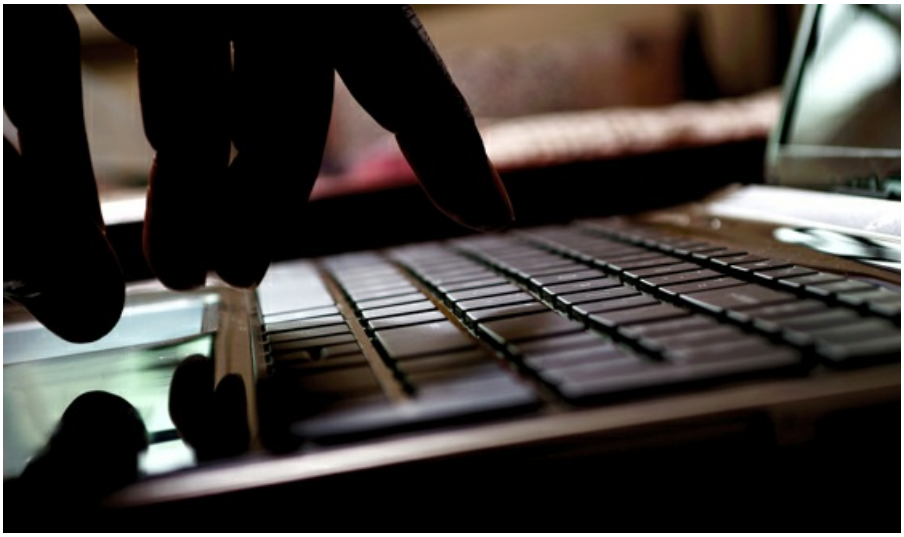
laTrompette



ISTOCK.COM/JAMINWELL

La guerre cybernétique est pire que jamais

- Richard Palmer
- 26/02/2018

L' Amérique est vulnérable aux cyberattaques. Vous n'êtes probablement pas surpris par cela. Mais vous pourriez être surpris d'apprendre *combien* vulnérable elle est. En 2017, près de deux fois le nombre de cybercrimes en Amérique ont été rapportés par rapport à l'année précédente. De 2015 à 2016, le nombre d'attaques de rançons (dans lesquelles les pirates informatiques détiennent les données d'une victime en tant que rançon) ne s'est pas accru de 100%, 200% ou 300%, mais de 16,700% selon une estimation.

Cela peut être qualifié de « cybercrimes », mais ce n'est souvent pas seulement des criminels véreux derrière ces attaques, mais des gouvernements étrangers.

L'expert en défense Peter W. Singer a passé en revue cette menace croissante dans un article intitulé « L'État de l'Union digitale 2018 : Les sept péchés capitaux de la cyber sécurité auxquels nous devons faire face », publié le 30 janvier sur *War on the Rocks*. Le danger des cyberattaques s'est dramatiquement aggravé ces dernières années. C'est une histoire que trop peu connaissent.

Voici un résumé de certains de ses points les plus importants :

Une explosion d'attaques

L'année dernière a été l'année la plus coûteuse pour les cyberattaques. FedEx est juste l'une des nombreuses entreprises bien connues à perdre des centaines de millions de dollars. Et ce n'est pas seulement le nombre d'attaques qui s'est accru, c'est aussi le danger. Singer a écrit qu'il y a eu une explosion dans le nombre de « méga-infractions »—des cyberattaques où au moins 10 millions d'identités sont exposées. En 2012, il n'y avait qu'une de ces violations. Maintenant, elles sont si communes que nous leur prêtons peu d'attention.

« Par exemple, beaucoup se souviennent de la violation du magasin *Target* d'il y a cinq ans qui a affecté 41 millions d'Américains », a écrit Singer. « Mais peu ont même remarqué la perte des données électorales de près de 200 millions Américains en 2017 (noms, date de naissance, adresse, numéros de téléphone, des détails d'inscription sur les listes électorales) par *Deep Root Analytics*, une firme de marketing qui travaille pour le Comité national républicain. »

Avec de plus en plus de ces données à l'air libre, les individus hostiles ou les gouvernements peuvent combiner les données divulguées et construire un énorme stock de connaissances sur des millions d'Américains.

'L'effondrement de la dissuasion'

L'Amérique a subi des attaques répétées de la part de nations étrangères. La Russie a ciblé à la fois les comités nationaux démocrates et républicains. Les pays étrangers ont également ciblé les institutions gouvernementales et les réseaux privés essentiels, tels que ceux de l'industrie financière. Quelle fut la réponse de
l'Amérique ?

Rien.

« L'échec à répondre clairement a enseigné non seulement à la Russie, mais à tout autre qui serait un attaquant potentiel, que de telles opérations sont relativement sans pertes du point de vue des coûts, et tout à gagner du coté des bénéfices, » a écrit Singer. « Avant que ce calcul soit modifié, les États-Unis devraient s'attendre à voir non seulement la Russie continuer à cibler ses citoyens et ses institutions ... mais aussi d'autres nations et groupes non étatiques à la recherche de gains similaires. »

Le terrain d'essai Ukrainien

L'Ukraine a vu certaines des pires cyberattaques ces dernières années. Le 23 décembre 2015, les pirates informatiques ont coupé le courant à 80,000 foyers pendant six heures. L'année suivante, ils ont frappé de nouveau, avec une attaque beaucoup plus sophistiquée. Singer a expliqué que ces attaques devraient être une grande préoccupation bien au-delà de l'Ukraine :

La Russie a traité l'Ukraine comme une sorte de laboratoire de combat pour toutes sortes de nouvelles cyber-menaces et tactiques. Pensez-y comme une version numérisée de comment la guerre civile des années 1930 en Espagne fut utilisée par les Allemands, pas seulement pour affiner la technologie de la Blitzkrieg, mais aussi pour apprendre exactement jusqu'où le monde leur permettrait d'aller. Le plus inquiétant a été une série d'attaques russes contre des réseaux électriques civils, le type d'attaques qui ont longtemps été le scénario cauchemardesque de la cyber sécurité, mais ici encore sans conséquence. Cela a été accompagné d'attaques exploratoires sur des domaines précédemment interdits dans les infrastructures cruciales, comme dans les centrales nucléaires aux États-Unis et en Europe.

Le dirigeant de l'équipe enquêtant sur les attaques contre l'Ukraine disait que lorsque l'auteur de ces piratages informatiques « détermine finalement l'infrastructure cruciale Occidentale, et que les gens réagissent comme si c'était une grande surprise, je vais la perdre ».

‘L'Internet des choses’

Les cyberattaques pourraient être sur le point de s'aggraver parce qu'il y a plus de « choses » qui continuent de se faire en ligne. On estime que 9 milliards d'appareils sont en ligne actuellement, et ceci pourrait doubler, tripler ou augmenter encore plus au cours des cinq prochaines années. De nouvelles voitures intelligentes, des téléviseurs, des thermostats, des centrales électriques et autres objets du monde réel sont en train d'être fabriqués avec une connectivité Internet, ce qui signifie qu'il y a de plus en plus de choses à attaquer. La sécurité de ces appareils est souvent effroyable. La *plupart* de ces périphériques compatibles avec l’Internet ont des failles de sécurité connues.

Ces nouvelles connections pourraient signifier que les pirates informatiques peuvent commencer à causer plus de dégâts *physiques* avec des *cyber*attaques. Ce genre d'attaques « coûtera non seulement de l'argent à venir, mais des vies, » a écrit Singer.

Dépendance envers les étrangers

Pour tous ces appareils intelligents, que ce soit à la maison, dans une centrale électrique ou dans l'armée, l'Amérique compte sur les nations étrangères pour fabriquer les composants clés. « Jamais auparavant une nation n'a été en compétition géostratégique avec une autre nation qui fabrique des parties substantielles de sa technologie commerciale et militaire », a écrit Singer. « C'est la situation embarrassante pour les États-Unis, qui se trouvent redevables à la Chine, jusqu'au niveau des puces électroniques. Cela crée non seulement un type de dépendance jamais vu auparavant, mais aussi celle qui peut être exploitée par le potentiel de ‘piratages matériels’, où des vulnérabilités pourraient être intégrées dans des systèmes d'une manière qui ne pourrait pas être rendue évidente pendant des années ou même des décennies. Les puces que vous achetez aujourd'hui pourraient vous coûter une guerre demain. »

Le talon d'Achille de l'Amérique

« L'Amérique est la plus grande superpuissance que ce monde ait jamais connue », a écrit le rédacteur en chef Gérald Flurry dans l'article « Le talon d'Achille de l'Amérique », publié dans le numéro de la *Trompette* de janvier 1995. « Mais nous avons un point très vulnérable dans notre armée—notre propre talon d'Achille. C'est si dangereux que je suis étonné que cela n'ait pas reçu plus de publicité. »

Il citait l'analyste de la défense Joseph de Courcy, qui a écrit : « La dépendance à l'ordinateur est le talon d'Achille du monde occidental, et dans quelques années cette faiblesse pourrait être testée au maximum. »

Au contraire, cette faiblesse est encore pire aujourd'hui. Et encore elle reçoit peu de publicité.

M. Flurry a écrit que l'avertissement de M. de Courcy lui rappelait immédiatement d’Ézéchiel 7 : 14 : « On sonne de la trompette, tout est prêt ; mais personne ne marche au combat ; car ma fureur éclate contre toute leur multitude. »

« Il semble que tout le monde s'attend à ce que notre peuple aille au combat, mais la plus grande tragédie imaginable se

produit ! » écrit M. Flurry. « Personne ne va au combat—même si la trompette sonne ! Cela sera-t-il à cause d'un terrorisme informatique ? »

Dans son article, M. Flurry attire une attention particulière sur l'Allemagne. En avril de l'année dernière, l'Allemagne a lancé un nouvel état-major du service Cyber et information. Quand il atteindra son plein effectif de 13 500, il comprendra presque autant de personnel que la marine allemande. Et il travaille pour mener des cyberattaques offensives.

L'image décrite par M. Flurry dans son article de 1995 est maintenant plus plausible que jamais.

Les cyber-vulnérabilités de l'Amérique existent pour une raison importante, écrivait M. Flurry :

L'une des principales raisons pour lesquelles nous avons gagné la Deuxième Guerre mondiale, c'est que les Britanniques avaient brisé le code radio allemand. Nous connaissions la plupart de leurs plans de guerre à l'avance. Tout un avantage gigantesque.

Je crois que la violation du code fut un miracle de Dieu pour nous aider à gagner la guerre. Mais nous refusons avec arrogance de donner le crédit à Dieu pour les nombreux miracles qui nous ont sauvés durant la Deuxième Guerre mondiale.

Dieu avait une main dans l'histoire de la Grande-Bretagne et de l'Amérique, et Il a une main dans les événements d'aujourd'hui. « La raison générale pour laquelle cette crise a eut lieu était parce que la ‘colère de Dieu est sur toute la multitude’, a écrit M. Flurry. « L'une des malédictions de Dieu viendra-t-elle sur nous sous la forme d'un terrorisme informatique ? Nous ne recevons pas les bénédictions de Dieu. Nous sommes maudits (Lévitique 26, Deutéronome 28). »

Dans Ézéchiel 7 : 9, Dieu dit qu'Il est derrière ces malédictions afin qu'ils « sachent que Je suis le Seigneur, celui qui frappe ».

Il y aura des conséquences épouvantables à cause de cette terrible faiblesse. Mais cela fait toute partie du plan de Dieu pour qu'Israël et le monde en viennent à le connaître.

Pour en savoir plus sur cette vulnérabilité, lisez notre article sur les tendances « Pourquoi la*Trompette* surveille les cyber-vulnérabilités de l'Amérique ». ▪