08 février 2023 l Jean-Marie Dhainaut, traduction de l'article publié le 25.01.2023 au Tagesspiegel et signé par Dr. Reinhard Brandl, membre du Bundestag allemand (CSU).

Point de vue

Réaliser le changement d'époque dans la cyberdéfense

Par Reinhard Brandl, membre du Bundestag allemand (CSU)

La guerre d'agression russe a clairement montré le danger que représentent les cyberarmes. C'est pourquoi l'Allemagne a un besoin urgent de réorienter la cyberdéfense, commente Reinhard Brandl (CSU). Dix propositions pour renforcer la sécurité de la République Fédérale et augmenter ses options d'action.

L'Allemagne a un besoin urgent de réorienter la cyberdéfense. La guerre d'agression russe contre l'Ukraine a clairement montré que la Russie ne se contente pas de lutter au moyen de bombes, de chars et de drones, mais qu'elle utilise également des cyberarmes. L'attaque présumée russe contre l'opérateur satellite Viasat, dont l'armée ukrainienne utilise également les services, eut comme dommage collatéral qu'environ 3.000 éoliennes en Allemagne furent temporairement incontrôlables. Nous devons reconnaître que les menaces internationales qui pèsent sur l'Allemagne dans le cyberespace croissent fortement. Les mesures purement préventives et l'attribution actuelle des compétences ne suffiront plus.

Dans le cyberespace aussi, nous devons changer d’époque. Pour moi, cela implique que l'Allemagne prenne des responsabilités dans le cyberespace et qu'elle soit en mesure, par exemple, de parer à des cyberattaques en cours depuis l'étranger et de les élucider. Pour ce faire, nous devons créer à la fois les bases juridiques d'une cyberdéfense active et forte en Allemagne et les capacités humaines et techniques nécessaires à cette fin.

Les options d'action au niveau fédéral ne suffisent pas

Actuellement, la cybersécurité au niveau fédéral relève principalement du Ministère fédéral de l'Intérieur et des territoires (BMI) et de l'Office fédéral pour la sécurité dans les technologies de l'information (BSI) qui lui est subordonné. Le BSI est chargé de renforcer la sécurité informatique au niveau fédéral et de protéger les réseaux gouvernementaux. La panoplie d'outils va des avertissements jusqu’aux activités de conseil aux administrations en passant par la définition et le contrôle de normes imposées comme minimum aux outils informatiques fédéraux.

Cependant, le BSI ne peut aider les « Länder » à lutter contre les cybermenaces, par exemple en déployant ses « Mobile Incident Response Teams » (MIRT), que si ceux-ci en font la demande. En effet, conformément à l'article 30 de la Constitution, la sûreté relève par principe de la compétence des Länder, à quelques exceptions près. En bref : Lors d'une cyberattaque à grande échelle contre l'Allemagne, le pouvoir fédéral n'est actuellement que spectateur.

10 propositions pour réorienter la cyberdéfense

Voici dix propositions que je présente pour réorienter la cyberdéfense.

Premièrement, garantir la cybersécurité doit être une tâche de l'État dans son ensemble. Pour ce faire, le pouvoir fédéral a besoin d'une compétence pour la défense contre les cyberattaques, en particulier en cas de cyberattaques graves. Le pouvoir fédéral devrait pouvoir activement assigner celles-ci et y faire mettre fin.

Deuxièmement, les décideurs au niveau fédéral et au niveau des Länder ont besoin d'avoir accès à une image constamment tenue à jour de la situation dans le cyberspace, couvrant tous les niveaux de l'État ainsi que les principales infrastructures critiques.

Troisièmement, le pouvoir fédéral devrait tenir en réserve active des capacités cybernétiques pour interrompre, y compris sur des réseaux étrangers, les attaques en cours et pour effectuer des analyses criminologiques qui aider à attribuer l'attaque et à identifier d'autres victimes.

Quatrièmement, les capacités civiles et militaires en matière de cyberdéfense devraient mieux interagir. Afin de renforcer les MIRT, il faut affecter des soldats au BSI. En temps de paix, ceux-ci doivent pouvoir acquérir de l'expérience pratique dans un environnement civil sous la direction du

BSI. En cas de guerre, ils retourneraient dans les structures de l'armée fédérale avec les compétences acquises.

Cinquièmement, il conviendrait de désigner un CISO BUND (Chief Information Security Officer au niveau fédéral). Cela confère à la question de la cybersécurité l'importance politique appropriée.

Sixièmement, dans le domaine de la cyberdéfense, il faut mieux entrainer aux interactions de tous les niveaux de la fédération. Pour cela, je propose des exercices cyber réguliers et communs au niveau fédéral, au niveau des Länder et au niveau communal.

Septièmement, nous devons mettre au point des stratégies efficaces pour attirer un personnel d'excellence dans le domaine du cyberespace. Cela implique notamment de modifier la convention collective de la fonction publique afin d'améliorer les rémunérations des cyber-professionnels et de limiter l'interdiction d'avantages relatifs (*NdT : règle allemande liant les organisations auxquelles sont octroyés des fonds publics*). En outre, nous devons continuer à développer la formation de spécialistes de la cyberdéfense dans les universités fédérales.

Huitièmement, le gouvernement fédéral devrait prévoir d'importantes dérogations au droit fédéral des marchés publics dans le domaine de l'équipement matériel pour les autorités de cybersécurité. Dans ce domaine précis, il est important d'être rapide et, dans certains cas, de restreindre d'un point de vue national le cercle des fournisseurs. Le pouvoir fédéral devrait se donner l'objectif de renforcer l'écosystème national des solutions de sécurité informatique.

Neuvièmement, les autorités fédérales devraient, à l'avenir, appliquer obligatoirement le principe de confiance zéro, au moins pour les nouveaux systèmes informatiques.

Dixièmement, le gouvernement fédéral devrait encourager activement la généralisation d'approches de Security-by-design et de Security-by-default.

Conclusion

Dans le contexte actuel de danger, l'Allemagne peut chaque jour être l'objet d'une cyberattaque majeure. C'est pourquoi nous devons nous y préparer dès à présent et non pas réagir lorsqu'il sera trop tard. Cela nécessite notamment de reconnaître qu'il faut adapter l'organisation de notre cyberdéfense aux défis actuels. Dans ce contexte, la séparation traditionnellement et institutionnellement stricte en Allemagne de la sécurité extérieure du cyberespace par rapport à sa sécurité intérieure semble obsolète.

Reinhard Brandl (CSU) est le porte-parole du groupe CDU/CSU du Bundestag pour la politique numérique.