La note du CERPA
N°198
01 / 2019

Chargé d'études Éric Raharimbolamena

La nouvelle stratégie cyber des États-Unis

La posture cyber américaine actuelle se lit au prisme de plusieurs textes publiés en 2018 : le White House National Cyber Strategy, *l'*Unclassified Summary Department of Defense Cyber Strategy *et le* Department of Homeland Security (DHS) Cyber Security Strategy. *Ces documents permettent de dessiner les contours d'une nouvelle stratégie globale plus offensive que les précédentes, mise en œuvre par le* United States Cyber Command, *devenu officiellement un des commandements interarmées unifiés du* United States Strategic Command *le 4 mai 2018*.

La *White House National Cyber Strategy* : le noyau dur de la cyber stratégie 2018

La nouvelle stratégie cyber américaine s'articule autour de celle de la Maison Blanche, qui parachève le contenu des diverses positions prises entre 2017 et 2018. Cette déclaration confère une nouvelle autorité politique à la posture américaine, en ce qu'elle représente le premier texte à vocation globale dans le domaine cyber depuis 2011[1]. Les objectifs de la nouvelle doctrine consistent à assurer le renforcement de la capacité américaine de dissuasion dans le cyberespace, ainsi qu'à maintenir son influence et sa prospérité.

Elle est supportée par le résumé déclassifié de la cyber stratégie du département de la Défense, qui décline les modalités militaires de la compétition interétatique dans le cyberespace. Sur le territoire national, le *DoD* et le *DHS* se partagent les missions. Ces dernières consistent en la protection de 16 types d'infrastructures, dites « critiques »[2] ; un domaine large qui s'étend de la sécurité des réacteurs nucléaires jusqu'aux usines de traitement des eaux usées.

Une stratégie offensive : « *Preserve Peace Through Strength* »

La version de 2015 du département de la Défense, évoquant le concept d'« *active cyber defense* », reposait sur les principes de « *dilution* » des risques cyber et de contrôle du « *risque d'escalade* ». Ces termes ont disparu dans la nouvelle version, plus offensive, qui s'appuie sur l'usage d'un nouveau concept doctrinal : « *defend forward* », ou « *arrêter la menace avant qu'elle n'atteigne sa cible* ». Les É.-U. veulent « *se préparer à la guerre, en construisant une force plus létale* » face à des États explicitement cités : la Russie, la Chine, l'Iran et la Corée du Nord. La distinction entre les stratégies de 2015 et de 2018 repose ici essentiellement sur une gradation entre les concepts d'« *active cyber defense* » et de « *defend forward* ».

Par ailleurs, la Révision de la posture nucléaire américaine (*NPR*) interroge quant à son articulation avec la stratégie cyber : elle est remarquable pour ce qu'elle ne contient plus, depuis que sa version préliminaire a fuité. Elle indiquait que « *le Président aura une gamme élargie d'options limitées et graduées pour dissuader de manière crédible les attaques stratégiques ou non-stratégiques russes, ce qui pourrait maintenant inclure les attaques contre le NC3*[3]*, dans l'espace et le cyber espace* ».

L'accent porté sur les logiques de multilatéralisation et de coopération avec le privé

Avec l'*International Cyber Deterrence Initiative*, les É.-U. déclarent vouloir prendre la tête d'une coalition avec leurs alliés pour coordonner les réponses aux cyber-attaques, partager du renseignement, et surtout appliquer collectivement des sanctions. Cette posture de *leadership* s'appuie sur la promotion d'un internet « *ouvert, libre et fiable* ». Les É.-U. comptent assurer la cyber sécurité des espaces et des transports, ce qui s'inscrit dans la continuité de ses opérations *FONOPs*[4].

En outre et depuis 2008, les É.-U. maintiennent leur cyberdéfense des entreprises privées, en particulier celles de la BITD – aussi classées « *infrastructures critiques* » –, afin d'améliorer la confidentialité de leurs informations, garantes de la supériorité militaire américaine. Ceci s'inscrit dans une logique globale de promotion des entreprises américaines et de défense de leurs parts de marchés mondiales, dans un contexte de très forte concurrence et d'espionnage économique.

Le cyber s'érige de plus en plus comme la cinquième dimension des affaires militaires. Le budget alloué à cet effort est en nette croissance. Entre 2016 et 2017, il a cru de 35% – portant l'effort à 19Md$ – pour des programmes tels que le Cyber Excepted Service, *qui vise à attirer et retenir des compétences au sein d'une armée qui se prépare activement à tous les types de conflits.*

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

1 United States International Strategy for Cyberspace, 2011.
2 U.S. Department of Homeland Security Cybersecurity Strategy 2018, p.11.
3 « *Nuclear Command and Control and Communications* ».
4 *Freedom Of Navigation Operations* (*FONOPs*), en mer de Chine méridionale notamment.