laTrompette

Cyber attacks by Christiaan Colen on flickr/CC by 2.0

L'Allemagne se prépare pour la guerre du futur

Berlin a créé une nouvelle branche militaire pour prendre les devants dans la guerre hybride de haute technologie.

- Josue Michels
- 21/06/2017

Des centaines de milliers de cibles dans le monde ont été frappées par des armes dangereuses en mai. Ces armes n'étaient pas cinétiques, biologiques, chimiques ou nucléaires ; ils étaient électroniques. Les cibles étaient des ordinateurs dans 150 pays, y compris 70,000 appareils dans le Service national de la santé de la Grande-Bretagne, tels que les ordinateurs, les scanners et les équipements de stockage. L'attaque a également frappé FedEx, Deutsche Bahn, Telefónica, Taiwan Power Co., les entreprises d'investissement, les compagnies d'assurance et de nombreuses autres entreprises, organisations et particuliers.

Les armes étaient des variations d'une cyber-attaque appelée *WannaCry*. Le logiciel malveillant accède aux fichiers informatiques, les crypte et les maintient en rançon, exigeant des paiements de 300 $ à 600 $ par ordinateur en échange du retour des fichiers à leur état non chiffré. Europol a déclaré que l'attaque était sans précédent.

WannaCry est le dernier rappel que le monde est entré dans un nouvel âge qui n'était autrefois que de la science-fiction. La cyber-guerre n'est plus une fantaisie de film, mais plutôt une réalité réelle qui menace des nations entières. Une nouvelle course aux armements a commencé, pas pour les navires de guerre, les avions, les chars ou même les armes nucléaires, mais pour les armes cybernétiques.

Et l'Allemagne vient de se positionner en avant dans la course, de façon spectaculaire.

Le 1er avril, l'armée allemande a lancé sa plus grande entreprise pour lutter contre les cyber-menaces, en établissant une nouvelle sixième branche: le Commandement de l'information et du cyberespace. Le commandement fonctionnera au même niveau que l'armée, les forces aériennes et la marine.

La ministre de la Défense, Ursula von der Leyen, a nommé le lieutenant-général Ludwig Leinhos pour être le premier cyber-général de l'Allemagne. Leinhos finira par diriger une équipe de 13,500 spécialistes en informatique, dont beaucoup sont déjà employés par la Bundeswehr dans divers endroits. C'est une force énorme. Le personnel est proche de celui de la marine allemande.

L'Allemagne veut prendre ce cyber-militaire massif et l'entraîner non seulement pour se défendre contre des attaques comme *WannaCry*, mais aussi pour lancer ses propres cyber-attaques.

« Plus qu'une étape importante »

Le 5 avril a été le premier jour au bureau pour la nouvelle équipe et un grand jour dans l'histoire militaire allemande. Von der Leyen l'appelait « plus qu'une étape importante » pour la Bundeswehr. « Cela nous positionne à l'avant-garde au niveau international, » a-t-elle déclaré (traduction de *la Trompette* tout au long).

Le journal hebdomadaire de l'armée allemande, *Bundeswehr Aktuell*, a loué le nouveau commandement en avril et a

déclaré qu'avec cela, l'armée allemande « prend un rôle de pionnier au sein de l'OTAN ».

Le ministère allemand de la Défense affirme que la cyber-sécurité est cruciale. Il estime que jusqu'à 80 pour cent des nouveaux développements pertinents pour l'armée se déroulent actuellement dans la cyber-aréna et affirme que la plupart des conflits sont combattues—en tout ou en partie—dans le cyberespace.

Seulement au cours des neuf premières semaines de cette année, 284,000 attaques étaient destinées aux ordinateurs de la Bundeswehr.

L'Allemagne crée également un centre de cyber-recherche à l'Université de la Bundeswehr à Munich. Ce centre de cyber-innovation vise à combiner les ressources de la Bundeswehr avec l'ingéniosité du secteur privé et des nouveaux entrepreneurs. En 2016, la Bundeswehr a embauché 60% de plus d'informaticiens qu'il n'a engagé en 2015, grâce en grande partie à des campagnes de relations publiques réussies et à des allocations généreuses. Si cette tendance se poursuit, l'obtention de personnel qualifié sera un problème du passé.

La meilleure défense : une bonne offensive

Comme dans tout autre type de guerre, une attaque offensive est la meilleure défense. La seule façon d'éliminer complètement la menace d'une cyber-attaque est d'éliminer la source.

« Si les réseaux de l'armée allemande sont attaqués, nous pouvons nous défendre, » a déclaré von der Leyen lors du lancement de la nouvelle installation. « Dès qu'une attaque met en danger la préparation fonctionnelle et opérationnelle des forces de combat, nous pouvons répondre avec des mesures offensives ».

Le secrétaire adjoint à la Défense Katrin Suder a dit qu'une partie de la mission étrangère du Commandement de l'information et du cyberespace était de surveiller, perturber et isoler les communications des adversaires.

La nouvelle équipe disposera des moyens technologiques et de la formation pour mener ces attaques offensives, mais la base juridique nécessite encore des éclaircissements. Dans une interview avec *Die Welt* publiée le 16 avril, von der Leyen a déclaré que, selon la loi fondamentale allemande, la Bundeswehr est autorisée à réagir lorsque l'armée elle-même est attaquée directement. Elle a dit que la même chose est vraie dans le cyberespace. Mais la situation est différente lorsque l'état allemand est attaqué. S'il y a une attaque contre le Bundestag, par exemple, von der Leyen veut que l'armée puisse réagir. Étant donné que les capacités cybernétiques se sont développées longtemps après la formulation de la Loi fondamentale allemande, les tribunaux allemands devront préciser dans quelle mesure l'équipe peut utiliser ses capacités offensives.

Un âge de post-dissuasion

Quelle que soit la légalité, l'Allemagne développe la capacité de lancer des cyber-attaques dans un âge où nous commençons tout juste à voir le potentiel de ces attaques. Les leaders comparent la puissance potentielle des cyber-armes aux armes nucléaires. En 2013, le sénateur américain John Kerry a qualifié les nouvelles cyber-technologies de « l'équivalent des armes nucléaires du XXIe siècle ».

Une nation n'a plus besoin de craindre les armes nucléaires de son adversaire si elle peut utiliser la cyber-guerre pour paralyser sa capacité à lancer ces armes. La nation avec une technologie cybernétique suffisamment supérieure pourrait geler l'infrastructure de son adversaire et immobiliser sa capacité à aller en guerre.

Il y a quelques décennies, l'Allemagne était la plus grande menace pour la paix mondiale. Aujourd'hui, il commence à développer une technologie puissante qui pourrait constituer une menace majeure, mais le monde ne se préoccupe pas.

L'économie américaine et les militaires dépendent fortement des types de systèmes d'information qui peuvent être exploités par des cyber-attaques. On pourrait penser que l'Amérique ferait de son mieux pour rester en tête dans la course afin que personne ne puisse exploiter sa faiblesse. Mais en réalité, les États-Unis exhortent en fait l'armée allemande à rattraper son retard. Washington a encouragé l'Allemagne à doubler son budget militaire et a amélioré les armes nucléaires qu'ils ont stationnées en Allemagne.

Le monde serait choqué de voir l'Allemagne entrer soudainement dans la course aux armements nucléaires, mais elle vient de progresser dans une autre course menaçante, dont le vainqueur pourrait prendre le contrôle de son adversaire sans lancer un seul missile ou laisser tomber une seule bombe.

Aucun va au combat

À quoi ressemblerait une guerre lorsqu'une nation comme les États-Unis se trouve sous l'attaque et appelle ses militaires à aller à la guerre—mais pas un navire, un avion ou un char d'assaut fait un mouvement?

La Bible décrit exactement ce scénario. Le rédacteur en chef de la *Trompette*, Gerald Flurry, a souligné cette description en 2005: « Je crois qu'une *prophétie biblique clé du temps de la fin* pourrait être remplie par ... le cyber-terrorisme ...: « On sonne de la trompette, tout est prêt, mais personne ne marche au combat ; car ma fureur éclate contre toute leur multitude.

(Ezéchiel 7:14). La trompette de la guerre doit être sonnée en Israël—principalement l'Amérique et la Grande-Bretagne. ... Il semble que tout le monde s'attend à ce que nos gens viennent au combat, mais la plus grande tragédie possible se produit ! Personne ne va au combat—même si la trompette est sonnée ! Serait-ce à cause du terrorisme informatique ? « (*La Trompette*, mai 2005).

La technologie a finalement rattrapé une prophétie enregistrée il y a plus de 2000 ans.

Les menaces sont réelles, et n'importe qui peut les reconnaître. Mais, apparemment ayant largement oublié ce qui s'est passé dans deux guerres mondiales, le monde semble indifférent à propos des avancées allemandes dans la cyber-guerre. Ceci est certain pour s'avérer une erreur de calcul critique. À mesure que la technologie nous amène à un avenir incertain de nouvelles dimensions dans la façon de faire la guerre, l'Allemagne se positionne à l'avant-garde. ▪