Özge Gencer

COMİTÉ: Conseil des secrétaires d'État des ministres de la Défense et des Armées

SUJET: Comment l'UE peut-elle assurer un usage éthique du numérique?

PAYS: Danemark

Brève présentation du Danemark - situé au nord de l'Allemagne, au sud de la Norvège. Le Royaume du Danemark est constitutionnellement un État unitaire comprenant le Danemark et deux territoires autonomes dans l'océan Atlantique Nord, les îles Féroé et le Groenland. En 2022, le Danemark couvre une superficie totale de 42 951 kilomètres carrés, avec une population de 5 873 420 habitants. Le Danemark est une monarchie constitutionnelle, dotée d'un système parlementaire représentatif et d'un chef de gouvernement. Depuis le 14 janvier 1972, la reine de Danemark est Margrethe II de Danemark. Le PIB danois en 2022 était de 399 100 milliard dollars et le PIB par habitant de 69 273,996 dollars. Le taux de chômage est de 5,1%. Le Danemark est un pays de l'Union européenne et, comme d'autres États membres, il éprouve des difficultés à lutter contre les cyber-attaques.

En tant que délégation danoise, nous pensons qu'il faut trouver rapidement des solutions pour lutter contre les cyberattaques. Les attaques contre le Danemark et d'autres États membres de l'Union européenne ont déjà fortement augmenté depuis la pandémie de 2019. Selon l'ENISA (L'Agence européenne pour la cybersécurité), plus de 10 téraoctets d'informations ont été volés chaque mois depuis la pandémie et il y a eu plus de 600 attaques graves au cours de l'année. Par conséquent, la situation vécue par l'Union européenne, dont le Danemark est membre, est urgente et doit être résolue le plus rapidement possible.

Tout d'abord, depuis 2014 la Commission a adopté des règlements visant à protéger les données personnelles et à garantir la circulation de l'information. Ces règlements sont les suivants : Règlement sur la libre circulation des données à caractère non-personnel, Règlement de l'UE sur la cybersécurité, Directive de l'UE sur les données ouvertes, Règlement général sur la protection des données, Plan coordonné avec les États membres dans le domaine de l'intelligence artificielle, Lignes directrices en matière d'éthique pour une intelligence artificielle de confiance et Le combat contre les cybermenaces. Bien que de grands progrès aient été réalisés grâce aux règlements élaborés, il reste encore une grande lacune dans la lutte contre les cybermenaces.

En outre, la raison principale de cette insuffisance est l'augmentation de la numérisation après la pandémie de 2019 et la crise entre la Russie et l'Ukraine. Les données personnelles et les données collectées numériquement et mises à disposition par les États et les entités juridiques sont devenues les principales cibles des cyberattaques. L'Union européenne dispose d'une équipe d'experts CERT (Computer Emergency Response Team) pour intervenir lorsqu'une attaque est détectée. En raison de l'augmentation soudaine des attaques, les experts ont annoncé qu'ils avaient besoin de personnel et de soutien financier. Bien que 61 % des entreprises de l'UE aient déjà adopté des technologies numériques avancées, environ 26 % des entreprises n'ont pas investi dans la transition numérique à tous les niveaux dans la pandémie de corona.

De plus, la crise entre la Russie et l'Ukraine n'étant pas encore terminée, des experts ont annoncé qu'ils s'attendaient à d'autres cyberattaques dans un avenir proche et qu'ils demandaient de l'aide. Outre le personnel et le soutien financier à l'ENISA et au CERT, qui sont les principales institutions responsables du développement de la cybersécurité, des programmes de supervision technique et de prévention des cyberattaques devraient être élaborés par des personnes compétentes, des mesures juridiques devraient être prises et la coopération internationale devrait être assurée de toute urgence.

Pour résumer, l'Union européenne doit avant tout agir le plus rapidement possible pour protéger ses États membres. Afin d'éviter que les cyber-attaques ne causent davantage de dommages aux États, outre les mesures juridiques, elle devrait imposer des sanctions sévères à la personne ou à l'organisation responsable de l'attaque, consulter des experts formés à la cybersécurité et, surtout, assurer une coopération internationale. C'est pourquoi la délégation danoise est tout à fait disposée à travailler avec les États membres pour y parvenir.