GUILLAUME POUPARD (92) *directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)*

LA GUERRE NUMÉRIQUE N'AURA PAS LIEU

Les capacités destructives des armes informatiques sont considérables, mais la complexité de l'environnement dans lequel elles interviennent conduit à repenser les modèles permettant d'assurer la cybersécurité des pays. Le choix fait par la France en la matière devrait s'imposer dans la plupart des États membres de l'Union européenne.

« Les mots ne sont pas assez nombreux pour courir aussi vite que la guerre » écrit Le Clézio [1]. Il est effectivement prudent d'utiliser le mot « guerre » avec parcimonie. Et plus encore lorsqu'il est question de l'appliquer au numérique. Malgré tout, depuis quelques années, le terme fait florès et prétend caractériser l'opposition entre nations manifestée dans le cyberespace. Des États comme des entreprises développent et vendent des armes informatiques, des armées sont créées, des experts se réunissent à l'Otan ou à l'ONU pour évoquer les conditions qui devraient permettre un déroulement ordonné, conforme aux principes du droit international d'une guerre numérique que chacun juge inéluctable ou plutôt déjà en cours.

« En 2016, les attaques informatiques auraient coûté 450 milliards de dollars aux entreprises »

Mais pas de sang versé ou de mort sur le champ de bataille numérique. Pas de populations qui fuient les zones de combat cybernétique. Pas de ruines parmi les nuages, les applications ou les sites internet.

DES EFFETS DÉVASTATEURS

C'est que la guerre numérique n'existe pas. Seuls existent les effets produits par les attaques informatiques dans le monde matériel. Et ils peuvent être dévastateurs. Détruire des vies humaines, par exemple par une attaque contre une infrastructure critique de production d'énergie, de distribution d'eau, de transport ou de télécommunication ou encore contre des usines pouvant émettre des produits toxiques. Au début de l'été dernier, deux vagues d'attaques successives ont eu le même effet, bien que poursuivant des objectifs différents. En chiffrant les informations stockées dans les réseaux des entreprises compromises, c'est la survie économique de ces entreprises qui a été mise en jeu. Une étude judicieusement intitulée « business blackout » publiée par le Lloyd's mi-juillet analyse le risque que font porter les attaques informatiques sur l'économie. Selon les scénarios étudiés, les dommages attribués à une attaque informatique d'envergure évoluent dans une fourchette allant de 15 à 120 milliards de dollars ! En 2016, les attaques informatiques auraient coûté 450 milliards de dollars aux entreprises…

© COREPICS / FOTOLIA.COM

Les attaques de l'été dernier ont été rendues possibles par la dissémination de vulnérabilités informatiques volées – par une attaque informatique – à la NSA américaine.

LES X ET LA CYBERSÉCURITÉ

Ainsi, les armes informatiques peuvent se révéler de « destruction économique massive », et l'agresseur – État, terroriste, criminel – est potentiellement en mesure de porter atteinte à nos intérêts fondamentaux par les conséquences économiques et sociétales d'une attaque. Si la guerre numérique n'existe pas, la situation de guerre est, elle, bien réelle et permanente. Ce n'est sans doute pas un hasard si, dans ce contexte et face à ces enjeux, tant de polytechniciens contribuent à la cybersécurité de la France.

D'abord parce que notre formation nous permet d'appréhender la complexité de l'environnement et de prendre en compte l'ensemble des facteurs pertinents pour la prise de décision. C'est ainsi que nous avons grandement participé à la conception, à l'instruction de la décision politique puis à la mise en place du modèle français de cybersécurité, décidé il y a moins de dix ans au travers du Livre blanc sur la défense et la sécurité nationale. Le modèle retenu qui, j'en suis persuadé, s'imposera aux États membres de l'Union européenne, est le seul capable de concilier stabilité et développement économique durable par la séparation entre missions de défense et de sécurité confiées à l'agence nationale de la sécurité des systèmes d'information (ANSSI) et des capacités d'attaque confiées au ministère des Armées.

RISQUE DE DISSÉMINATION DES VULNÉRABILITÉS

Les pays qui ont choisi un modèle regroupant capacités opérationnelles de défense et d'attaque donnent priorité

Dans le modèle français de cybersécurité, les missions de défense et de sécurité sont confiées à l'agence nationale de la sécurité des systèmes d'information (ANSSI).

à cette dernière et participent même, parfois malgré eux, à la diffusion de vulnérabilités informatiques susceptibles de détruire une large part du progrès économique porté par le numérique. C'est ce qu'ont montré les attaques de l'été dernier, notamment rendues possibles par la dissémination de vulnérabilités informatiques volées – par une attaque informatique – à la NSA américaine.

« Il est indispensable de maîtriser des aspects techniques issus de domaines scientifiques multiples »

L'USAGE DÉLICAT DE LA LÉGITIME DÉFENSE

En matière de sécurité du numérique, il est indispensable de maîtriser des aspects techniques issus de domaines scientifiques multiples pour éviter de reproduire des raisonnements tirés du monde matériel mais inapplicables dans ce contexte, comme il est également nécessaire d'inclure les facteurs politiques, humains ou les relations entre États pour concevoir et mettre en place les stratégies qui permettront à la France de tenir son rang parmi les nations, de résister à des attaques informatiques majeures comme de participer à la stabilité du cyberespace. À titre d'exemple, c'est bien la connaissance technique des modes d'attaques utilisés et de la difficulté d'attribuer une attaque informatique qui permet d'expliquer aux spécialistes du droit international comme aux décideurs politiques qu'il n'est pas souhaitable de laisser se mettre en place sans précaution particulière un mécanisme de légitime défense en cas d'attaque informatique quand bien même le droit international le prévoit dans le monde matériel.

CONSTRUIRE LA PAIX

Enfin, comme l'a affirmé le Président de la République le 13 juillet dernier, « Le rôle de la France, c'est de partout construire la paix. Mais nous ne pouvons construire la paix dans le monde d'aujourd'hui que si nous sommes crédibles, autonomes dans nos stratégies. » En matière de sécurité du numérique et pour construire cette crédibilité, des polytechniciens participent à la conception d'armes informatiques au ministère des Armées pour protéger nos intérêts pendant que d'autres, notamment à l'ANSSI, travaillent à construire la défense et la sécurité de notre espace numérique national.

C'est de cette compétence, de cet engagement et de la cohérence globale de cette approche que dépendra dans un futur proche une part importante de notre souveraineté nationale. ■

1. In *La Guerre*, Gallimard, 1970.