La Cyber Verte :
un Manifeste pour un Numérique Durable

Elise BRUILLON
Directeur Général
STRAAD.A

El Yamani HAMEDI
Directeur Général associé
STRAAD.A

Les entreprises et les institutions publiques, engagées dans leur transformation numérique, évoluent dans un monde toujours plus ouvert et plus connecté. Si l'économie numérique offre de nouvelles opportunités, elle s'accompagne également de risques et de menaces de plus en plus sophistiqués.

Dans ce contexte, les activités de protection et de sécurisation génèrent une dette écologique croissante : la sécurisation des infrastructures critiques, notamment énergétiques, repose sur l'ajout de protections physiques et numériques, entraînant une augmentation des équipements, du traitement des données et par conséquent de la consommation énergétique.

Paradoxalement, cette nécessité s'oppose à la dynamique actuelle d'optimisation énergétique, où l'objectif est de consommer moins et mieux. Ce paradigme soulève un défi majeur : comment renforcer la cybersécurité sans compromettre l'efficacité énergétique, comment renforcer la cybersécurité en prenant en compte une nécessaire frugalité dans la consommation de ressources par essence énergivore ?

L'enjeu réside dans l'équilibre entre résilience aux cyberattaques et sobriété dans la consommation, notamment en développant des solutions innovantes et éco-efficaces capables de protéger les infrastructures tout en minimisant leur impact environnemental. Il s'agit ici du concept de la dette "Cyber".

Ce paradigme est particulièrement pertinent dans le contexte des villes intelligentes (Smart Cities), où la convergence entre cybersécurité et efficacité énergétique devient un enjeu majeur. Si ces villes optimisent la gestion urbaine, elles n'en demeurent pas moins vulnérables aux cyberattaques : la prolifération des objets connectés et des systèmes automatisés élargit la surface d'attaque, exigeant des protections renforcées. Il est donc crucial d'adopter une approche équilibrée, intégrant l'analyse des risques cybersécurité dans une démarche éco-responsable pour aligner de concert sécurité et durabilité.

Mais comment garantir la résilience numérique des villes intelligentes tout en respectant les impératifs de sobriété énergétique ?

Les défis et les opportunités de la convergence entre cybersécurité et efficacité énergétique dans le contexte des villes intelligentes

La convergence entre cybersécurité et efficacité énergétique représente à la fois un défi et une opportunité pour les villes intelligentes. D'un côté, la sécurisation des infrastructures urbaines connectées nécessite une puissance de calcul accrue, entraînant une consommation énergétique plus importante. De l'autre, une approche intelligente permet d'intégrer l'efficacité énergétique dans l'évaluation des risques

cyber, en identifiant des solutions moins énergivores sans compromettre la sécurité.

Par exemple, dans une ville intelligente, la gestion du trafic en temps réel repose sur un réseau d'objets connectés et de capteurs. Sécuriser ces flux de données tout en réduisant leur empreinte carbone implique de développer des stratégies de protection adaptées, privilégiant des algorithmes d'optimisation énergétique et des infrastructures résilientes mais sobres.

L'implémentation d'une gestion des données économe est également cruciale : limiter la redondance des traitements, favoriser le stockage décentralisé et adopter des technologies plus vertes permettent de réduire l'impact écologique des opérations cybersécurité. Enfin, la sensibilisation joue un rôle clé : éduquer les citoyens et décideurs sur les bonnes pratiques d'une cybersécurité verte encourage l'adoption de solutions responsables et durables. En alignant cybersécurité et sobriété énergétique, les Smart Cities peuvent ainsi allier innovation, résilience et respect de l'environnement.

Un Nouveau Paradigme de Protection Durable

Face aux défis et opportunités qu'offre la convergence entre cybersécurité et efficacité énergétique dans les villes intelligentes**,** un nouveau paradigme de protection durable doit émerger. Ce modèle repose sur trois piliers essentiels.

D'abord, l'autonomie locale, en développant une cybersécurité décentralisée, mieux adaptée aux réalités régionales et plus résiliente face aux menaces globales. Cela passe par l'éco-conception des systèmes de sécurité, intégrant des architectures plus sobres en énergie et optimisées dès leur conception pour limiter leur impact environnemental.

Les politiques publiques ont un rôle clé à jouer dans cette transition vers des infrastructures numériques plus durables. La mise en place de datacenters verts par exemple doit répondre à des exigences de durabilité claires, mesurables et auditées, en intégrant des solutions comme la récupération des eaux de pluie et l'utilisation d'énergies renouvelables. Par ailleurs, les stratégies de sauvegarde des données ne doivent pas être uniquement centrées sur l'Île-de-France : il est essentiel de repenser l'aménagement du territoire en valorisant les expertises et les infrastructures régionales, afin de renforcer la résilience nationale face aux défis numériques et environnementaux.

Ensuite, la diversité des profils en cybersécurité ; il s'agit, tout d'abord, de favoriser les entreprises et institutions locales, en adoptant une approche de circuit court, permettant de répondre plus efficacement aux besoins des utilisateurs tout en limitant l'empreinte carbone des infrastructures numériques, en encourageant une plus grande mixité, notamment par la présence féminine dans la cybersécurité, et en facilitant l'accès à la formation et à la montée en compétences. Cette diversité est une réponse essentielle au manque de ressources en cybersécurité, en apportant des perspectives nouvelles et en comblant les besoins en expertise.

Enfin, l'innovation responsable, en promouvant des solutions créatives et durables, comme les mises à jour intelligentes qui réduisent la fréquence des patchs de sécurité sans compromettre la protection des infrastructures. Cela fait écho à l'adoption du Security by Design, qui intègre la cybersécurité dès la conception des infrastructures et des systèmes évitant ainsi les corrections coûteuses et énergivores a posteriori. En repensant la sécurité en amont, cette approche permet de réduire la fréquence des mises à jour, de limiter la consommation de ressources et de favoriser des solutions plus légères et plus efficientes. Elle encourage également la créativité en incitant les entreprises à développer des architectures numériques plus résilientes et moins énergivores. En combinant anticipation des risques et efficacité énergétique, le Security by Design s'impose comme un modèle durable, conciliant protection des infrastructures et réduction de l'empreinte environnementale.

Par ailleurs, au-delà des entreprises et des

institutions, chaque individu peut jouer un rôle dans cette démarche en adoptant de simples gestes militants pour une cybersécurité plus durable. Une action accessible à tous consiste à supprimer régulièrement les données en doublon ou obsolètes, réduisant ainsi l'infobésité et l'empreinte énergétique liée au stockage inutile. Ce geste, appliqué à grande échelle, contribue à alléger la charge des serveurs, à optimiser les ressources numériques et à favoriser une utilisation plus responsable des infrastructures informatiques.

En adoptant cette approche, les villes intelligentes pourront concilier protection numérique et sobriété énergétique, garantissant un avenir à la fois sécurisé, inclusif et respectueux de l'environnement.

Vers une Cybersécurité Éthique et Durable

Les règles déontologiques professionnelles occupent une place centrale pour aligner cybersécurité et préservation de l'environnement. Les sociétés spécialisées en cybersécurité doivent s'engager à repenser leurs pratiques en intégrant des principes de sobriété numérique et d'optimisation énergétique. Il ne s'agit plus de bâtir des forteresses numériques imprenables, exigeant des infrastructures massives et énergivores, mais d'adopter une cybersécurité flexible et adaptative, inspirée de stratégies de résilience plutôt que d'une logique d'éradication totale du risque.

Cette approche repose sur une distinction essentielle entre prévention et résilience. Plutôt que de poursuivre un idéal de sécurisation absolue, synonyme de surconsommation de ressources, il s'agit de protéger l'actif vital en intégrant une réflexion plus réaliste sur la gestion des risques et la priorisation des ressources essentielles. Là où la cybersécurité traditionnelle se focalisait sur une vision défensive massive, exigeant des capacités et une énergie quasi illimitée, cette nouvelle approche prône une gestion intelligente et ciblée du risque, optimisant ainsi l'impact environnemental.

Enfin, cette transition vers une cybersécurité durable implique un changement de mentalité : il ne s'agit plus de contrôler à tout prix, mais d'accepter une part de risque maîtrisé dans une logique d'adaptation continue. Cette philosophie, ancrée dans une vision éthique et responsable, redéfinit les engagements des entreprises du secteur, leur imposant d'intégrer les enjeux environnementaux au cœur de leurs stratégies de protection.

Ce nouveau paradigme de protection durable nous conduit donc inévitablement vers une cybersécurité éthique, durable et responsable, où plusieurs principes clés doivent être intégrés pour assurer un avenir à la fois sécurisé et respectueux de l'environnement.

La première étape exige avant tout le courage, de la part des professionnels du secteur, de prendre une certaine distanciation vis-à-vis des approches traditionnelles. Trop souvent, la cybersécurité a été pensée dans une logique d'accumulation de défenses, avec des infrastructures de plus en plus complexes, énergivores et coûteuses. Il ne s'agit plus de tout verrouiller, mais d'optimiser les protections en fonction des enjeux réels, en réduisant les surconsommations inutiles et en favorisant des solutions plus sobres et intelligentes. Accepter cette évolution, c'est faire preuve de lucidité et de responsabilité, en intégrant dès aujourd'hui la nécessité d'une protection numérique alignée avec les défis environnementaux.

Cela consiste aussi à penser hors du cadre, penser autrement, à sortir des schémas classiques pour développer des approches plus ingénieuses et audacieuses Cela implique d'oser remettre en question nos partis pris, de dépasser nos biais cognitifs et d'explorer de nouvelles manières d'aborder la cybersécurité et l'efficacité énergétique. Il ne s'agit pas simplement d'innover pour innover, mais d'inventer un modèle repensé en profondeur. Si cette transformation aboutit à une innovation, alors le pari sera véritablement gagné. Concrètement, cela passe par le développement de solutions disruptives comme les smart grids, ainsi que par une refonte de la gouvernance énergétique,

en encourageant une gestion intelligente, décentralisée et optimisée des ressources, tout en intégrant des mécanismes de sécurité robustes. Ensuite, il est essentiel de mettre en place une gestion responsable, qui assure une utilisation durable et sécurisée des ressources communes, notamment face aux cybermenaces.

Cette approche doit garantir une distribution équitable de l'énergie, en conciliant protection des infrastructures et sobriété énergétique, pour un monde connecté, résilient et respectueux de l'environnement.

Une autre dimension essentielle est d'adopter une logique du vivant, en reconnaissant que la cybersécurité n'est ni figée ni immuable, mais qu'elle doit évoluer en permanence pour s'adapter aux nouvelles menaces et aux transformations technologiques. Redevenir agile, c'est accepter que la protection numérique ne repose pas sur des forteresses imprenables, mais sur des mécanismes adaptatifs capables de résister, de se transformer et de se renforcer face aux attaques. Nous pouvons ainsi établir un parallèle avec la méthode agile dans le développement informatique, qui privilégie une approche itérative, l'amélioration continue et l'adaptation rapide aux imprévus. Appliquer cette philosophie à la cybersécurité, c'est favoriser des stratégies évolutives, basées sur l'anticipation, l'apprentissage en temps réel, plutôt qu'une vision rigide et centralisée

Cela implique aussi de travailler sur la résilience des écosystèmes et des infrastructures, en intégrant des technologies et des stratégies qui permettent aux systèmes de se régénérer et de s'adapter aux évolutions technologiques et environnementales. Enfin, il est indispensable de développer une approche humaine, en plaçant l'humain au cœur des stratégies de cybersécurité et d'efficacité énergétique. Cela inclut la protection des individus et de leurs données, mais aussi l'accès à une énergie propre et sécurisée, en s'assurant que tous puissent bénéficier de ces technologies de manière responsable et équitable.

Une dernière dimension essentielle repose sur la coopération globale, un levier fondamental pour bâtir une cybersécurité durable et efficace à l'échelle internationale. Face à des menaces qui ne connaissent pas de frontières, s'appuyer sur les initiatives existantes menées par les entreprises, les institutions et les acteurs de la cybersécurité est indispensable. Mutualiser les connaissances, partager les meilleures pratiques et renforcer les synergies permettent de construire des modèles de sécurité alignés avec les impératifs environnementaux. Dans cette dynamique, contribuer à un manifeste étendu au niveau de l'Union européenne offrirait un cadre structurant pour encourager des politiques de cybersécurité responsables, intégrant sobriété énergétique, innovation durable et résilience numérique. En fédérant les acteurs autour d'une vision commune, cette coopération renforcerait non seulement la protection des infrastructures critiques, mais aussi la souveraineté numérique européenne, tout en inscrivant la cybersécurité dans un modèle plus éthique et respectueux de l'environnement.

Ce paradigme de que nous pouvons qualifier de cyberfrugalité nous invite donc à concevoir un avenir où la cybersécurité et l'efficacité énergétique ne sont pas seulement des outils techniques, mais des leviers éthiques et responsables pour une société plus résiliente et respectueuse de son environnement.

Conclusion

La convergence entre cybersécurité et efficacité énergétique dans le cadre des villes intelligentes offre de nombreux défis mais aussi des opportunités considérables. Il est essentiel de développer des solutions novatrices qui permettent de renforcer la sécurité tout en minimisant l'impact environnemental, en intégrant des pratiques éco-responsables et en adoptant des stratégies adaptées aux enjeux locaux. Ce nouveau paradigme de protection durable invite à repenser la manière dont nous concevons la cybersécurité, en la plaçant au cœur de la transition énergétique et en veillant à ce que la résilience numérique soit synonyme de durabilité. En favorisant l'innovation responsable, la

diversité des compétences et l'autonomie locale, nous pouvons bâtir des villes plus sûres, plus intelligentes et plus respectueuses de l'environnement. Ce modèle de cybersécurité éthique et durable représente un véritable levier pour construire un avenir équilibré, où la technologie et l'écologie se nourrissent mutuellement, assurant ainsi un développement harmonieux et inclusif pour les générations futures.

Manifeste pour une Cybersécurité Verte

5 Engagements Clés pour les Entreprises

Intégration de la Cybersécurité dans les politiques de durabilité

Les entreprises doivent prendre l'engagement d'intégrer la cybersécurité dès la conception des systèmes pour garantir une protection durable et efficace.

Promotion de la Recherche et du Développement dans les Technologies Vertes et Sécurisées

Les entreprises doivent investir activement dans des technologies innovantes qui optimisent l'efficacité énergétique tout en assurant une protection robuste contre les cyberattaques.

Sensibilisation aux Risques Cybersécurité dans les Initiatives de Développement Durable

Les entreprises doivent s'engager dans l'éducation et la sensibilisation des employés et des parties prenantes aux enjeux de la cybersécurité et à son rôle dans la durabilité.

Collaboration entre les Secteurs Public et Privé pour Renforcer la Cybersécurité

Les entreprises doivent encourager les partenariats entre les secteurs public et privé pour partager les meilleures pratiques et renforcer la résilience des systèmes face aux cybermenaces.

Optimisation des Ressources Numériques et Réduction de l'Infobésité

Les entreprises doivent s'engager à réduire l'empreinte écologique liée aux données et aux systèmes numériques en supprimant les données obsolètes et inutilisées.

Ce manifeste vise à guider les entreprises vers une approche plus durable et sécurisée de la gestion énergétique, en mettant l'accent sur l'importance de la cybersécurité dans la transition vers des économies plus vertes et résilientes.