Le processus de Pall Mall : un effort diplomatique pour encadrer l'essor commercial des outils de hacking

Léonard ROLLAND
Sous-directeur de la cybersécurité
Ministère de l'Europe et des Affaires étrangères

Face à la prolifération et l'usage irresponsable des capacités de cyber-intrusion disponibles sur le marché, la diplomatie française est à la manœuvre pour faire émerger un consensus international sur un dossier complexe, où volontarisme politique et sens de la nuance sont invités à faire bon ménage.

Une « bombe à retardement ».

C'est sur ce signal d'alarme adressé par Vincent Strubel, le Directeur général de l'ANSSI, que s'est ouverte la deuxième conférence internationale du Processus de Pall Mall le 3 avril dernier, à l'initiative du Ministère de l'Europe et des Affaires étrangères et en partenariat avec le Foreign Office britannique.

L'objet de cette inquiétude : la prolifération de capacités de cyber-intrusion disponibles sur le marché, ou CCIC (commercial cyber intrusion capabilities) dans le jargon diplomatique international. Cette catégorie recouvre des produits « clés-en-main », comme les logiciels espions de type Pegasus, Predator, ou plus récemment Graphite, pour ne citer que les plus connus. Les CCIC peuvent également être commercialisées sous la forme de prestation de services, on parle alors de « hackers-for-hire », à l'instar de l'entreprise I-SOON dont l'ampleur des activités cyber-offensives ont été révélées l'année dernière. Enfin, certaines entreprises sont spécialisées dans la vente de composants critiques au développement de capacités de cyber-intrusion, à l'instar des failles « zéro day », ces vulnérabilités informatiques dont le coût – jusqu'à plusieurs millions d'euros l'unité – est proportionnel à la rareté.

Utilisés de manière responsable, les capacités commerciales de cyber-intrusion jouent un rôle crucial au service de notre sécurité nationale, par exemple en matière de lutte contre le terrorisme ou contre la criminalité organisée.

Mais leur usage abusif, régulièrement documenté à travers le monde, porte un triple risque pour :
- les libertés fondamentales, les CCIC étant régulièrement utilisés à des fins de surveillance arbitraire d'opposants politiques, de journalistes ou de défenseurs des droits de l'Homme,
- la sécurité nationale des Etats, ces capacités venant accroître la menace de cyber-espionnage voire de sabotage pesant sur nos intérêts,
- la paix et la stabilité internationale du cyberespace, car la prolifération des CCIC abaisse d'une part le seuil d'accès aux capacités cyber-offensives et rend d'autre part le travail d'attribution encore plus ardu.

Identifier des solutions à ce phénomène inquiétant, c'est tout l'objet du Processus de Pall Mall, une initiative diplomatique lancée en 2024 par la France et le Royaume-Uni, qui vise d'une part à lutter contre la prolifération de telles capacités, mais également d'autre part à en établir un cadre d'emploi responsable par les Etats.

Le Processus de Pall Mall, c'est tout d'abord une méthode innovante.

Lancé en février 2024 à Londres, ce processus a donné lieu quelques mois plus tard au lancement par la France et le Royaume-Uni d'une grande consultation auprès des Etats, de l'industrie, de la société civile et de la recherche. Le but ? Identifier quelles pourraient être les meilleures pratiques en matière de régulation, mais aussi les défis en la matière.

A l'image de l'Appel de Paris pour la sécurité et la confiance dans le cyberespace lancé par le Président de République en 2018, dont il est une déclinaison « sectorielle » sur les enjeux de prolifération cyber, le Processus de Pall Mall se caractérise en effet par une forte dimension « multi-acteurs ».

Lors de ses réunions, s'y côtoient des diplomates, des représentants des services de renseignement et d'agences de cybersécurité, des ONG de défense des droits de l'Homme, des acteurs industriels de la cyber-intrusion…et d'autres acteurs industriels en charge de lutter contre les outils de cyber-intrusion. Ce format permet d'une part d'avoir accès à une expertise la plus large possible ; il permet d'autre part de créer des ponts entre communautés afin de mieux comprendre les points de vue et les contraintes de chacun, voire parfois de favoriser la coopération entre parties prenantes lorsque les intérêts sont partagés.

Ce format inclusif, de même qu'un calendrier soutenu des travaux, font du Processus de Pall Mall un véritable « accélérateur de discussions », pour reprendre les termes d'un participant à la conférence d'avril. Tant au niveau national, où les Etats ont dû faire émerger en quelques mois une position consolidée sur le sujet (en France c'est le fruit d'une étroite concertation interservices), qu'au niveau international, où le sujet est désormais bien identifié à l'ordre du jour diplomatique, y compris au sein de l'Organisation des Nations Unies.

25 Etats s'engagent à Paris.

La conférence d'avril à Paris a permis l'adoption d'un Code de bonnes pratiques à destination des Etats pour lutter contre la prolifération et l'usage irresponsable des CCIC. Ce document rappelle le cadre normatif international applicable à l'action des Etats, détaille quatre grands principes d'action (redevabilité, précision, transparence et contrôle) et recense un grand nombre de bonnes pratiques dans différents domaines, du contrôle export au contrôle des techniques de renseignement, en passant par la transparence en matière de gestion des vulnérabilités ou l'accès au recours juridictionnel par les victimes de cyber-intrusion.

Compte-tenu du caractère extrêmement régalien et sensible du sujet, s'accorder sur un tel document – même si celui-ci est de portée volontaire – représente une avancée importante, a fortiori dans le contexte actuel de polarisation de l'environnement géopolitique et de désagrégation du cadre international de stabilité stratégique. Pour autant, c'est bien la phase de mise en œuvre des engagements qui s'ouvre qui s'avère la plus cruciale. Le processus de Pall Mall aura ainsi vocation à servir de plateforme d'échange entre ses membres pour l'échange de bonnes pratiques, tandis que la société civile s'organise déjà pour assurer un suivi des engagements pris par les Etats à Paris. En parallèle, le processus de Pall Mall sert de catalyseur pour la mise en place d'initiatives dédiées au soutien aux victimes.

A moyen terme, l'objectif est de négocier un nouveau Code de bonnes pratiques, cette fois à destination des entreprises. Ce document aura vocation à établir un cadre d'action responsable pour le secteur de la cyber-intrusion aussi bien que pour les entreprises de cybersécurité en charge de lutter contre cette menace.

Cybersécurité et cyberdiplomatie.

A l'heure où le numérique rebat les cartes de la puissance, entre Etats, mais également avec certains acteurs privés, la diplomatie a plus que jamais un rôle à jouer dans l'organisation de ces nouveaux rapports de force. Le processus de Pall Mall, s'il ne constitue qu'une partie de l'exercice de désamorçage de la « bombe à retardement » évoquée par Vincent

Strubel, a déjà démontré sa capacité à briser les silos qui freinent l'identification de solution : silos entre Etats, secteur privé et société civile, entre acteurs offensifs et défensifs, ainsi qu'entre les différents leviers dont disposent les Etats pour lutter contre la menace issue de la commercialisation des outils de hacking.