LES DÉMOCRATIES À L'ÉPREUVRE DE LA MENACE CYBER

Plus d'écrans, plus d'informations, plus d'instantanéité : qu'on le veuille ou non, la transformation digitale fait désormais partie de nos vies. Pour le meilleur, comme pour le pire. Car si cette révolution a apporté son lot d'opportunités, les attaques par *ransomware*[1] ou les multiples campagnes de désinformation, montrent qu'elle est aussi un vecteur de risques autant pour les individus et les entreprises, que pour les institutions politiques. Comment nos démocraties sont-elles impactées par cette nouvelle vague de menaces ?

Quels sont les grands équilibres de ce "cyberespace" qui englobe toutes les activités numériques ?
Et surtout, que faire, pour anticiper sereinement l'avenir ?

Le 2 novembre 2020, à la veille de l'élection américaine, **Alix Desforges**, chercheuse au centre GEODE de l'Université Paris 8, **Jean-Louis Gergorin**, ancien vice-président exécutif d'EADS, et **Michel Monneret**, directeur de l'Agence Française de Numérique de la société civile, ont répondu à ces grandes interrogations au cours d'une conférence digitale organisée par Synopia. Cette note synthétise leurs échanges.

I. CYBER ESPACE : UNE GÉOPOLITIQUE DÉBRIDÉE, MAIS UNE GÉOPOLITIQUE QUAND MÊME !

Le cyberespace, cet espace de communication lié à Internet, est très jeune, moins d'une cinquantaine d'années. Il a très rapidement été mis à profit par certains États qui en ont fait un outil géopolitique leur permettant de gagner, entre autres, en influence.

a. Un espace nouveau avec des règles nouvelles ...

Utiliser internet comme moyen d'attaque est particulièrement « rentable » : jamais le risque n'aura été si faible au regard des bénéfices que les organisations peuvent en tirer. Les rançongiciels l'ont démontré : ces virus, véritable pandémie sur la toile, ont une croissance quasi exponentielle ces dernières années, et sont désormais distribués comme des produits logiciel classiques aussi bien via des solutions *ransomware as a service*[2] que sur le dark-web. Une attaque de ce type peut rapporter aux assaillants de plusieurs dizaines de milliers à plusieurs millions d'euros en cas de paiement de la rançon.

Ce type d'outils met en lumière les atouts de la sphère cyber pour les activités criminelles ou militaires : les assaillants expérimentés jouissent d'une capacité de brouillage de leur identité, leur permettant de mener des attaques sous faux drapeau, en laissant un minimum de traces, d'une capacité de projection illimitée et instantanée, d'une disponibilité inégalée des outils (une arme nucléaire se déplace difficilement, un virus se copie sur une clé USB), et d'une remarquable uniformité des technologies. Dès lors, pour les États et groupes criminels divers (notamment les mafia) les barrières à l'entrée sont faibles.

[1] Ransomware : ou en français *rançongiciel* sont des virus informatiques chiffrant les données présentes sur un ordinateur ou sur les ordinateurs d'un réseau informatique. Un paiement (souvent en crypto monnaie) est demandé par les attaquants pour le déchiffrement des données.
[2] Ransomware as a service : fait références au modèle d'exploitation commerciale … *as a service* qui consiste à héberger le service non plus sur l'ordinateur de l'utilisateur, mais sur un serveur distant maintenu par la société fournissant le service. Grâce à ce système, l'utilisateur final paye le service pour un résultat, et ne veut pas avoir à se préoccuper d'un investissement en licence, ni de l'installation du logiciel. Un *ransomware as a service* est donc un service qui fournit la possibilité de mener une attaque par ransomware en indiquant une cible et en payant simplement un prix.

C'est donc une occasion pour les nations de taille moyenne de compenser des manques ou d'équilibrer des rapports de force : tandis que la Corée du Nord a créé *Wanna Cry*[3] pour équilibrer son manque de devises, les Émirats Arabes Unis quant à eux ont mené une guerre informationnelle contre le Qatar en 2017, engendrant la *Crise du Golfe* qui visait à faire pression sur l'Émirat Qatari.

b. … mais des fondamentaux toujours au rendez-vous

La géopolitique du cyberespace est donc plus malléable, flexible, débridée même, et bouge aussi plus rapidement que la géopolitique "classique", mais elle n'en reste pas moins de la géopolitique.

Sur le podium des grandes puissances d'abord, on retrouve quelques têtes connues : les États-Unis, grâce à leur puissance autant offensive que défensive ainsi que leur industrie, et qui font leur propre police sur le web. On retrouve aussi la Chine, la Russie, Israël, l'Inde et des nations Européennes comme la Grande Bretagne ou la France qui sont également des puissances nucléaires.

On peut aussi penser que les frontières sont dissoutes dans le cyberespace, alors que ce n'est pas le cas. Bien sûr, les échanges sont naturellement transfrontaliers, les États voient leur souveraineté plus facilement remise en cause sur leur territoire national sur des processus qui s'inscrivent hors des lois. Mais c'est sans compter sur la capacité que les États ont de contrôler les réseaux et les activités qui y sont liées. On le voit avec le RGPD (Règlement Général sur la Protection des Données) : les démocraties légifèrent sur les usages numériques de leurs citoyens. Et les régimes autoritaires poussent le trait en contrôlant les accès aux réseaux, à l'image des restrictions que la Chine impose directement à sa population ou par la mise en place de rapport de force avec les grands acteurs du web, comme Google.

Mais paradoxalement, l'omniprésence du secteur privé matérialise les frontières dans le cyberespace : la législation des pays d'origine des entreprises s'applique sur les plateformes détenues par les entreprises nationales. Les GAFAM sont soumises au Cloud Act, impliquant la possibilité pour l'administration américaine de consulter les données d'une de ces plateformes. En utilisant ces services, en tant que citoyen Européen, vous êtes protégés par le droit Européen, mais vous êtes en « territoire américain ».

II. LES PROCESSUS DEMOCRATIQUES TOUCHÉS EN PLEIN CŒUR PAR LE CHOC DES NOUVELLES TECHNOLOGIES

Techniquement, les pays peuvent tous être la cible d'attaques. Pourtant, ce sont les démocraties, nos démocraties, qui sont le plus en danger dans cette guerre informationnelle qui se joue dans le cyberespace.

a. Démocratie et menace cyber

Un régime autoritaire a de multiples moyens de tirer profit de la révolution numérique : pour des coûts relativement minimes, il permet à chacun de disposer d'un moyen de communication contrôlé ou influencé par l'État. Cet outil peut donc permettre à la fois la surveillance de masse, l'influence des opinions personnelles, la diffusion de messages favorables au régime... Ce qui est impensable en démocratie où toute mesure de ce type ferait scandale.

Le régime démocratique tire son essence de la confiance que le peuple place en ses représentants. La pire situation dans laquelle pourrait se retrouver une démocratie serait donc de voir ses dirigeants considérés comme des usurpateurs. De plus, la démocratie se base aussi sur le respect des libertés et sur une certaine vérité commune issue du débat démocratique.

b. L'exemple américain

À ce titre, les élections américaines de 2016 ont été un choc pour les Américains. Après avoir été "actifs" depuis plusieurs décennies dans les processus électifs de leurs voisins, le pays de la liberté tombe des nues en voyant ses propres élections secouées par plusieurs déstabilisations : piratage des mails des *Democratic National Committee*,

[3] Wanna Cry : virus informatique développé à partir de 2017. C'est un rançongiciel auto-répliquant ayant touché un grand nombre d'organisations privées ou publiques tout autour du monde.

et publication dans *WikiLeaks* de ces mails ; scandale post-élection sur Cambridge Analytica – on passe des craintes d'attaque du contenant à la manipulation effective du contenu. Tous les éléments de la guerre informationnelle sont utilisés : des attaques vont permettre de récupérer des informations sensibles à diffuser, comme en 2016 ; des "trolls"[4] vont renforcer la polarisation ; et des virus peuvent perturber certains systèmes clé dans l'élection, comme le mécanisme de recensement ou de remontée des résultats le jour J.

Les services américains ont, en effet, longtemps cru que ce serait l'infrastructure des machines à voter qui serait la cible des attaquants. Mais la réalité semble différente. Qu'ils soient Russes, Chinois, ou Iraniens, les groupes qui ciblent les États-Unis en période d'élection ne poursuivraient qu'un seul but : alimenter la dissension au sein de l'électorat. Et ceci tant pour empêcher les débats de fond que pour remettre en cause la validité du scrutin. Ainsi, le président élu verrait son pouvoir diminuer, et c'est donc la puissance du pays qui en pâtit.

c. Plus qu'une menace extérieure, un enjeu structurel

Si les tentatives d'influence de certains États dans le processus démocratique sont manifestes, ces attaques sont-elles responsables du climat de doute et de défiance qui plane dans nos démocraties ? En réalité, la mécanique des réseaux sociaux est au cœur du malaise de nos démocraties, car elles sont en dissonance avec certaines de leurs valeurs fondatrices, en donnant pourtant l'illusion d'être des outils de liberté.

Les réseaux sociaux, ont "le pouvoir d'organiser sans organisation", c'est-à-dire de rassembler les individus sans l'intermédiaire des institutions. Une chance pour ceux qui partagent des intérêts communs, mais qui provoque un véritable choc de désintermédiation : tandis que les médias de masse s'affaiblissent, sur Twitter ou LinkedIn les discours de haine sont difficilement régulés, les fausses nouvelles circulent sans vraiment de filtrage, et des « chambre d'écho » – des communautés autonomes sans accès à l'information autrement que par le réseau de leur communauté – se créent même, comme on peut le voir à l'extrême chez les QAnon[5].

Ces espaces qui pourraient apparaître comme des "zones de liberté" sont au contraire des zones où la liberté est très limitée, essentiellement pilotée par des algorithmes optimisés pour maximiser la consommation de contenu. Ceci est associé au « micro targeting » qui permet de pousser des contenus ciblés à des utilisateurs, comme un ami le ferait en vous connaissant bien. Ces mécanismes sont d'autant plus pervers, qu'ils viennent influencer les utilisateurs dans leur for intérieur, sans débat possible, renforçant encore la polarisation des individus.

De plus, un processus d'égalisation se crée entre les citoyens et les gouvernants, entre les néophytes et les experts : tout le monde peut répondre à tout le monde, la perception du monde de chacun en est donc influencée et les repères disparaissent. La "présomption de compétence" décrite par Michel Serre dans *Petite Poucette* vient remettre en cause les flux d'information verticaux qu'on pouvait connaître jusqu'alors, en faisant croire à chacun qu'il peut être sachant sur tous les domaines. La qualité de ce savoir est pourtant très hétérogène, et devrait donc être considéré avec du recul.

Enfin, la temporalité des plateformes est en dissonance avec celle de nos démocraties : il y a, par exemple, une tension entre l'immédiateté du débat post-scrutin et la lenteur du décompte des voix par correspondance. La crise démocratique arrive, en effet, lorsqu'il y a découplement entre le temps des citoyens et celui de l'État, et on peut surtout craindre que nos démocraties soient dirigées par ce temps "court", alors que les périodes de prospérité ont toujours été guidées par des visions de long terme.

Nous sommes donc loin de l'espace délibératif au sens d'Habermas qui demande respect des intervenants, rationalité et argumentation. Il faut aussi considérer que la multitude des utilisateurs n'est pas le peuple. Ce n'est donc pas ici qu'on pourra construire une démocratie numérique directe, contrairement à ce que de nombreuses personnes pourraient penser. Et c'est à nos gouvernants les premiers de ne pas tomber dans ce piège.

[4] Trolls : individu ou robot dont le but est de générer des polémiques, via un message dans un forum ou sur les réseaux sociaux qui attise un débat conflictuel.
[5] QAnon : mouvance venue des États-Unis regroupant les promoteurs de théories du complot. Ce complot opposerait Donald Trump à des élites américaines, en particulier démocrates.

III. DES RAISONS D'Y CROIRE ENCORE

Nos démocraties ne semblent pas forcément être les mieux engagées dans la bataille du numérique. Les manipulations informationnelles de tout type les secouent, et leur souveraineté numérique est mise à mal. Pour autant, nos pays disposent d'atouts dans cette nouvelle aire.

a. Premier atout : le secteur privé européen

Au niveau international, la France doit continuer à se positionner comme un acteur moteur du multilatéralisme, en menant jusqu'au bout deux initiatives lancées ces dernières années : le PoA (Programme of Action) à l'ONU, inscrivant les discussions autour de la cybersécurité sur le temps long, et l'Appel de Paris pour la confiance et la sécurité dans le cyberespace de 2018, qui ont envoyé un signal positif sur ces sujets.

Si la France veut jouer un rôle de pointe sur la scène internationale, elle doit utiliser les meilleurs outils numériques pour rester compétitive. Il ne faut donc pas acheter dogmatiquement français, et l'utilisation de Cloud privés étrangers restera essentielle. L'enjeu réside donc dans les outils qui minimisent la dépendance et maximisent la sécurité de l'utilisation de ces plateformes, comme le chiffrement homomorphique, une technique qui permet de faire des calculs sur des données chiffrées.

La filière française dispose justement de talents et de structures fortes en la matière. Cependant, ces entités sont principalement axées aujourd'hui autour du conseil, donc un modèle peu exportable, peu réplicable et coûteux. Il faut transformer ces prestations de conseil en produits, qui seraient de fait exportables. Un bon exemple de ce schéma est la startup Sqreen qui propose un produit de détection et de prévention des menaces – mettant à la disposition des entreprises françaises un produit français.

Le développement de la filière cyber en France doit être maintenu, en collaboration avec les écoles d'ingénieurs et université, dans un secteur qui peut être, comme celui de la transition écologique, grand pourvoyeur d'emploi, et moteur de la relance. Notons que la France et Paris ont plus que jamais gagné, ces dernières années, en attractivité vis-à-vis des talents à l'échelle européenne. Cet effort de marketing doit être poursuivi : la France doit être reconnue comme un leader de l'innovation cyber. Les entreprises doivent aussi y contribuer en valorisant les métiers de la cybersécurité par, entre autres, des salaires attrayants, comme les États-Unis l'ont fait jadis avec succès pour les informaticiens, drainant ainsi les réservoirs de talent du monde entier. La bataille du numérique a un coût, elle nécessite des investissements.

b. Deuxième atout : la culture et l'éducation

Enfin, une des composantes clé du débat ne sera pas technique, mais culturelle. Nos gouvernants doivent d'abord sortir de la dynamique réactive qu'ils ont vis-à-vis des réseaux et qui les pousse à agir sur un temps court. Ils ne doivent pas être, dans leur prise de décision, influencés par les réseaux. Ils doivent s'inscrire dans une démarche proactive.

Chacun de nous doit, ensuite, être conscient des enjeux d'information numérique et de sécurité informatique, à tous les âges : cela passe à la fois par une éducation à ces concepts, dès le plus jeune âge, puis avec les cours d'éducation civique au collège qui offriraient une formation permettant à chacun d'interroger les contenus trouvés en ligne et sensibiliser aux enjeux cyber. Pour les publics plus âgés, des formations pourraient être proposées au sein d'associations, et viendraient compléter des programmes télévisés réalisés par des experts issus des associations de terrain ou de la communauté scientifique : spécialistes de l'apprentissage, chercheurs ou psychologues.

Nous avons donc les plus grandes raisons d'espérer : l'agilité de nos démocraties et de nos marchés, l'initiative individuelle couplée à un ambition politique forte, et notre culture Française et Européenne basée sur la liberté individuelle et la vie privée, devraient nous permettre d'axer nos ressources dans le bon sens et de sauter cette marche qui est, non seulement un enjeu pour l'avenir, mais aussi une composante structurelle du monde de demain.

Directeur de la publication : Alexandre Malafaye
Comité éditorial : Xavier Dupont, Jean-Claude Mailly, Jean-Marc Schaub, Joséphine Staron
Contributeur : Damien Gallet, membre du groupe de travail « Numérique »