Cyber Resilience

In the digital age, humans are immersed in digital services even before their birth. Ultrasounded on digital media in their mother's womb, identified by a QR code in their crib, photographed by the hundreds or thousands on tablets or phones, not to mention all the data that begins to be recorded in various data centers installed all over the planet. This, of course, continues at every stage of life and even after death. The digital world surrounds us more than anything else. More than fine particles, more than raindrops, more than sunlight! Not a gesture, nor an emotion, nor a thought occurs without the digital realm and the zeros and ones intervening to command, record, or guide them. A human's day begins and ends with the digital. Upon waking, we open our eyes to the phone screen. We read messages, we like some, we are surprised by others, and then we check the weather and the state of the roads or transport! During the day, there's an AI here and an AI there to give us advice, suggest a text, or provide a summary! We use Google search to understand a word, to get home, and to prepare our dinners. Our lifestyle, which has become universal over the years, forces us to entrust our data to large centers across the Internet, and then to wait for the instructions provided by algorithms running on machines in these data centers.

Depending on digital technology is not a fatality. We have adopted these behaviors with the help of digital services to improve our daily lives, optimize our resources, reduce waste, and lessen the burden of tasks. The only problem that arises is our ability to survive without these new services.

What is human resilience to a digital outage? If everything stops, what happens? Are we resilient to a massive power outage? Are we resilient to a network operator failure? And worse, are we resilient to a data center outage?

If you cut access to data centers for a human who is largely accustomed to and nurtured by digital services, what will happen? Will they be able to navigate the

streets, register for an exam, do their shopping, prepare their meals, take care of themselves, and fulfill their work duties? The answer, obviously, is no! We still have people from previous generations who remember the processes before the digital age, but due to lack of practice, the reflexes are no longer there. Even if we used road maps more than 30 years ago, one reflex imposes itself before even starting the vehicle's engine: plug in the navigation system!

A data center then becomes a source of our intelligence, and without constant access to this space, we can feel lost, deprived of identity, power, and action. This center can thus represent a point of failure in our daily lives.

Nowadays, attacking this weak point, this center that contains our data and our intelligence, is child's play. The number of cyberattacks per day is staggering. It is so frequent and with a very high success rate that we arm ourselves with substantial budgets to protect ourselves. Despite this, many attacks are unfortunately successful. The network to access data centers can also fail. It only takes a natural disaster, a network operator failure, sabotage, or even an overload to lose access.

Being cyber resilient means continuing to function without access to data centers. How can this be possible when we have entrusted our thinking to them and they now concentrate all our intelligence? Just like with electricity, resilience in the face of an outage is about storing energy in a battery. When a country emerges from a long war, its electricity production infrastructure is down and produces only a tiny amount, far from satisfying the population. Rationing then occurs, and with the help of batteries, we manage to store energy when it arrives, and then consume it for our resilience.

In the digital realm, to survive during an outage due to a cyberattack, the only possibility is to rely on local digital services set aside to continue our dependent activities. This is called an edge. The edge becomes our battery of digital services to ensure our resilience. When access to the cloud, which contains the data centers, becomes operational again, we can then use it and return to our usual behaviors.

What are the essential services we need to retain to maximize our cyber resilience? This is a crucial question for building our edge. For example, in electricity, the size of the battery we choose is determined by listing the machines we need to power that are essential to us. Regarding digital services, it also depends on the use cases. If we take that of a hospital, we will need at least a messaging service, telephony, file exchange, patient records, and a traceability system!

Cutting off from central points, which are the clouds, and switching to local and distributed systems, the edges, represents a significant challenge. This amounts to creating communities that evolve locally and separately, which, when they return to a connected and shared environment, will have undergone changes, leading to inconsistencies and discrepancies. Significant work is then required to bring order, with a consensus to be found to harmonize the different evolutions from an original version to a unified version.

As the CAP theorem reminds us, we cannot simultaneously guarantee a partition of our systems with availability and consistency of their data and services. During a cyberattack, services will be established in different locations in the form of edges, thus serving the people and objects present in the areas covered by these edges. Some edges may interconnect with each other, while others may remain isolated. During the merging of edges, consensus algorithms must operate to resolve all conflicts that arise during this period of resilience.
To better understand the advantages of edges in resilience, let's take the example of a hospital. Given the criticality of its data and the importance of its continuous operation, it is required to build a continuity and recovery plan in case of major issues. This plan can be based on access to multiple data centers in SaaS (Software as a Service) mode, avoiding the consolidation of all services in one place to reduce risks.

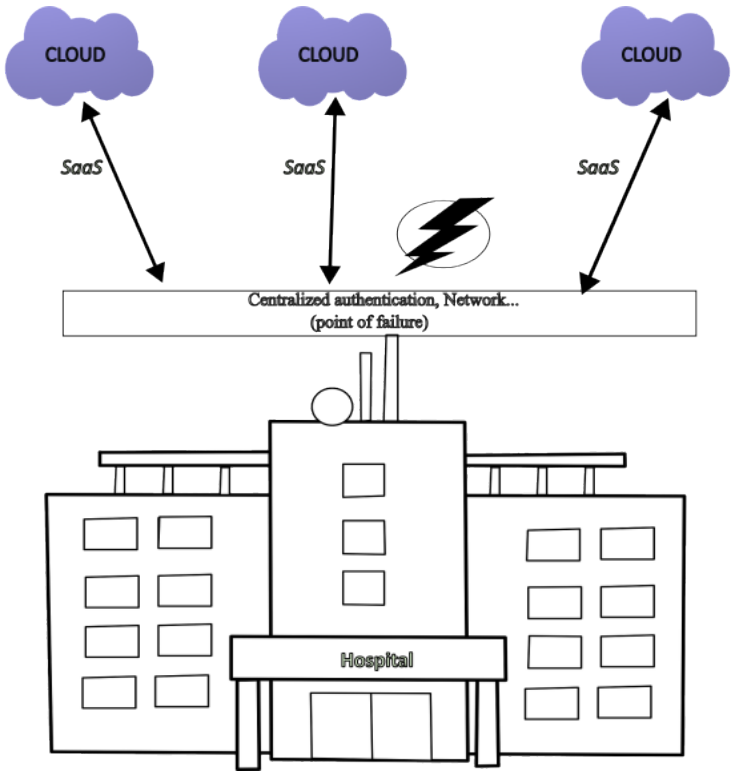

Figure 1: SaaS access.

Despite these precautions, these plans do not take into account the failure of networks and centralized authentication. Information systems, even when data is distributed across multiple locations, use an authentication server, thus representing a significant weak point in a resilience plan (Figure 1). In contrast, when data and

services are hosted on-site and accessed in a fully distributed manner, no failure is possible (Figure 2).

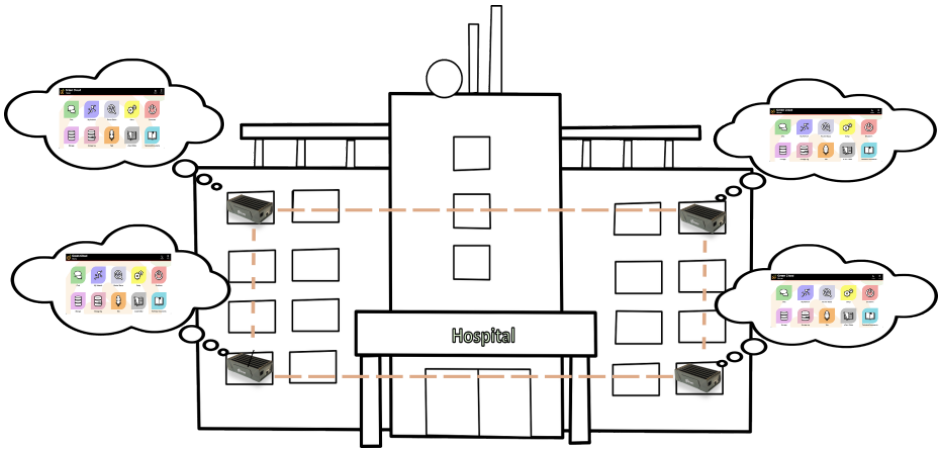

Figure 2: Distributed edge.

Green Communications offers the perfect solution for cyber resilience. When a digital infrastructure becomes inoperable due to a natural disaster, a terrorist attack, an adversary, a virus, or ransomware, no digital service can function. Thanks to very lightweight platforms that integrate numerous services, the IoE (Internet of Edges) provides you with a digital infrastructure equipped with a range of essential services to continue communicating, collaborating, and evolving with the same habits and reflexes as in normal times. The IoE solution is the Noah's ark of the digital world. When everything is struck down by a physical or cyber attack, the IoE transports you to a new world, offering essential digital services that ensure your resilience.

How does the IoE platform work :

Everything is very simple! You just need to power a set of portable units (approximately 300 g) so that they can communicate with each other and form a digital space. The number of units depends on the size of the area to be covered with this infrastructure. In this digital space, a set of services is available by default:

- A visualization application for the platform that allows users to see the covered area, the location of the machines providing coverage and their interactions, as well as all connected users and many other pieces of information.
- An instant messaging (chat) service that allows the creation of conversation rooms among all clients connected to the infrastructure.

- A voice service that enables the creation of audio conversation rooms. It can also operate in Push-to-talk mode (walkie-talkie).
- A file-sharing system for exchanging files between participants connected to the infrastructure or for creating and modifying directories. This system is coded in the form of a blockchain, where every operation performed is recorded and listed across all the units forming the digital infrastructure.
- A set of tools for the infrastructure administrator to test the performance of the infrastructure, generate logs, modify configurations, perform updates, connect to other networks, change passwords, configure DHCP, DNS, etc.
- A tool for creating a PKI (Public Key Infrastructure) to generate certificates that customize the routers of the infrastructure.
- An embedded web server so that the aforementioned services are easily accessible as web applications, without the need to download applications on a client workstation.

The infrastructure has the capability to integrate additional services necessary for the location where it is installed (for example, backup services). These services are installed on machines that connect to the infrastructure so that clients can access them. A very simple configuration tool, in the form of a web page, allows users to provide a static lease (IP address) and a domain name with just a few clicks, ensuring that the use of the service is as straightforward as possible for clients connected to the infrastructure.

The user journey

In terms of user experience, the cyber resilience infrastructure offers very user-friendly interfaces, similar to those that people use daily on their computers, tablets, or phones. The user journey takes place in several steps:

1. Take your digital device (phone, tablet, or computer) and connect to the Wi-Fi of the digital infrastructure. This can be done by using a QR code or by entering credentials on the keyboard.
2. Open a browser (Chrome, Edge, Safari, Firefox, etc.) and enter the address of the local portal. This can also be done by using a QR code or by entering the address in the URL field of the browser.
3. Accept the certificate of your infrastructure if it is not already installed on your device.

4. Figure 3 shows the web page of the local portal with all the services offered by the cyber resilience infrastructure.

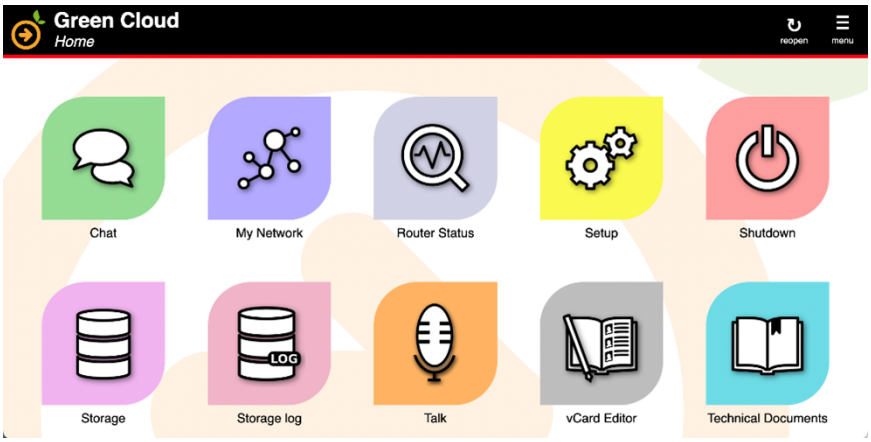

Figure 3: Le Green Cloud.

5. By clicking on the "My Network" application, the user accesses the page shown in Figure 4, where they can visualize the infrastructure, locate its nodes, connected users and their profiles, as well as a mapping and other information to enhance crisis management during the period of cyber resilience.

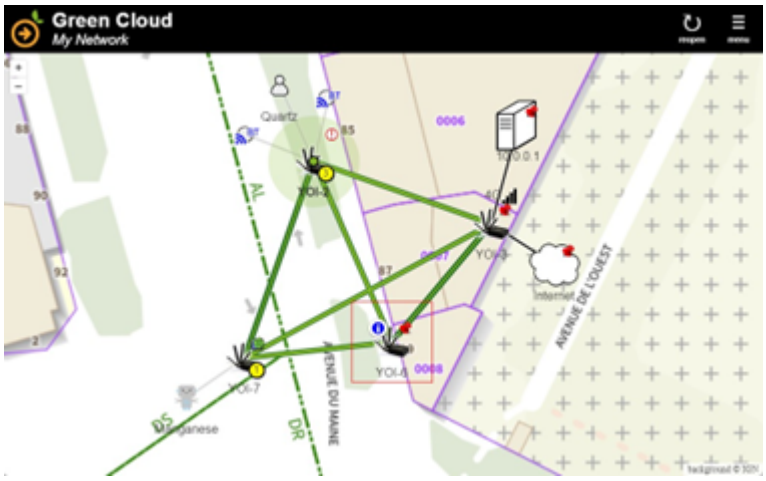

Figure 4: Application “My Network”.

6. By clicking on the "Chat" application, the user is directed to the page shown in Figure 5 where they have an instant messaging interface with user rooms

and users per room. They can send and receive messages, upload files, receive notifications, etc.

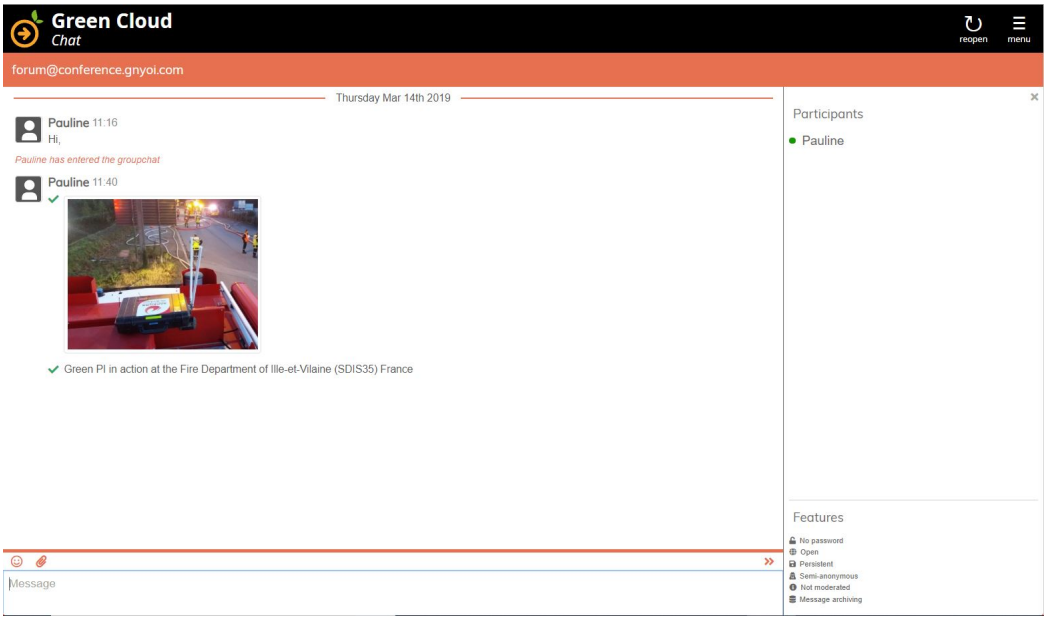

Figure 5: Application “Chat”.

7. By clicking on the "Talk" application, the user is directed to the page shown in Figure 6, where they access an audio conversation interface. They can join voice rooms, create rooms, converse with one or more users, and see the list of people in each room. The application can be used in Push-to-talk mode (open mic with a press) or in phone mode with the mic always open.

8. By clicking on the "Storage" application, the user accesses the page shown in Figure 7. This is a file-sharing space that utilizes the storage capacities of all the nodes in the infrastructure. In this application, users can upload and download files, create directories, delete directories or files, and encrypt a file with a password. The application is coded in the form of a blockchain, where every modification, addition, or deletion is recorded in a chain of blocks that is replicated across all the nodes of the infrastructure. The blockchain can be accessed by the infrastructure administrator using the "Storage log" application.

9. By clicking on "Router Status," "Setup," "Storage log," "Shutdown," "vCard Editor," users can test the performance of the infrastructure, configure it, shut it down or restart it, view logs, create user profiles (with vCards), and many

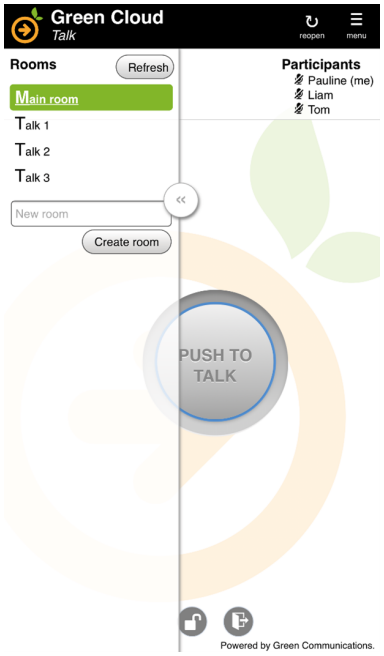

Figure 6: Application “Talk”.

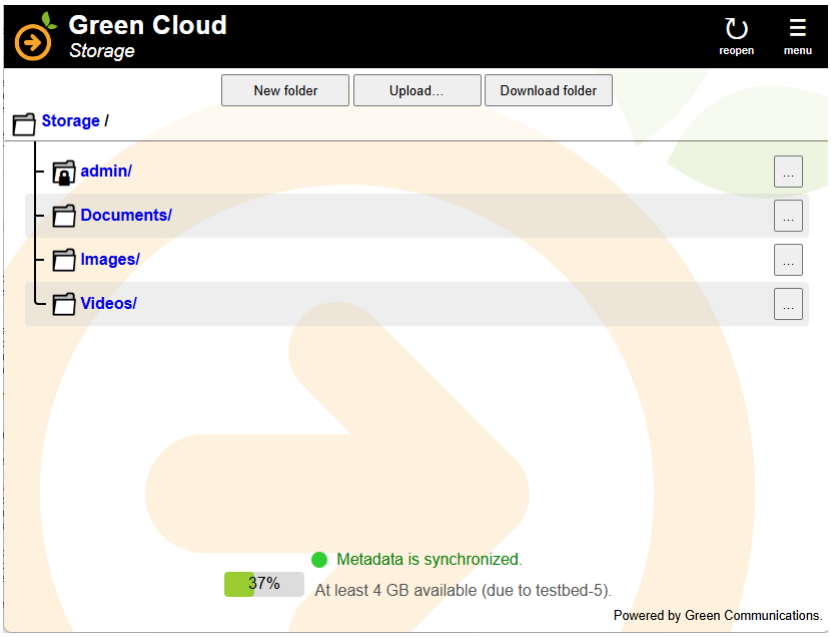

Figure 7: Application “Storage”.

other features. These applications are accessible only by the administrator, who must enter a password.

Conclusion

In the twenty-first century, the entire planet has shifted towards a lifestyle that is heavily dependent on digital technology. The model consists of a concentration of data and intelligence in large data centers, accessed via the Internet. This centralized model introduces significant points of weakness: if access is interrupted, all services become inaccessible! Many malicious behaviors have developed from this reality, rendering access to data centers inoperative. Cyber resilience becomes our ability to continue our activities despite the inaccessibility of data centers.
Inspired by battery models for storing energy and functioning in the absence of electricity access, the IoE solution provides the necessary digital services to continue operations, even in the event of attacks that make access to the cloud and data centers impossible.