# Les États-Unis intensifient leurs attaques en ligne contre le réseau électrique russe

*Une centrale thermique à Moscou. Les responsables ont qualifié le coup porté au réseau russe et à d'autres cibles d'action secrète afin de dénoncer publiquement les manœuvres de désinformation et de piratage de Moscou lors des élections de mi-mandat de 2018. Maxim Shemetov/Reuters*

Le 15 juin 2019, Par David E. Sanger et Nicole Perlroth
https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

WASHINGTON - Selon les responsables gouvernementaux actuels et précédents, les États-Unis intensifient leurs incursions numériques au sein du réseau électrique russe dans un avertissement au président Vladimir V. Poutine afin de lui démontrer comment l'administration Trump utilise de nouvelles technologies pour déployer des cyber outils de façon plus agressive.

Au cours d'entretiens lors des trois derniers mois, les responsables ont décrit de précédents déclenchements non signalés du code informatique américain dans le réseau russe et autres cibles comme un moyen secret pour dénoncer publiquement les actions de désinformation et de piratage de Moscou lors des élections de mi-mandat de 2018.

Les partisans d'une stratégie plus agressive ont déclaré qu'il était grand temps, voilà des années que le Département de la sécurité intérieure et le F.B.I lançaient des avertissements publics pour signaler que la Russie avait inséré des logiciels malveillants qui pouvaient, lors d'un éventuel conflit avec les États-Unis, saboter les centrales électriques, les oléoducs et gazoducs américains ou les réserves en eau.

Mais cette manœuvre comporte aussi un fort risque d'escalade de la guerre froide numérique quotidienne entre Washington et Moscou.

L'administration a refusé de décrire les mesures spécifiques qu'elle prenait en vertu des nouvelles compétences accordées l'an dernier, tant par la Maison-Blanche que par le Congrès au Cyber

Commandement des États-Unis, le bras du Pentagone qui dirige les opérations offensives et défensives virtuelles de l'armée.

Mais lors d'une intervention publique mardi, le conseiller à la sécurité nationale du président Trump, John R. Bolton, a déclaré que les États-Unis élargissaient dorénavant leur champs de vision concernant les cibles numériques potentielles dans le cadre d'un processus visant à " dire à la Russie, ou à quiconque se lancerait dans des cyber opérations contre nous,'Vous allez le payer cher.'"

Depuis des années, les réseaux électriques sont un champ de bataille de faible intensité.

Selon les responsables actuels et précédents, les États-Unis ont placé des sondes de reconnaissance dans les systèmes de contrôle du réseau électrique russe depuis au moins 2012.

Les responsables précisent que maintenant, la stratégie américaine s'oriente davantage vers l'offensive, avec l'introduction de logiciels malveillants potentiellement invalidant au sein du système russe à une intensité et avec une agressivité jamais été tentées auparavant. Il s'agit, d'une part, de servir d'avertissement mais, d'autre part, à être en mesure de mener des cyber-grèves si un conflit majeur éclatait entre Washington et Moscou.

Le commandant du Cyber Commandement des États-Unis, le général Paul M. Nakasone, s'est exprimé ouvertement sur la nécessité d'une " défense en attaque " au cœur des réseaux de l'adversaire pour démontrer que les États-Unis réagiront à une ligne d'attaques à leur encontre.

*Le conseiller à la sécurité nationale du président Trump, John R. Bolton, a déclaré que les États-Unis adoptaient une vision plus large des cibles numériques potentielles dans le cadre d'un effort visant à avertir quiconque "s'engage dans des cyber-opérations contre nous".Doug Mills/The New York Times*

"Ils n'ont pas peur de nous ", a-t-il déclaré au Sénat il y a un an lors de son audition de prise de mandat.

Mais trouver les moyens pour ajuster l'intensité des réponses dans un effort de dissuasion sans déclencher une escalade dangereuse a été la source d'un débat constant.

L'été dernier, M. Trump a accordé de nouvelles autorisations au Cyber Command dans un document encore confidentiel connu sous le nom de National Security Presidential Memoranda 13,accordant au général Nakasone beaucoup plus de latitude pour mener des opérations offensives en ligne sans avoir besoin de l'approbation du président.

Mais l'action conduite au sein du réseau électrique russe semble avoir été menée sous de nouvelles autorisations législatives peu connues, glissées dans le projet de loi sur les autorisations militaires adopté par le Congrès l'été dernier. La mesure a approuvé la conduite régulière d'"activités militaires clandestines" dans le cyberespace, pour "décourager, se protéger ou se défendre contre des attaques ou des cyber-activités malveillantes contre les Etats-Unis".

En vertu de la loi, ces actions peuvent maintenant être autorisées par le secrétaire de la défense sans approbation spécifique du président.

" Au cours de cette dernière année, c'est devenu beaucoup plus agressif ", a déclaré un haut responsable du renseignement, s'exprimant sous couvert d'anonymat, mais refusant de discuter de programmes classifiés particuliers. "Nous faisons des choses à une échelle que nous n'avions jamais envisagée il y a quelques années."

La question cruciale - impossible à connaître sans avoir accès aux détails classifiés de l'opération - est de savoir jusqu'à quel point les États-Unis se sont immiscés dans le réseau russe. Ce n'est qu'alors qu'on saura clairement s'il est possible de plonger la Russie dans les ténèbres ou de paralyser son armée - une question à laquelle il est impossible de répondre tant que le code n'est pas activé.

Tant le général Nakasone que M. Bolton, par la voix de leurs porte-paroles, ont refusé de répondre aux questions concernant les incursions dans le réseau russe. Les responsables du Conseil national de sécurité ont également refusé de commenter, mais que les détails des reportages du New York Times sur le ciblage du réseau russe ne les inquiétaient aucunement en matière de sécurité nationale, ce qui montre peut-être que certaines de ces intrusions avaient pour objectif d'être connues des Russes.

Prenant la parole mardi lors d'une conférence organisée par le Wall Street Journal, M. Bolton a déclaré : "Nous avons pensé que la réponse dans le cyberespace contre l'ingérence électorale était l'an dernier la plus grande priorité, et c'est donc ce sur quoi nous nous sommes concentrés. Mais nous ouvrons maintenant la brèche, élargissant ainsi les domaines dans lesquels nous sommes prêts à agir."

Il a ajouté, se référant aux nations ciblées par les opérations numériques américaines, "Nous vous ferons payer le prix jusqu'à ce que vous nous compreniez."

Deux responsables de l'administration ont déclaré qu'ils pensaient que M. Trump n'avait pas été pleinement informé des étapes à suivre pour placer des "implants" - code logiciel qui peut être utilisé pour la surveillance ou une attaque - du réseau Russe.

Les responsables du Pentagone et du renseignement ont décrit une grande hésitation pour entrer dans les détails avec M. Trump au sujet des opérations menées contre la Russie par crainte de sa réaction - et la possibilité qu'il puisse s'y opposer ou en discuter avec des responsables étrangers, comme il l'avait fait en 2017 quand il avait mentionné au ministre russe des affaires étrangères une opération sensible en Syrie.

Comme la nouvelle loi définit les actions dans le cyberespace comme s'apparentant à une activité militaire traditionnelle au sol, dans les airs ou en mer, une telle information ne serait pas nécessaire, ont-ils ajouté.

La finalité des opérations a été qualifiée de différentes façons par plusieurs responsables actuels et précédents de la sécurité nationale. Certains l'ont intitulée " signalement " à la Russie, une sorte de tir numérique de sommation. D'autres ont dit que ces mesures visaient à permettre aux États-Unis de réagir si M. Poutine devenait plus agressif.

*Le général Paul Nakasone, commandant du Cyber Commandement des États-Unis, a obtenu plus de latitude pour mener des opérations offensives en ligne hors de l'approbation du Président. Erin Schaff pour le New York Times*

Jusqu'à présent, rien ne prouve que les États-Unis aient effectivement coupé le courant dans des tentatives visant à établir ce que les responsables américains appellent une "présence persistante" dans les réseaux russes, tout comme les Russes n'ont pas coupé le courant aux États-Unis. Mais l'introduction de codes malveillants au sein des deux systèmes ravive la question de savoir si le réseau électrique d'un pays - ou toute autre infrastructure critique assurant le fonctionnement des maisons, des usines et des hôpitaux - constitue une cible légitime pour une attaque en ligne.

Déjà, de telles attaques figurent dans les plans militaires de nombreux pays. Dans un de ses précédents postes, le général Nakasone a été largement impliqué dans l'organisation d'une opération nommée Nitro Zeus, qui constituait un dispositif de guerre visant à débrancher l'Iran si les États-Unis entraient en guerre avec ce dernier.

La façon dont le gouvernement de M. Poutine réagit à la plus grande agressivité américaine décrite par M. Bolton n'est pas encore connue.

"C'est la diplomatie de la canonnière du XXIe siècle ", a déclaré Robert M. Chesney, professeur de droit à l'Université du Texas, qui a beaucoup écrit sur l'évolution du fondement juridique des opérations numériques. "Nous montrons à l'adversaire que nous pouvons infliger des coûts importants sans avoir à faire grand-chose. Nous avions l'habitude de mouiller les bateaux à portée de vue du rivage. Maintenant, peut-être qu'on a accès à des systèmes clés comme le réseau électrique."

Depuis plus d'une décennie, l'intrusion russe dans les infrastructures américaines est le bruit de fond de la compétition entre superpuissances .

*On ne sait pas encore comment le gouvernement du président Vladimir V. Poutine réagirait à la plus grande agressivité américaine. Dmitri Lovetsky/Associated Press*

Une intrusion russe couronnée de succès dans les réseaux de communications classifiés du Pentagone en 2008 a entraîné la création de ce qui est devenu Cyber Command. Sous le président Barack Obama, les attaques se sont multipliées.[Le United States Cyber Command est un des dix commandements interarmées de combat des forces armées des États-Unis, chargé de la sécurité de l'information pour le Département de la Défense.NdT]

Mais M. Obama hésitait à répondre à une telle agression de la Russie par des contre-attaques, en partie parce qu'il craignait que les infrastructures des États-Unis soit plus vulnérables que celles de Moscou et en partie parce que les responsables du renseignement craignaient que le Pentagone, en répondant de la même façon, ne révèle certaines de ses meilleures technologies.

À la fin du premier mandat de M. Obama, les représentants du gouvernement ont commencé à découvrir un groupe de pirates informatiques russes, également connu des chercheurs en sécurité privée, sous le nom de Energetic Bear ou Dragonfly. Mais on a supposé que les Russes faisaient de la surveillance et n'iraient pas jusqu'à la désorganisation réelle.

Selon deux anciens fonctionnaires, cette hypothèse a été battue en brèche en 2014, lorsque le même groupe de pirates informatiques russes a corrompu les mises à jour de logiciels, atteignant des centaines de systèmes ayant accès aux commutateurs électriques.

"C'était la première étape de la préparation à long terme d'une attaque ", a déclaré John Hultquist, directeur de l'analyse du renseignement chez FireEye, une société de sécurité qui avait repéré ce groupe.

En décembre 2015, une unité de renseignement russe a privé de courant des centaines de milliers de personnes en Ukraine occidentale. L'attaque n'a duré que quelques heures, mais elle a suffi à soulever les inquiétudes de la Maison-Blanche.

*En 2012, le secrétaire à la Défense de l'époque, Leon E. Panetta, a été mis en garde contre les intrusions en ligne de la Russie, mais le président Barack Obama était réticent pour déclencher des contre-attaques en réponse à cette agression de Moscou.Luke Sharrett pour le New York Times*

Selon des responsables et un avis de sécurité intérieure qui n'a pas été publié avant décembre 2016, une équipe d'experts américains a été dépêchée sur place pour examiner les dégâts et a conclu qu'une de ces mêmes unités de renseignement russes qui avaient fait des ravages en Ukraine avait aussi fait des incursions importantes dans le réseau énergétique des États-Unis.

"C'était notre traversée du Rubicon ", a déclaré David J. Weinstein, qui travaillait auparavant pour Cyber Command et qui est maintenant chef de la sécurité chez Claroty, une entreprise de sécurité spécialisée dans la protection des infrastructures critiques.

Fin 2015, au moment même où commençaient les intrusions au Comité national démocrate, une autre unité russe de piratage informatique a commencé à cibler les infrastructures américaines essentielles, notamment le réseau électrique et les centrales nucléaires. A partir de 2016, les pirates surveillaient de près les systèmes qui commandent les interrupteurs d'alimentation dans les usines.

Jusqu'aux derniers mois de l'administration Obama, le Cyber Commandement se limitait en grande partie à mener des opérations de surveillance à l'intérieur des réseaux russes. Lors d'une conférence organisée cette année par la Fondation Hewlett, Eric Rosenbach, ancien chef d'état-major du secrétaire à la Défense et actuellement à Harvard, a averti que lorsqu'il s'agissait d'opérations offensives, " ce n'est pas si souvent que nous y avons recours ". Il a ajouté : "Je peux compter sur les doigts de la main, littéralement, le nombre d'opérations offensives que nous avons menées au Département de la Défense."

Mais après les intrusions au moment des élections et les incursions dans le réseau électrique, l'administration Obama a estimé qu'elle avait été trop passive.

M. Obama a secrètement donné l'ordre pour une sorte d'envois de messages au sein du réseau russe, les détails n'en ont jamais été rendus publics. Il n'est pas sûr qu'il y en ait eu beaucoup.

La cybernétique offensive n'est pas la cyberattaque magique où l'on dit : " D'accord, envoyez l'avion et nous laisserons tomber la cyberattaque au-dessus de la Russie demain ", a déclaré M. Rosenbach lors de la conférence, refusant de discuter d'opérations spécifiques.

Après l'investiture de M. Trump, les pirates russes n'ont cessé de multiplier les attaques.

La première cyber-équipe de M. Trump a décidé d'être beaucoup plus transparente dans sa dénonciation de l'activité russe. Au début de 2018, elle a désigné la Russie comme le pays responsable de " la cyber attaque la plus destructrice de l'histoire humaine ", elle a paralysé une grande partie de l'Ukraine et affecté des entreprises américaines comme Merck et FedEx.

Quand le général Nakasone a pris le commandement du Cyber Command et de la N.S.A. il y a un an, son état-major estimait qu'il y avait des actes de piratage commis par les Russes sur des cibles, notamment la Wolf Creek Nuclear Operating Corporation, qui exploite une centrale nucléaire près de Burlington (Kan.), ainsi que des tentatives non signalées d'infiltrer la centrale nucléaire Cooper du Nebraska Public Power District, située à Brownville. Les pirates s'étaient introduits dans les réseaux de communication, mais n'avaient jamais pris la main sur les systèmes de contrôle.

En août, le général Nakasone a utilisé la nouvelle compétence accordée au Cyber Command par la directive présidentielle secrète pour submerger les systèmes informatiques de l'Agence russe de recherche sur Internet - le groupe qui avait été au cœur du piratage lors des élections de 2016 aux États-Unis. C'était l'une des quatre opérations que son soi-disant petit groupe russe avait organisées autour des élections de mi-mandat. Les fonctionnaires en ont parlé publiquement, bien qu'ils aient fourni peu de détails.

Mais les récentes actions des États-Unis contre les réseaux électriques russes, qu'il s'agisse d'avertissements ou d'armes offensives potentielles, semblent avoir été menées dans le cadre des nouvelles directives du Congrès.

Alors que se préparent les élections de 2020, le Cyber Command a examiné la possibilité que la Russie tente des coupures de courant sélectives dans des États clés, ont déclaré certains responsables. Pour cela, ils ont indiqué avoir besoin d'un moyen de dissuasion.

Ces derniers mois, la détermination de Cyber Command a été mise à l'épreuve. Au cours de l'année écoulée, des sociétés énergétiques des États-Unis et des exploitants pétroliers et gaziers de toute l'Amérique du Nord ont découvert que leurs réseaux avaient été fouillés par les mêmes pirates informatiques russes qui avaient démantelé avec succès les systèmes de sécurité en 2017 à Petro Rabigh, une usine pétrochimique et raffinerie de pétrole saoudienne.

La question est maintenant de savoir si le dépôt de l'équivalent des mines terrestres dans un réseau électrique étranger est la façon la plus efficace de dissuader la Russie. Bien qu'il s'agisse d'un mode d'action parallèle à la stratégie nucléaire de la guerre froide, cela fait également des réseaux électriques des objectifs légitimes.

"Il se peut que nous devions prendre le risque de prendre des coups dans le cadre de représailles, juste pour montrer au monde que nous ne nous couchons pas et que nous ne subissons pas" a déclaré Robert P. Silvers, associé du cabinet juridique Paul Hastings et ancien fonctionnaire du gouvernement Obama. "Parfois, il faut accepter de saigner du nez pour ne pas se prendre une balle dans la tête en chemin."

David E. Sanger, de Washington, et Nicole Perlroth, de San Francisco.