations parfois personnelles ou sensibles pourraient alors être récupérées par des tiers. Outre l'exemple du reconditionnement, d'autres mesures encouragées par les expert.e.s de la cybersécurité comme la redondance des données ou l'utilisation de logiciels de détection des menaces basées sur l'intelligence artificielle ont souvent un impact environnemental important. Néanmoins, il n'est pas envisageable d'avoir dans les entreprises ou dans les organisations des équipes RSE allant à l'encontre des principes clés appliqués par les équipes SSI, et inversement. Une collaboration et une concertation doit impérativement se faire entre les deux.

La nécessité d'allier sobriété numérique et cybersécurité au sein des entreprises et organisations

Si « *au cœur de la transformation numérique, l'humain est le principal facteur d'évolution de l'entreprise moderne et au même titre le maillon faible de la cybersécurité* [6] », il est également essentiel dans le dialogue qui doit s'opérer entre cybersécurité et sobriété numérique.
Le rapprochement entre ces deux dimensions du numérique doit se faire en fonction de deux dimensions :

- Qu'est-ce qu'il est vraiment nécessaire de mettre en place pour sécuriser les systèmes d'information ?
- Quelles sont les mesures de *Green IT* qui ont un impact environnemental important ?

Ainsi, une matrice comme celle qui suit pourrait être utilisée pour définir quelles actions devraient être privilégiées.

[6] Voir note 2.

Impact environnemental / Impact sécurité informatique	Important	Limité
Important	Arbitrage nécessaire	Mesures de sobriété numérique priorisées
Limité	Mesures de cybersécurité priorisées	Arbitrage nécessaire Possibilité de ne rien faire en fonction du coût et de la complexité des mesures à mettre en œuvre

Figure 1. Matrice des impacts environnementaux et de sécurité

Ainsi, nous pouvons prendre deux exemples :

- Le cas des terminaux reconditionnés que nous évoquions dans la partie 2. Avoir recourt à des terminaux reconditionnés est une mesure ayant un impact environnemental fort. Néanmoins, l'impact sur la sécurité des informations transitant par le terminal peut également être fort. Un arbitrage doit alors être fait, notamment en fonction des données accessibles par ledit terminal.

Ainsi, le décret n° 2023-266 du 12 avril 2023 fixant les objectifs et modalités de réemploi et de réutilisation des matériels informatiques réformés par l'Etat et les collectivités territoriales indique que « *le décret fixe un objectif annuel de réemploi et de réutilisation des matériels informatiques réformés des personnes publiques applicable à compter de l'année 2023* [7] ». Néanmoins, les matériels informatiques contenant « *des informations et des supports classifiés* » ou « *régies par des obligations de sécurité spécifiques propres aux personnes publiques* » sont exclus de ce calcul.

[7] République Française, Décret n° 2023-266 du 12 avril 2023 fixant les objectifs et modalités de réemploi et de réutilisation des matériels informatiques réformés par l'Etat et les collectivités territoriales [en ligne]. Legifrance, 15 Avril 2023 [28 Avril 2023]. Disponibilité et accès : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047439314.

En revanche, les cas dans lesquels la sécurité prime sur l'impact environnemental doivent être explicités afin que cette excuse ne soit pas utilisée trop fréquemment par les organisations pour s'abroger de leurs obligations législatives et citoyennes.

- À l'inverse, le cas du recyclage de papiers contenant des informations confidentielles est plus facilement solvable. Le déchiquetage de tels documents empêche leur recyclage. Mais le gain environnemental du recyclage du papier étant relativement faible, il semble logique de privilégier ici la mesure de cybersécurité.

Cette matrice et ces exemples ne sont qu'un point de départ d'un travail bien plus complet. Pour construire ce référentiel croisant sobriété numérique et cybersécurité, il nous faut maintenant :

- Comparer les référentiels existant dans les deux domaines et définir des priorités et des impacts pour chacune des actions édictées dans les référentiels étudiés.
- Interroger les acteurs de la cybersécurité sur l'impact environnemental de leurs solutions.
- Consolider ces informations dans un document d'aide à la décision et au choix entre les mesures de sobriété numérique et de cybersécurité, adapté à toutes les organisations.






publication@jeunes-ihedn.org