Cyber Résilience

À l'heure du numérique, l'humain est baigné dans les services numériques avant même sa naissance. Échographié sur support numérique dans le ventre de sa maman, identifié par un QR code dans son berceau, photographié par centaines ou par milliers sur des tablettes ou des téléphones, sans compter toutes les données qui commencent à être enregistrées dans les différents centres de données installés un peu partout sur la planète. Cela, bien entendu, continue à toutes les étapes de sa vie, et même après sa mort. Le numérique nous entoure plus que tout. Plus que les particules fines, que les gouttes de pluie, que les rayons de soleil ! Pas un geste, ni une émotion, ni une pensée sans que le numérique et les zéros et les uns n'interviennent pour les commander, les enregistrer ou les guider. La journée d'un humain commence et se termine par le numérique. Au réveil, on ouvre les yeux sur l'écran du téléphone. On lit des messages, on en like certains, on est surpris par d'autres puis on se met à regarder la météo et l'état des routes ou des transports ! Dans la journée, une IA par ici et une IA par là pour nous donner un avis, nous suggérer un texte ou une synthèse ! On se sert de la recherche Google pour comprendre un mot, pour rentrer chez soi et pour préparer ses dîners. Notre mode de vie, devenu universel au fil des années, nous impose de léguer nos données à de grands centres à travers Internet, puis d'attendre les instructions fournies par les algorithmes fonctionnant sur des machines dans ces centres de données.
Dépendre du numérique n'est pas une fatalité. Nous avons adopté ces comportements avec l'aide des services numériques pour améliorer notre quotidien, optimiser nos ressources, réduire le gaspillage et diminuer la pénibilité des tâches. Le seul problème qui se pose est notre capacité à survivre sans ces nouveaux services.
Quelle est la résilience de l'humain à une panne du numérique ? Si tout s'arrête, que se passe-t-il ? Sommes-nous résilients à une giga panne de courant électrique ?

Sommes-nous résilients à une panne d'opérateur de réseau ? Et pire, sommes-nous résilients à une panne des centres de données ?
Si vous coupez l'accès aux centres de données à un humain largement habitué et biberonné aux services numériques, que va-t-il se passer ? Va-t-il pouvoir s'orienter dans la rue, s'inscrire à un examen, faire ses courses, préparer ses repas, se soigner, accomplir ses missions au travail ? La réponse, de toute évidence, est non ! Nous avons encore des personnes des générations précédentes qui se souviennent des procédés avant l'ère du numérique, mais par manque de pratique, les réflexes ne sont plus là. Même si nous utilisions les cartes routières, il y a plus de 30 ans, un seul réflexe s'impose avant même d'allumer le moteur du véhicule : brancher le GPS !
Un centre de données devient alors une source de notre intelligence, et sans un accès constant à cet espace, nous pouvons nous sentir perdus, privés d'identité, de pouvoir et d'action. Ainsi, ce centre devient un point de vulnérabilité majeur dans notre quotidien.
De nos jours, attaquer ce point de faiblesse, ce centre qui contient nos données et notre intelligence, est un jeu d'enfants. Le nombre de cyberattaques par jour est vertigineux. C'est tellement fréquent et avec un taux de succès très élevé que nous nous armons avec des budgets très conséquents pour nous en prémunir. Malgré cela, beaucoup d'attaques sont malheureusement couronnées de succès. Le réseau pour accéder aux centres de données peut aussi tomber en panne. Il suffit d'une catastrophe naturelle, d'une panne de l'opérateur du réseau, d'un sabotage, ou encore d'une surcharge pour ne plus y accéder.
Être cyber résilient, c'est continuer à fonctionner sans l'accès aux centres de données. Comment cela peut-il être possible alors qu'on leur a offert notre réflexion et qu'ils concentrent aujourd'hui toute notre intelligence ? Comme pour l'électricité, la résilience face à une panne est de stocker l'énergie dans une batterie. Lorsqu'un pays sort d'une longue guerre, son infrastructure de production électrique est à terre et ne produit qu'une infime quantité, très loin de satisfaire la population. Un rationnement se fait alors et, avec l'aide des batteries, nous arrivons à emmagasiner l'énergie quand elle arrive, puis à la consommer pour notre résilience.
En numérique, pour survivre pendant une coupure due à une cyberattaque, la seule possibilité est de s'appuyer sur les services numériques locaux mis en réserve pour poursuivre notre activité qui en dépend. On appelle cela un edge. L'edge devient notre batterie de services numériques pour garantir notre résilience. Lorsque l'accès au cloud, qui contient les centres de données, redevient opérationnel, nous pouvons alors nous en servir et revenir à nos comportements habituels. Quels sont les services essentiels que nous devons conserver pour maximiser notre cyber-résilience ? C'est une question cruciale pour construire notre edge. Par exemple, en électricité, la taille de la batterie que nous choisissons se détermine en énumérant les machines à alimenter qui nous sont indispensables. En ce qui concerne les

services numériques, cela dépend également des cas d'usage. Si l'on prend celui d'un hôpital, il nous faudra au minimum un service de messagerie, de téléphonie, d'échanges de fichiers, le dossier des patients et un système de traçabilité !
Se couper des points centraux, qui sont les clouds, et basculer vers des systèmes locaux et distribués, les edges, représente un grand défi. Cela revient à créer des communautés évoluant localement et séparément, qui, lorsqu'elles reviendront à un environnement connecté et partagé, auront opéré des changements, entraînant des incohérences et des inconsistances. Un travail important s'impose alors pour mettre de l'ordre, avec un consensus à trouver pour homogénéiser les différentes évolutions d'une version originelle et vers une version unifiée.
Comme le théorème de CAP le rappelle bien, on ne peut pas garantir en même temps une partition de nos systèmes avec une disponibilité et une consistance de leurs données et de leurs services. Pendant une cyberattaque, des services vont se mettre en place dans différents lieux sous la forme d'edges, servant ainsi les personnes et les objets présents dans les zones couvertes par ces edges. Certains edges peuvent s'interconnecter entre eux, tandis que d'autres peuvent rester isolés. Lors des fusions des edges, des algorithmes de consensus doivent opérer afin de résoudre tous les conflits survenant pendant cette période de résilience.
Pour mieux comprendre les avantages des edges dans la résilience, prenons l'exemple d'un centre hospitalier. Vu la criticité de ses données et l'importance de son fonctionnement permanent, il est amené à construire un plan de continuité et de reprise d'activité en cas de problèmes majeurs. Ce plan peut se baser sur des accès à plusieurs centres de données en mode SaaS (Software as a Service), évitant de regrouper tous les services au même endroit pour réduire les risques.
Malgré ces précautions, ces plans ne prennent pas en compte la défaillance des réseaux et de l'authentification centralisée. Les systèmes d'information, même lorsque les données sont réparties dans plusieurs lieux, utilisent un serveur d'authentification, représentant ainsi un important point de faiblesse d'un plan de résilience (figure 1). À l'inverse, lorsque les données et les services sont hébergés sur site et en accès totalement distribué, aucune défaillance n'est possible (figure 2).

Green Communications avec l'**Internet des Edges (IoE)**, offre la solution parfaite en matière de cyber-résilience. Lorsqu'une infrastructure numérique est rendue inopérante par une catastrophe naturelle, une attaque terroriste, un adversaire, un virus ou un ransomware, aucun service numérique ne peut alors fonctionner. Grâce à des plateformes très légères qui intègrent de nombreux services, l'IoE vous propose une infrastructure numérique dotée d'un panel de services essentiels pour continuer à communiquer, collaborer et évoluer avec les mêmes habitudes et réflexes qu'en temps normal. La solution IoE est l'Arche de Noé du numérique. Lorsque tout est foudroyé par une attaque physique ou cybernétique, l'IoE vous transporte dans un nouveau monde, offrant des services

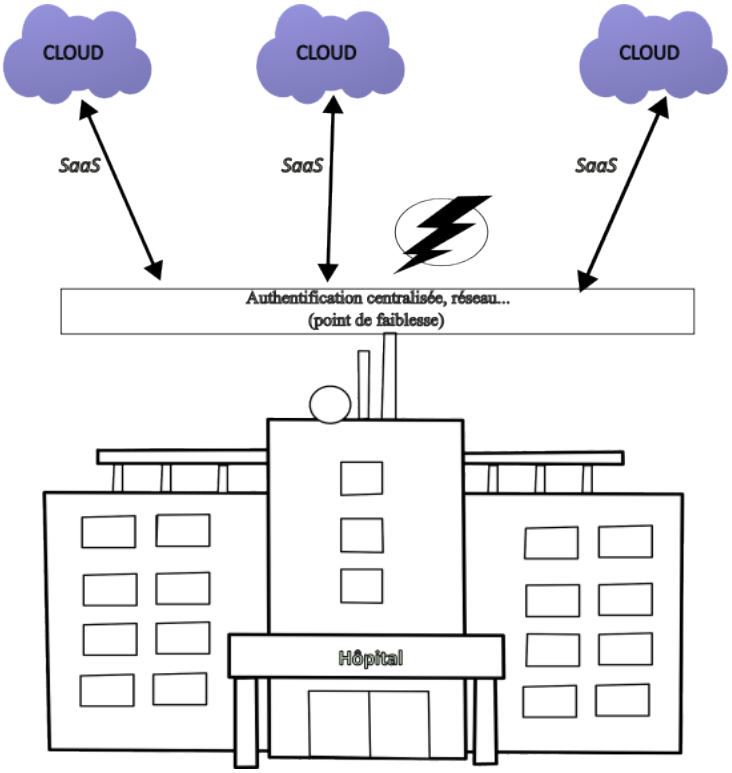

Figure 1: En mode SaaS.

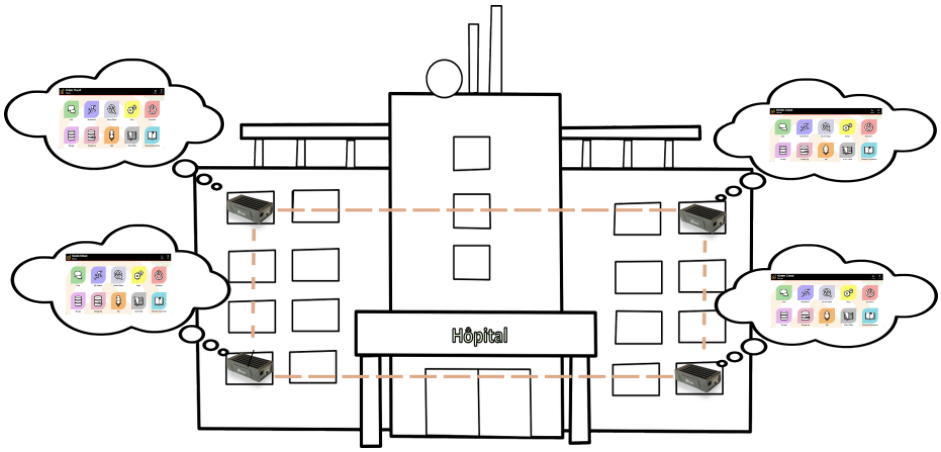

Figure 2: En mode Edge distribué.

numériques essentiels qui garantissent votre résilience.

Comment fonctionne la plateforme IoE :

Tout est très simple ! Il suffit de mettre sous tension un ensemble de boîtiers portatifs (d'environ 300 g) pour qu'ils communiquent entre eux et forment un espace numérique. Le nombre de boîtiers dépend de la taille du lieu à couvrir avec cette infrastructure. Cet espace numérique propose par défaut un ensemble de services :

- Une application de visualisation de la plateforme qui permet de voir le lieu couvert, la localisation des machines le couvrant et leur interaction, ainsi que tous les utilisateurs connectés et bien d'autres informations.
- Une messagerie instantanée (chat) qui permet de créer des salons de conversation entre tous les clients connectés à l'infrastructure.
- Un service de voix qui permet de créer des salons de conversation audio. Il peut également fonctionner en mode Push-to-talk (talkie-walkie).
- Un système de partage de fichiers pour échanger des fichiers entre les participants connectés à l'infrastructure ou créer et modifier des répertoires. Ce système est codé sous la forme de blockchain, où toute opération effectuée est enregistrée et répertoriée dans l'ensemble des boîtiers formant l'infrastructure numérique.
- Un ensemble d'outils destinés à l'administrateur de l'infrastructure pour tester les performances de l'infrastructure, réaliser des logs, modifier la configuration, effectuer des mises à jour, la connecter à d'autres réseaux, changer les mots de passe, configurer le DHCP, le DNS, etc.
- Un outil de création d'une PKI (Public Key Infrastructure) pour générer les certificats pour personnaliser les routeurs de l'infrastructure.
- Un serveur web embarqué pour que les services cités ci-dessus soient facilement accessibles en tant qu'applications web, sans qu'il soit nécessaire de télécharger des applications sur un poste client.

L'infrastructure a la possibilité d'intégrer des services supplémentaires nécessaires au lieu où elle est installée (par exemple, des back-ups de secours). Ces services sont installés sur des machines qui se connectent à l'infrastructure afin que les clients puissent y accéder. Un outil de configuration très simple, sous forme de page web, permet en quelques clics d'offrir un bail statique (adresse IP) et un nom de domaine, afin que l'utilisation du service soit la plus simple possible pour les clients connectés à l'infrastructure.

Le parcours utilisateur

En termes d'expérience utilisateur, l'infrastructure de cyber-résilience offre des interfaces très simples d'utilisation, similaires à celles que les personnes utilisent au quotidien sur leurs ordinateurs, tablettes ou téléphones. Le parcours utilisateur se déroule en plusieurs étapes :

1. Prendre son terminal numérique (téléphone, tablette ou ordinateur) et se connecter au Wi-Fi de l'infrastructure numérique. Cela peut se faire en utilisant un QR-Code ou en renseignant des identifiants sur le clavier.

2. Ouvrir un navigateur (Chrome, Edge, Safari, Firefox, etc.) et entrer l'adresse du portail local. Cela peut également se faire en utilisant un QR-Code ou en renseignant l'adresse dans le champ URL du navigateur.

3. Accepter le certificat de votre infrastructure s'il n'est pas déjà installé sur votre appareil.

4. La figure 3 montre la page web du portail local avec l'ensemble des services offerts par l'infrastructure de cyber-résilience.

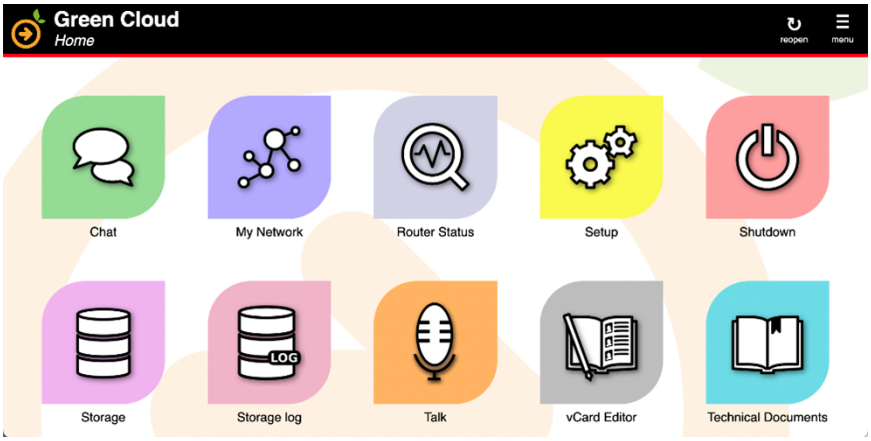

Figure 3: Le Green Cloud.

5. En cliquant sur l'application « My Network », l'utilisateur accède à la page de la figure 4 où il peut visualiser l'infrastructure, localiser ses nœuds, les utilisateurs connectés et leur profil, ainsi qu'une cartographie et d'autres informations permettant d'améliorer la gestion de crise pendant la période de cyber-résilience.

6. En cliquant sur l'application « Chat », l'utilisateur est dirigé vers la page de la figure 5 où il dispose d'une interface de messagerie instantanée avec les

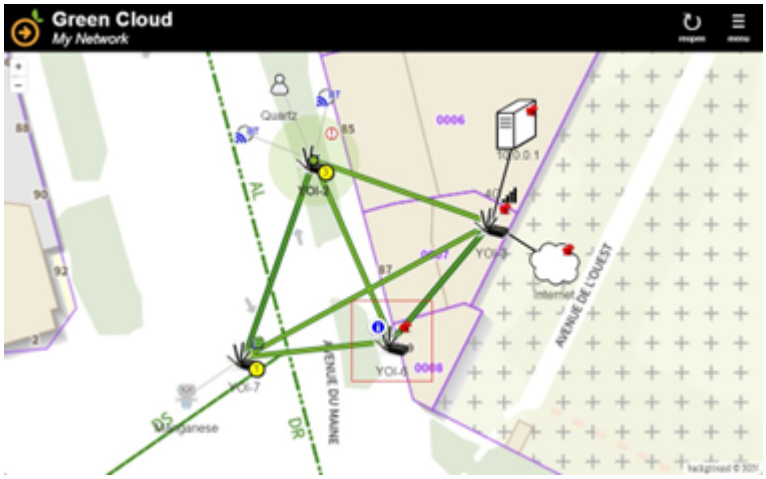

Figure 4: Application “My Network”.

salons des utilisateurs et les utilisateurs par salon. Il peut envoyer et recevoir des messages, téléverser des fichiers, recevoir des notifications, etc.

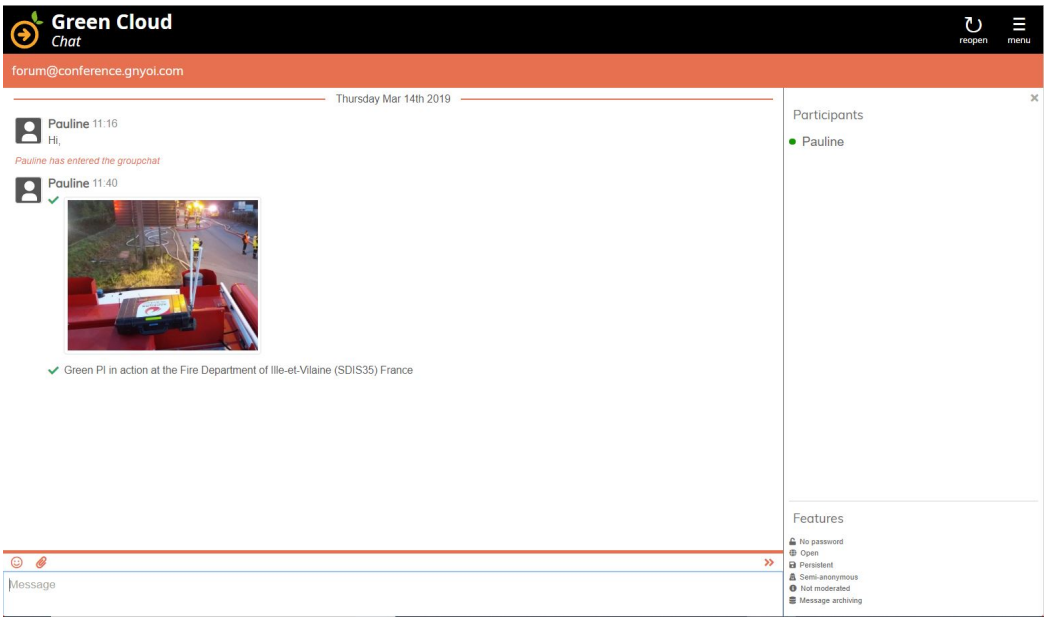

Figure 5: Application “Chat”.

7. En cliquant sur l’application « Talk », l’utilisateur est dirigé vers la page de la figure 6 où il accède à une interface de conversations audio. Il peut rejoindre des salons de voix, en créer, converser avec un utilisateur ou plusieurs, et voir la liste des personnes par salon. L’application peut être utilisée en mode

Push-to-talk (micro ouvert avec un appui) ou en mode téléphone avec un micro ouvert en permanence.

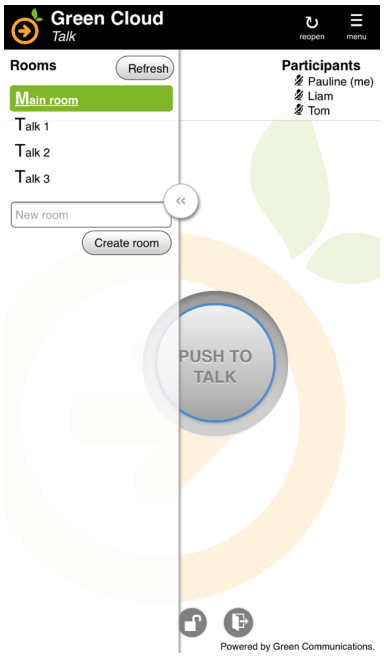

Figure 6: Application “Talk”.

8. En cliquant sur l’application « Storage », l’utilisateur accède à la page de la figure 7. Il s’agit d’un espace de partage de fichiers exploitant les espaces de stockage de tous les nœuds de l’infrastructure. Dans cette application, on peut téléverser et télécharger des fichiers, créer des répertoires, supprimer des répertoires ou des fichiers, et chiffrer un fichier avec un mot de passe. L’application est codée sous forme de blockchain, où toute modification, ajout ou suppression est enregistrée dans une chaîne de blocs qui est répliquée sur tous les nœuds de l’infrastructure. La blockchain peut être consultée par l’administrateur de l’infrastructure en utilisant l’application « Storage log ».

9. En cliquant sur « Router Status », « Setup », « Storage log », « Shutdown », « vCard Editor », on peut tester les performances de l’infrastructure, la configurer, l’éteindre ou la redémarrer, observer des logs, créer des profils d’utilisateur (avec des vCards) et bien d’autres fonctionnalités. Ces applications sont accessibles uniquement par l’administrateur, qui doit renseigner un mot de passe.

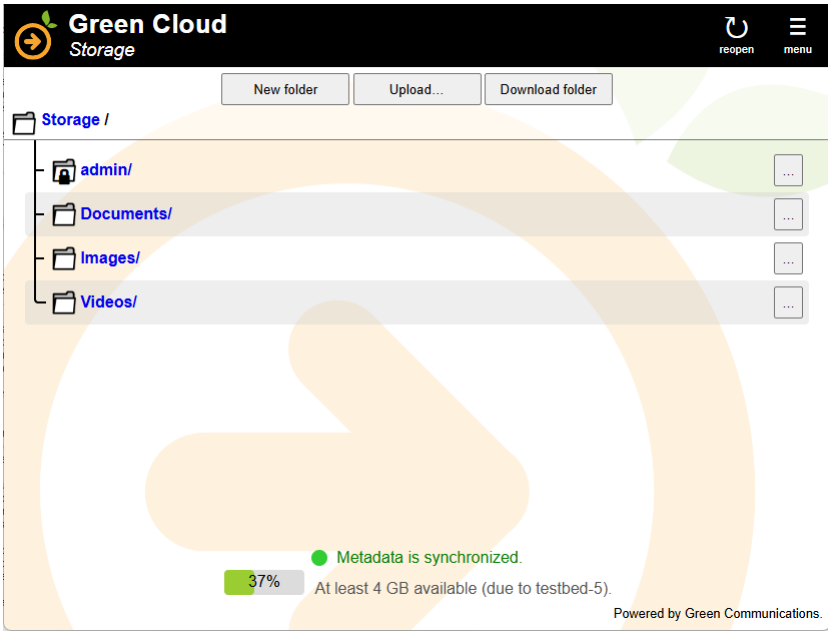

Figure 7: Application “Storage”.

Conclusion

Au vingt-et-unième siècle, toute la planète s’est orientée vers un style de vie fortement dépendant du numérique. Le modèle consiste en une concentration des données et de l’intelligence dans de grands centres de données, dont l’accès se fait par le réseau Internet. Ce modèle centralisé introduit de grands points de faiblesse : si l’accès y est interrompu, tous les services deviennent alors inaccessibles ! De nombreux comportements malveillants se sont développés à partir de cet état de fait et ont rendu l’accès aux centres de données inopérant. La cyber-résilience devient notre capacité à continuer notre activité malgré l’inaccessibilité des centres de données.

S’inspirant des modèles de batteries pour stocker l’énergie et fonctionner en l’absence d’accès à l’électricité, la solution IoE permet d’offrir les services numériques nécessaires pour continuer ses activités, même en cas d’attaques rendant l’accès au cloud et aux centres de données impossible.