La note du CERPA
N°181
10 / 2018

Chargé d'études Arthur Kremski

Transition numérique : le *Cloud Computing* au Pentagone

*Le 22 septembre 2017, l'*US Air Force *(*USAF*) a annoncé un plan d'environ un milliard de dollars sur cinq ans afin d'assurer la migration de 750 000 utilisateurs vers des services de messagerie, de communication et autres services fondés sur le* Cloud*. Cette décision résulte de la politique nationale de « priorité au* Cloud *», amorcée par le gouvernement américain depuis 2010.*

Des avantages économiques, logistiques et opérationnels

En février 2010, le gouvernement américain publie la *Federal Data Center Consolidation Initiative* (*FDCCI*). Cette étude met en exergue le caractère exponentiel du modèle de croissance des centres de données qui consomment de plus en plus d'énergie et coûtent de plus en plus cher. Pour freiner cette croissance, un plan de rationalisation des systèmes d'information est lancé. La technologie du *Cloud Computing* est au cœur de cette réforme. Elle permet de mettre en commun les capacités des centres de données et de rendre leurs capacités de calcul beaucoup plus efficaces. Cette technologie est une rupture avec une structure en réseau classique. Elle n'est plus indépendante de l'Internet et offre, en tout lieu, un accès à des informations en diffusion restreinte. En parallèle, l'*US Army,* qui entretient un réseau fermé et coûteux (le *Global Information Grid, GIG*) se saisit de cette problématique et lance son propre plan de rationalisation, le *Army Private Cloud Computing* (*APC2*) pour 249 millions de dollars[1]. Ce projet s'articule autour d'un partenariat public-privé qui repose sur l'idée que la contractualisation, dans un contexte de réduction des coûts, permet une qualité accrue du service de prestation.

Pour les opérations extérieures, l'*US Army* a créé le programme de modernisation prioritaire *LandWarNet*, un programme de partage des informations qui s'appuie sur une architecture commune aux armées et sécurisée. Il permet de transmettre une information du *Cloud* aux unités afin d'agir plus efficacement. Pour la première fois, une infrastructure *Cloud*, mise au point avec la société *Lockheed Martin*, a été déployée dès septembre 2010 en Afghanistan, le pays étant couvert par un réseau IP terrestre avec couverture sans fil (3G). Cette connexion est sécurisée et permet la transmission d'informations capitales par les soldats de manière beaucoup plus fluide et directe.

Pour ses centres de données, l'*US Army* négocie à partir de 2013 un partenariat avec *Amazon Web Services* (*AWS*), la filiale informatique de la société *Amazon* (elle accueille aujourd'hui plus de 600 agences gouvernementales pour un chiffre d'affaire d'environ 3 milliards de dollars par an). L'entreprise offre à moindre coût la mise à disposition de ses propres centres de données, assure la sécurité de ses réseaux, ce qui lui permet de garantir l'accès à des logiciels simples comme la gamme *Microsoft Office* et des logiciels plus complexes de *Big Data*, de « *deep learning* » ou encore d'analyse d'images.

Le *Cloud Computing,* un défi sécuritaire

Malgré des avantages économiques, logistiques et opérationnels avérés, le *Cloud Computing* souffre aujourd'hui d'une mauvaise réputation. En effet, il ne garantit pas le même niveau de sécurité qu'un réseau fermé, dans un monde où la surveillance serait massive et systématique. Cette représentation s'est construite tout au long des années 2010, à la suite des révélations par le site *Wikileaks* (2012), de l'affaire Snowden (2013) ou encore après le piratage du *Cloud* d'Apple (2014), révélant au grand public des photos de personnalités. Cette image est renforcée par l'activisme de la Chine et de la Russie dans le cyberespace. À cela s'ajoutent les problèmes concrets venus confirmer cette représentation. En septembre 2017, la plateforme de sécurité informatique *UpGard* révèle une faille informatique chez *AWS* permettant l'accès public à la documentation de bases de données du ministère de la Défense. En novembre 2017, le service *Web* et *Cloud* de l'entreprise *OVH* est indisponible pendant 36 heures, suite à la perte de données appartenant au Pentagone. Ces failles témoignent du problème principal de la sécurité informatique dans le *Cloud* comme sur un serveur fermé : le facteur humain. Afin de répondre à ce défi sécuritaire, le Pentagone cherche depuis mai 2018 un industriel capable d'élaborer son projet de *cloud* opérationnel (le *Joint Entreprise Defense Infrastructure*). Ce dernier devra être en mesure d'assurer la protection de données sensibles nationales ainsi que celles d'alliés.

Ainsi, le DoD *et plus largement le gouvernement américain continue à mener sa politique de transition numérique vers le* Cloud*. Le risque sécuritaire, pourtant avéré, ne semble pas remettre en question cette politique. Cela est dû au concept de cyber-résilience : le risque 0 n'existe pas et il s'agit, comme pour le domaine aérospatial, de concevoir des systèmes redondants qui peuvent continuer à fonctionner même s'ils sont affectés. Une autre voie consiste en la création d'une architecture informatique capable de se reconfigurer d'elle-même en cas d'attaque.*

Ces propos ne reflètent que l'opinion de l'auteur.

1 Le budget global pour la défense de l'année fiscale 2010 était de 680 milliards de dollars. 7,749 milliards étaient alloués à la cybersécurité.