laTrompette

KENZO TRIBOUILLARD/POOL/AFP VIA GETTY IMAGES

L'UE cherche à créer une unité cybernétique commune

Le monde se prépare à la cyberguerre. La question est : qui frappera en premier ?

- Josue Michels
- 27/12/2021

La Commission européenne a adopté, le 23 juin, un plan visant à créer une nouvelle unité cybernétique conjointe.

Dans notre monde moderne, la cybersécurité est essentielle à la prospérité d'une nation. Mais elle jouera également un rôle crucial dans la guerre. Actuellement, chaque État membre de l'Union européenne utilise ses propres ressources pour repousser les attaques. À l'avenir, l'UE espère assumer cette responsabilité. De telles avancées doivent être surveillées de près : la cyberdéfense est la première étape d'une offensive réussie.

L'UE affirme que ses récents efforts pour former une cyber unité sont en réponse à la menace croissante à laquelle le continent est confronté. Un exemple récent montre l'urgence de la question.

En juillet, l'Allemagne a fait face à sa première urgence de cyber catastrophe. Les systèmes informatiques du district allemand d'Anhalt-Bitterfeld en Saxe-Anhalt ont été piratés le 6 juillet. « Nous sommes pratiquement complètement paralysés », a rapporté un porte-parole de l'administration du district le 10 juillet. La capacité du district à verser des prestations sociales et d'autres tâches continue d'être entravée. Le quartier compte environ 157,000 habitants. On estime qu'il faudra deux semaines avant que les systèmes fonctionnent à nouveau.

Euroactiv a noté :

> Le nombre et la férocité des cyberattaques ont grimpé en flèche au cours de la dernière année, l'exemple le plus récent étant l'attaque à grande échelle en Belgique, qui a touché plus de 200 organisations.
>
> Le nombre d'attaques malveillantes importantes contre des secteurs critiques a plus que doublé en 2020, passant de 146 incidents en 2019 à 304 en 2020. Plus dramatique encore est l'augmentation du nombre d'attaques d'hameçonnage, dont la fréquence a augmenté de 667 pour cent au cours des premiers mois de la pandémie, a déclaré à *Euroactiv* un porte-parole de l'AESRI (l'Agence européenne chargée de la sécurité des réseaux et de l'information).

Le rapport de recommandation de l'unité cybernétique commune du 23 juin se lit comme suit : « La cybersécurité est essentielle au succès de la transformation numérique de l'économie et de la société. L'UE s'est engagée à investir à des niveaux sans précédent pour garantir que les citoyens, les entreprises et les autorités publiques aient confiance dans les outils numériques. »

Alors que les tâches gouvernementales et administratives continuent de se numériser, la cybersécurité devient un élément essentiel de chaque opération. Pour cette raison, le haut représentant de l'UE, Josep Borrell, a déclaré : « L'unité cybernétique commune est une étape très importante pour que l'Europe protège ses gouvernements, ses citoyens et ses entreprises des cybermenaces mondiales. Lorsqu'il s'agit de cyberattaques, nous sommes tous vulnérables et c'est pourquoi la coopération à tous les niveaux est cruciale. »

Un manque de cybersécurité risque de présenter de nombreuses vulnérabilités. Cela peut coûter de grosses sommes d'argent et entraîner des retards inutiles. Dans le pire des cas, un manque de sécurité dans le monde numérique peut coûter des vies.

Il n'est donc pas surprenant que l'UE recherche également davantage de coopération au sein de la communauté de la défense pour « renforcer les capacités de cyberdéfense et améliorer davantage les synergies, la coordination et la coopération ». La nouvelle unité cybernétique commune « devrait être construite pour permettre le partage d'informations avec la communauté de la cyberdéfense ».

Certaines équipes de cyber-réponse existent déjà parmi les États membres de l'UE. La nouvelle unité est principalement destinée à coordonner la coopération entre les cybers agences et les autorités.

Dans les milieux militaires des nations, la cyber-coopération a déjà commencé à travers la formation du cadre juridique introduit par le traité de Lisbonne. Différents projets de la coopération structurée permanente (CSP) permettent le partage d'informations, la formation et le support opérationnel. « Les représentants des projets CSP pertinents devraient soutenir l'unité cybernétique commune, notamment en ce qui concerne la connaissance de la situation et la préparation », indique la recommandation.

Mais le plan fait face aux obstacles habituels. *Politico* a noté : « La Commission a promis pour la première fois de créer une unité cybernétique conjointe en 2019 pour arrêter les cyberattaques qui ont compromis les institutions, les agences, les ministères et départements nationaux de l'UE, ainsi que les principales entreprises et organisations européennes. Mais le plan a mis plusieurs mois à être finalisé car l'UE n'a pas de compétence en matière de sécurité nationale et les pays de l'UE ont hésité à céder le contrôle. »

L'histoire prouve qu'il faut souvent une crise majeure pour que l'Europe s'unisse. Les récentes menaces ont propulsé le plan en avant.

Afin de se prémunir contre les cybermenaces, il faut développer des capacités de cyber offensives. Plutôt que de gérer les conséquences d'une attaque, les cyber-compétences offensives empêchent les attaques de se produire.

Jusqu'à présent, nous n'avons pas vu de cyberguerre totale. Mais certains des mêmes principes que nous connaissons de la guerre conventionnelle s'appliquent. L'un de ces principes est que les agresseurs doivent toujours craindre des représailles. Certains peuvent actuellement regarder l'UE et penser que l'Europe se prépare simplement à riposter. En effet, on est amené à le croire. Mais l'histoire prouve le contraire.

Il y a de nombreuses années, le rédacteur en chef de la *Trompette*, Gerald Flurry, a averti que l'UE se transformait en un empire dirigé par l'Allemagne qui frapperait en premier. Plus précisément, il a averti que la cyberguerre serait une caractéristique dominante de la guerre à venir de l'Europe. Une prophétie dans Ézéchiel a informé les prévisions de M. Flurry : « On sonne de la trompette, tout est prêt, mais personne ne marche au combat ; car ma fureur éclate contre toute leur multitude. (Ézéchiel 7 : 14).

« Il semble que tout le monde s'attend à ce que notre peuple parte au combat », a écrit M. Flurry en mai 2005, « mais la plus grande tragédie imaginable se produit ! Personne ne va au combat—même si la trompette est sonnée ! Est-ce à cause du terrorisme informatique ? » Au cours des derniers mois, la cyber-vulnérabilité américaine a été exposée. La Bible révèle qu'une nation de confiance ciblera cette vulnérabilité lors d'une attaque surprise.

Dans : « *Les cyberattaques révèlent la fragilité de notre monde* », Richard Palmer, rédacteur adjoint de *latrompette.fr* a écrit :

> Les cyberattaques réussies de ces derniers mois ne sont qu'un avant-goût de ce qui nous attend certainement à l'avenir. Une cyberguerre totale pourrait paralyser les États-Unis, ou tout autre grand pays.
>
> Imaginez les retombées potentielles. L'électricité est coupée. La production alimentaire s'arrête. Les stations-service sont vides. Les supermarchés aussi. Pratiquement du jour au lendemain, cela mettrait la nation à genoux.
>
> Un tel niveau d'attaque contre les États-Unis semble impensable. Mais aucune puissance ou empire dans l'histoire du monde n'a été à l'abri d'une attaque. Pourquoi l'Amérique devrait-elle être différente ?

Le monde se prépare à la cyberguerre. La question est : qui frappera en premier ? La Bible révèle la réponse claire pour ceux qui veulent écouter. Pour plus d'informations sur la faiblesse de l'Amérique et les avancées de l'Allemagne dans la cyberguerre, lisez l'article de Gerald Flurry « *Le talon d'Achille de l'Amérique—et l'Allemagne* » et demandez un exemplaire gratuit de son livre *Ezekiel—The End-Time Prophet* (disponible en anglais seulement).