TEXTE

Depuis les années 80 et l'arrivée des ordinateurs dans les ménages et les bureaux, la numérisation de la société l'a fait beaucoup évoluer. Ces dernières années, une grosse augmentation de la cybercriminalité a eu lieu, ceci causant des problèmes de sécurité nationale. La première attaque cybercriminelle date de 1982, lorsque les services secrets américains avaient effectué une série d'attaques sur des gazoducs canadiens. Aujourd'hui, cette cybercriminalité touche donc tous les secteurs: des particuliers (vols de mots de passes) jusqu'aux démocraties, mises à mal par des groupes de hackers. La question se pose donc: Quel rôle joue la cybersécurité au vue de la démocratie et quels dommages collatéraux s'en découlent ?

I. La cybercriminalité, une menace pour les démocraties

Nos démocraties sont fortement menacées par la cybercriminalité. De nombreuses attaques sont effectuées chaque jour. Il y a de nombreux exemples: Le vol d'informations et documents plus ou moins sensibles, le vol d'argent, notamment avec les attaques de la corée du nord sur des banques internationales effectuées afin de s'enrichir. Il y aussi des attaques d'infrastructure ayant pour but de rendre les services informatiques inaccessibles tant qu'une rançon n'a pas été payée. Par exemple, des attaques ont été faites envers des hôpitaux, qui ont été contraints de payer la rançon au plus vite, afin de sauver des vies. Des États achètent également des services de pirates informatiques ou achètent seulement des logiciels malveillants, afin de pouvoir espionner sur les autres Etats, par exemple, le logiciel "Pegasus", ayant infecté le téléphone de nombreux chefs d'Etat (y compris celui du président français) en étant mis sur écoute. Ces attaques entraînent de lourdes conséquences, comme des problèmes de confidentialité, notamment à cause de l'espionnage, des enjeux de sécurité nationale, avec les attaques sur infrastructures publique, et dans certains cas, la manipulation de l'opinion publique avec la répartition de "fake news" dans d'autres pays, souvent afin de changer les élections en faveurs du pays les répandant.

II. La cybersécurité, un outil pour protéger les démocraties

Pour faire face à ces menaces et afin de se protéger, les démocraties emploient des outils de cybersécurité. Les mesures prises par les

gouvernements peuvent varier, certaines sont “légères” ou minimalistes, comme sensibiliser la population envers les dangers du numérique ou même investir dans le développement d'infrastructures, permettant de se protéger de certains risques. D’autres mesures sont plus importantes, pour autant questionnables, comme la surveillance massive d’internet, la censure de contenu (en ligne), l'interdiction de plateformes et logiciels, comme en Russie, où la plupart des réseaux sociaux sont interdits, tout ceci, ajouté au fait qu’il y a une censure de la presse et une production massive de propagande, ce qui entraîne une liberté de penser et d’expression très limitée. De nombreux outils permettant de contourner la surveillance des fournisseurs d'accès à internet sont également interdits en Chine, en Russie et dans d’autres États. La Chine est aussi très connue pour surveiller chacun de ses citoyens à l'aide de caméras à reconnaissance faciale, afin d'attribuer des scores sociaux à chacun, pour ensuite mieux décider de quel droit bénéficie chaque citoyen. Les mesures les plus extrêmes, qui restreignent les libertés individuelles des citoyens, sont souvent utilisées par des “régimes totalitaires” mais cela n’est pas tout le temps le cas.

III. La cybersécurité, un outil utilisé contre les démocraties

Le problème que soulèvent ces mesures sont que, certes en occident les situations politiques ne sont pas si exigeantes, mais le fait d’avoir des outils si puissant à disposition sont une menace, étant donné que rien n’empêche aux états de l’occident de basculer petit à petit vers des régimes totalitaires en utilisant ces outils, afin d’avoir le contrôle sur la population. Un des exemple les plus connus d’abus de pouvoir des USA sur leur population fut quand le lanceur d’alerte Edward Snowden révéla aux médias, via des documents classifiées de la CIA en 2013, que les services secrets américain étaient en train de collecter massivement des données, plus que personnelles, sur les citoyens américains. Il a aussi été révélé que la CIA était en train de s'infiltrer discrètement dans certains états, afin de, s' ils le voulaient, couper totalement l’électricité du pays (Japon, Autriche …). Un autre exemple, est la vidéo disponible sur Wikileaks, montrant un drone américain en train d’abattre 4 journalistes Iraquien en 2007. L’exemple le plus récent est celui de cambridge analytica, où des millions de données facebook ont été utilisées, afin d’essayer de manipuler des élections nationales. Cela montre que les outils prévus pour conserver nos démocraties peuvent être utilisés à des fins contraires.

photo issue de la vidéo prise du drone américain en Irak (2007), Wikileaks

En conclusion, nos démocraties ont besoin d'outils de cybersécurité afin de se protéger des menaces de cybercriminalité. Pour autant, la frontière entre ces outils et nos libertés ne devrait pas être franchie, par risque d’atteindre et de nuire à nos démocraties.