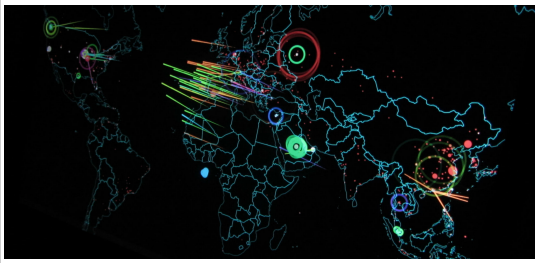
A quoi doit-on s’attendre en matière de cybersécurité à l’horizon 2020 ?

	A quoi doit-on s’attendre en matière de cybersécurité à l’horizon 2020 ?

A l'heure où les objets connectés continuent de se déployer et où les piratages de données personnelles ou professionnelles se multiplient, quel avenir peut-on envisager en termes de cybersécurité ? Un groupe de chercheurs a élaboré plusieurs scénarios.



Le Centre pour la cybersécurité à long terme, un groupe de chercheurs pluridisciplinaires de l'Université de Berkeley en Californie, s'est questionné sur ce possible avenir en fonction de divers paramètres (déploiement de l'IoT, avancées technologiques, initiatives politiques, etc.). Et selon eux, plusieurs scénarios émergent :

• The New Normal décrit un monde où les cyberattaques à grande ou petite échelle seront, en 2020, autant légion que personnelles, dépassant les pouvoirs publics par leur nombre et leur ampleur, et encombrant les cours de justice de dossiers liés à la criminalité digitale – une sorte de « Far West 2.0 » dans lequel les utilisateurs n'hésiteraient pas à se rendre justice par eux-mêmes ;

• Omega conte, quant à lui, le futur de l'analyse prédictive : bien au-delà des études démographiques, la nouvelle génération d'algorithmes pourrait cibler plus étroitement les caractéristiques et préférences d'un individu donné, ce qui pourrait introduire un débat des plus clivants, à la frontière du philosophique et du politique, sur la manipulation comportementale ;

• Sensorium, enfin, dépeint l'évolution du *quantified self* jusqu'à faire d'Internet un vaste système de « lecteurs d'émotions », comme le souligne The Conversation, touchant du doigt les aspects les plus intimes de la psychologie humaine. Au risque que les données des applications de *quantified self* émotionnelles puissent être « retournées » contre leurs utilisateurs.

Plus d'informations et plus de scénarios ici.

Réagissez à cet article

Source : *Quel avenir pour la cybersécurité à l'horizon 2020 ?*