

# *opinions*

## Et maintenant, un « 11 Septembre numérique » ?

LE POINT  
DE VUE

de Laurent Célérier

**L**a récente et fulgurante prise de pouvoir des talibans en Afghanistan conduit l'ensemble de la communauté internationale et les experts géopolitiques à s'interroger sur l'évolution de cette organisation depuis leur chute au début des années 2000. Ont-ils une doxa différente, une plus grande ouverture à l'égard de la place des femmes ou des autres religions ? Veulent-ils réellement intégrer la communauté internationale ? Par-delà ces potentielles évolutions doctrinales, c'est également leurs futurs modes d'action qu'il faut interroger.

La seule certitude est que le monde de 2021 n'est pas celui de 2001. Le numérique est devenu indispensable, tant en termes sociaux, économiques que politiques pour la plupart des sociétés. Cette transformation a également emporté avec elle des fragilités et vulnérabilités favorisant le développement de la cybercriminalité et convertissant l'espace numérique en un espace de confrontation entre Etats.

Daech a su prendre le virage du numérique et des réseaux sociaux pour frapper et fragiliser nos sociétés. L'organisation islamiste est parvenue à diffuser mondialement sa propagande, à recruter des combattants, notamment en Europe et en France, à financer et coordonner ses opérations, dont les

attentats à notre encontre. Le numérique a largement contribué à transformer le conflit syrien – local et éloigné – en une menace directe sur le territoire national conduisant à une mobilisation sans précédent des forces de sécurité, à un engagement militaire et des restrictions temporaires ou durables de liberté.

Depuis la fin du califat islamique, il y a maintenant deux ans, le champ du possible pour exploiter l'espace numérique à des fins offensives s'est encore étendu et facilité. Au-delà de l'influence grandissante des réseaux sociaux avec son corollaire de robots et d'infox, la conduite de cyberattaques est désormais une véritable activité économique avec ses acteurs spécialisés offrant leurs services de pénétration de systèmes, de vol de données, de blocage des systèmes IT par chiffrement des données et même de sabotage d'installations.

La prolifération des attaques par rançongiciels ou les récentes affaires d'espionnage sont la meilleure illustration de la vitalité de cet écosystème disponible au plus offrant et échappant encore à tout contrôle. Il est désormais possible de perpétrer des attaques mettant en grande difficulté des administrations, des entreprises ou des personnes avec relativement peu de moyens et de compétences.

Cette évolution du monde n'a pas échappé au régime taliban. La population afghane est désormais connectée à Internet (70 % dans les villes) et le nouveau pouvoir a démontré en l'espace de quelques jours sa maîtrise de la communication sur les réseaux sociaux, à l'égard de sa propre population, de Daech et de

la communauté internationale : incitation à la désertion de l'armée afghane, messages de paix et de tolérance à l'égard des minorités et des femmes, vidéos de forces talibanes victorieuses, de rencontres avec des représentants étrangers mais aussi intimidation des opposants et humiliation des forces occidentales.

Au-delà des réseaux sociaux, on peut s'inquiéter de l'utilisation que les talibans feront du numérique pour mener ou inciter à mener des actions offensives contre leurs ennemis de l'intérieur comme de l'extérieur. Vont-ils perpétrer, inciter ou laisser faire un « 11 Septembre numérique » ? La technologie est accessible et disponible, les scénarios sont documentés et démontrés : le risque existe.

Quelle que soit la nature des relations que nous entretiendrons avec les nouveaux maîtres de Kaboul et leurs intentions, l'espace numérique sera certainement impliqué, tant dans le champ des perceptions que de la technologie. Soyons vigilants et prêts à nous défendre à la hauteur des menaces.

**Laurent Célérier** est maître de conférences à Sciences Po et cadre dirigeant chez Orange Cyberdefense.

**La technologie est accessible et disponible, les scénarios sont documentés et démontrés : le risque existe.**