En mai dernier, la nouvelle stratégie de cybersécurité pour la Belgique a été validée par le Conseil national de Sécurité.

« La cybersécurité est devenue un enjeu géopolitique pour la Belgique comme pour tous les pays du monde. Que savons-nous sur ces nouveaux conflits ? »

Les conflits internationaux ont énormément évolué durant ce siècle. Non seulement, les acteurs se sont multipliés et diversifiés mais les formes que peuvent prendre ces conflits sont également inédites. Il y a encore quelques années, les guerres et les conflits internationaux opposaient des États dans les espaces maritime, aérien, terrestre ou sidéral. Aujourd'hui, un nouvel espace d'affrontement est apparu : le cyberespace.

Le cyberespace et ses particularités

Le cyberespace se compose d'un ensemble d'appareils connectés et interconnectés via l'Internet. Il comprend donc également un immense flux de données ainsi qu'un réseau d'humains aptes à le maintenir en fonction, à le faire évoluer et à l'utiliser[1].

Ce nouvel espace a des propriétés bien particulières. Pour commencer, il permet aux menaces de se propager à une vitesse et à une échelle sans précédent. Ensuite, il rend compliquée l'attribution avec certitude des actes à des personnes. De plus, dû à sa particularité matérielle, cet espace est traversé par plusieurs juridictions nationales et les normes internationales qui s'y rapportent sont, quant à elles, encore rares. Cela est notamment dû aux innovations technologiques et à la reconfiguration des réseaux qui produisent une évolution constante du secteur. Enfin, le faible coût et l'accessibilité de ces technologies offrent un rôle prépondérant aux acteurs privés au sein du cyberespace.

Néanmoins, les conséquences et les victimes d'attaques dans cet espace n'en sont pas moins réelles. Les cyberattaques s'en prennent à différentes cibles : des gouvernements, des villes, hôpitaux, des entreprises, ou même des citoyen·ne·s. Ce qui se déroule dans le cyberespace a donc des répercussions bien réelles sur la diplomatie internationale, la géopolitique des conflits, ainsi que notre quotidien.

La cybersécurité, la cyberdéfense et la souveraineté des États

Dans les années 2000, les États posent dans leurs discours, l'idée que le cyberespace est un territoire, comme la terre, la mer, l'air ou l'espace, à conquérir et à contrôler. Les États cherchent alors à imposer leur présence dans le cyberespace afin de préserver leur souveraineté. La grande dépendance de la société au monde numérique, la rend d'autant plus vulnérable aux cyberattaques et l'impact de ces attaques d'autant plus conséquent.

La sécurité nationale et la défense du territoire sont ébranlées par la menace des cyberattaques. La capacité de saboter des infrastructures dites vitales est une des premières menaces ressenties par les États. L'enjeu autour des communications est également extrêmement important, à travers la perturbation des canaux de communication ou encore la manipulation des informations. Sans compter, la menace d'une guerre idéologique sur les réseaux sociaux permettant d'influencer l'opinion publique et ce, anonymement. On pense notamment au scandale Cambridge-Analytica (voir encadré) qui vient questionner le rôle des GAFA dans la politique des Etats.

Le scandale Cambridge Analytica renvoie à la façon dont Facebook utilise les données personnelles de ses utilisateurs et utilisatrices. Cambridge-Analytica est une société qui exploite les données personnelles dans l'optique d'influencer sur les intentions de vote.

L'avènement du cyberespace n'a donc pas été l'avènement d'un territoire neutre exempt de frontières comme certains ont voulu le croire. Les révélations d'Edward Snowden, l'opération Stuxnet, l'affaire SolarWinds (voir encadrés) ou plus récemment l'intensification des cyberattaques à l'encontre des États-Unis à la suite de l'élection de Joe Biden, font monter la tension entre les grandes puissances (États-Unis, la Russie et la Chine principalement). Ce sont autant d'exemples qui viennent confirmer que le cyberespace est devenu le nouveau terrain des stratégies de domination entre puissances.

L'opération Stuxnet, en 2010, est souvent considérée comme le premier acte de cyberguerre, cela sous-entend qu'il s'agit d'un acte de guerre, ainsi le pays victime se confère le droit de répliquer par quelque forme que ce soit. De nombreux États annonçaient le développement de leurs capacités offensives. Stuxnet est le nom d'un virus informatique développé par la NSA (agence de sécurité américaine) avec l'appui d'Israël, qui avait pour but de s'attaquer aux infrastructures nucléaires de l'Iran.

L'affaire SolarWinds, en 2020, est reprise comme l'attaque de cyberespionnage la plus importante de cette décennie. Un logiciel espion a réussi à infiltrer les centres de pouvoir américains et par effet de ricochet, de nombreuses autres entreprises et administrations aussi bien en Europe qu'en Asie. Sans être ouvertement revendiqués, des affrontements sous forme de cyberattaques sont aujourd'hui encore en cours entre les États-Unis et la Russie à la suite de l'affaire Solarwinds[2].

La stratégie de cybersécurité de l'Union Européenne, adoptée en 2020, a pour objectif de renforcer la coordination et la coopération avec les capacités de la cyberdéfense[3]. Les membres de l'Union européenne ont décidé de collaborer étroitement concernant la cyberdéfense et la cybersécurité afin d'augmenter leur réactivité et leur capacité d'actualisation en la matière.

La cybersécurité et la cyberdéfense sont donc actuellement des enjeux de taille pour les États. Si la différence entre les termes cybersécurité et cyberdéfense peut sembler encore floue, leur utilisation tend à varier selon le contexte. Il semble néanmoins que la sécurité est un état recherché tandis que la défense est une posture. En Belgique, le département de la Défense comprend une division « cybersécurité » qui travaille à prévenir et empêcher de potentielles cyberattaques.

La cyberdiplomatie et le Cloud Act

Face à ces nouvelles menaces, les États développent des stratégies afin d'assurer leur cybersécurité et celle de leurs citoyen·ne·s. Au centre de la problématique se trouve la manipulation et le vol des données qui transitent dans nos outils numériques.

En 2018, les États-Unis ont mis en place le Cloud Act – « Claryifing Lawful Overseas Use of Data Act », une loi fédérale ayant pour but de réglementer l'utilisation et l'accès aux données et preuves électroniques[4]. Cette loi permet au gouvernement américain d'accéder aux données stockées sur les serveurs et ce, même à l'étranger, sans obligation d'avertissement au pays ou à la personne concernée. Critiquée pour son extraterritorialité, cette loi américaine trouve son pendant européen avec le projet de règlement e-evidence. L'Union européenne a également créé une Agence de l'UE pour la cybersécurité, répondant à l'acronyme ENISA, faisant écho au CISA américain – « Cybersecurity and Infrastructure Security Agency ». Comme on peut le remarquer, les réglementations qui régulent l'accès aux données au sein du cyberespace sont encore très récentes et s'inspirent mutuellement sans qu'il y ait pour autant une norme internationale permettant d'éviter des conflits liés au sentiment d'ingérence.

Depuis 2020, la stratégie de cybersécurité de l'Union européenne tient en trois prérogatives : renforcer sa capacité à se protéger contre les menaces informatiques, mettre en place un environnement sécurisé grâce au chiffrement quantique et garantir l'accès aux données à des fins judiciaires et répressives[5].

Et la cybersécurité en Belgique ?

Avec sa nouvelle stratégie 2.0, la Belgique va au-delà des prérogatives de l'Union européenne et développe sa stratégie en six objectifs : renforcer l'environnement numérique et accroître la confiance des utilisateur·trice·s en ce dernier ; armer ceux/celles-ci et les personnes responsables de l'-administration des réseaux ; protéger les organisations d'intérêt vital contre toutes les cybermenaces ; répondre à la cybermenace ; améliorer les collaborations publiques, privées et universitaires ; tenir un engagement international clair. Il est intéressant de noter que la résilience numérique n'est, dans cette stratégie, pas du tout synonyme de sobriété numérique.

Les différents acteurs impliqués dans cette nouvelle stratégie sont nombreux et multiples : Police fédérale, Ministère public, Sureté de l'État, la Défense, Institut Belge des services postaux et de communication, Service public fédéral économie …[6] En effet, la collaboration entre les services est primordiale dans l'établissement d'une cybersécurité efficace et c'est

également dans cette optique qu'a été créé le centre belge de la cybersécurité. Ce centre a pour objectif de faciliter la collaboration entre les différents services publics et privés concernés (la Défense, la police fédérale, les renseignements mais également les sociétés fournisseurs d'accès internet).

Aujourd'hui, l'État Belge identifie quatre groupes d'acteurs de la menace : l'hacktivisme[7], le terrorisme, la cybercriminalité et, les services militaires étrangers[8]. Récemment, la Belgique a fait face à une attaque de grande ampleur touchant le fournisseur d'accès national belge « Belnet » révélant la vulnérabilité de nos infrastructures et des deux cents administrations qui y sont liées. Si différentes hypothèses sont émises concernant l'objectif de cette attaque, aucune certitude n'est encore donnée quant à l'identité de l'auteur de l'attaque. La conclusion, suite à cette cyberattaque, a été de promouvoir une augmentation des investissements de l'Etat dans la cybersécurité.

Une régulation nécessaire du cyberespace

Devant le constat de la perpétuelle accélération de notre société due à la transformation numérique, le rôle de l'État dans la régulation de cette accélération et de ses conséquences semble essentiel. Les investissements de l'État dans la lutte contre les cyberattaques sont de plus en plus grands, c'est pourquoi, la population se doit d'être informée de ces nouveaux enjeux.

Plusieurs questions se posent : entre sécurité et vulnérabilité, comment éviter la surveillance de tous et toutes, partout et tout le temps, à travers les objets connectés qui se multiplient dans notre quotidien (montre, télévision, téléphone, tablette, …) ? Entre ingérence politique et influence des citoyens, les réseaux sociaux sont-ils des plateformes dédiées à la liberté d'expression des citoyens du monde ou des instruments de pouvoir et d'influence aux mains des GAFAM ? Entre écologie et dépendance, serons-nous prêts à changer nos standards de vie et opter pour la sobriété ?

Nous pouvons désormais nous questionner sur la stratégie employée. L'objectif de ces investissements est d'atteindre une résilience permettant d'être moins vulnérables aux cyberattaques, toujours plus nombreuses, plus complexes et plus dangereuses. Est-ce la meilleure stratégie d'investir dans toujours plus de technologies pour pourvoir à l'accélération perpétuelle de ce système ou serait-il plus intéressant de considérer les alternatives à ce numérique qui nous rend vulnérables ?

Pourrait-on imaginer, en parallèle à la cybersécurité, qu'une des missions de l'État serait de réduire notre dépendance à cette technologie plutôt que de prôner un « tout au

numérique » ? Prôner cette sobriété numérique semble pouvoir être un bon appui qui facilitera le travail des agents de la cybersécurité et qui serait plus durable à terme, concernant l'écologie.

Au-delà de cette recherche de sobriété numérique, il semble évident qu'une régulation internationale est nécessaire et attendue afin de diminuer les risques de conflits internationaux liés au sentiment d'ingérence et à l'escalade des soupçons.

Mila Gati.

---

[1] Douzet Frédéric, « La géopolitique pour comprendre le cyberespace », Hérodote, 2014, n°152-153.

[2] France Inter, émission de radio, « Le monde d'après », 3 juin 2021.

[3] FEB, Fédération des Entreprises de Belgique

[4] Brincourt Laura, « Le Cloud Act, trois ans après : révélateur du besoin de définition de notre souveraineté dans l'espace numérique, Diploweb, 16 mai 2021.

[5] Centre pour la cybersécurité en Belgique, « Stratégie de cybersécurité – Belgique 2.0 – 2021-2025 », mai 2021.

[6] Idem.

[7] L'hacktivisme est un ensemble d'actions délibérées dont l'objectif est de promouvoir un programme politique ou idéologique.

[8] Idem.