PV Audition
CyberPeace Institute

M. Stéphane Duguin - Directeur exécutif du CyberPeace Institute (Genève)

Mission du CyberPeace Institute : quelles sont les menaces pertinentes à étudier?

Le CyberPeace Institute s'intéresse à la convergence de plusieurs menaces qui n'ont pas forcément à voir les unes avec les autres. Les problématiques étudiées sont les suivantes:

- *La sophistication des capacités criminelles:* accroissement de l'exploitation des vulnérabilités pour créer de nouvelles attaques, interconnexion de la sous-traitance, explosion du nombre de victimes de campagnes de *ransomware* plus ou moins sophistiquées.

De manière inédite et significative, les campagnes de *ransomware* sont passées d'une problématique de droit pénal à une problématique élevée au niveau de la sécurité de l'État.
Les compagnes d'attaques informationnelles ne sont pas toutes organisées par des acteurs étatiques mais également par des groupes criminelles. Une cyber-attaque, en son cœur, est une manipulation cognitive, il s'agit de faire croire à quelque chose que l'on n'est pas censé croire.
Ces attaques sont motivées par l'appât du gain financier et ont un effet très néfaste sur la confiance qu'ont les utilisateurs dans les interfaces numériques, et envers l'ensemble de l'information qui leur parvient.

- *La désinformation opérationnelle pour asseoir des agendas géopolitiques précis.* Il s'agit d'une manipulation cognitive avec une motivation politique et ayant un impact sur le terrain.

EX: travail conséquent du CyberPeace Institute sur la désinformation liée à la pandémie et comment les fausses informations dans ce contexte peuvent devenir presque une arme. L'Institut a œuvré pour la défense du monde hospitalier face à cette menace: focus sur les attaques dures *ransomware*, le cyber-espionnage (États qui essaient de voler des informations sur les vaccins par exemple).

- *La recherche et la vente d'outils pour attaquer ou pour surveiller*

EX: La compétence et la capacité technologique à développer ces outils se trouve dans le privé: NSO, Pegasus et autres boîtes qui travaillent sur la vulnérabilité cognitive et sur la cyber-insécurité. Ce phénomène existe parce que les États achètent et laissent faire et peut s'apparenter à une course à l'armement dans le cyber-espace.

La mission du CyberPeace Institute est de protéger les populations vulnérables dans cette asymétrie globale d'informations. La structure s'est spécialisée dans la défense et la protection des ONG dans le secteur humanitaire. Ces acteurs ont à leur disposition des données multiples et extrêmement sensibles, instrumentalisables par les criminels, alors que leur capacité technologique de défense est proche de 0.

En quoi la nature systémique des opérations informationnelles peut entraîner une vulnérabilité à l'échelle de la société?

Pour mener une opération informationnelle, il faut faire de la R&D sur des méthodes qui vont permettre d'aller dans les trous de l'Internet et exploiter des vulnérabilités d'ordre technologique.
Il est illusoire de croire que si c'est l'État qui les mène, cela restera domestique, dans un certain cadre et sous un certain contrôle. Sauf que concrètement, les individus bougent, les outils se font voler/*leaker.*
Par conséquent, il n'est pas possible d'anticiper les débouchés d'une attaque informationnelle, même si celle-ci est menée par l'État. Faire exister ce type d'opérations dans le cadre étatique va à l'encontre de ce que l'on attend de lui dans ce domaine, à savoir de protéger l'environnement informationnel dans lequel tout le monde est actif pour qu'on puisse avoir confiance dans cet environnement. Cela crée des vulnérabilités d'ensemble et le système n'est plus sûr.
L'impact sociétal de ces opérations peut être très important. Si on ne peut plus faire confiance à l'environnement numérique, on crée une relation biaisée à l'outil. Or l'outil est notre vecteur principal pour

la relation à l'autre. Par conséquent, cela crée un climat d'insécurité permanente entre les individus et un manque de confiance en l'information numérique.

La supervision éthique et démocratique des opérations informationnelles est illusoire selon Stéphane Duguin.
Comment s'assurer qu'il existe bien des garde-fous et des mécanismes de surveillance de l'utilisation par l'État de stratégies d'opérations informationnelles, via *ransomware* ou autres, pour des raisons de sécurité et de défense? Comment les utilisateurs auront la certitude que leurs intérêts sont pris en compte?
Ensuite, il y a toujours cette illusion du contrôle de l'attaque dans un cadre précis sauf que les choses ne restent jamais dans leur écosystème.

Stéphane Duguin exprime une forte inquiétude quant à l'adoption par l'État de tactiques et de stratégies d'opérations informationnelles. Il s'agit de la même tactique que celle employée par Daesh avec sa propagande entre 2015 et 2018. Jouer au même jeu que les criminels, utiliser les mêmes méthodes et modes opératoires est dangereux et pourrait se retourner contre nous. Quand on crée de la manipulation, on peut mécaniquement créer de la radicalisation, quelle qu'elle soit : terroriste, anti-vax, etc.

Le rôle de l'Etat doit être la mise en place de mesures pour lutter contre ces opérations et cette criminalité dans le cyber-espace. Cela implique de l'investissement et des moyens massifs ainsi qu'une coopération internationale accrue.
L'utilisation et le détournement des innovations technologiques par les criminels rend le travail de cyber-défense extrêmement délicat.

Pour contrer ces menaces, il y a un double manque : à la fois de compétences et de communication entre les services de cyber-défense.

1) La réponse ne sera pas entièrement technologique, il faut des ressources et compétences humaines, des investissements et une spécialisation accrue. Il est nécessaire que les experts soient capables d'informer les pouvoirs publics et de peser sur la décision politique.
Dans le cas de l'élaboration de nouvelles langues visuelles (Daesh sur Tumblr avec les lions), il faut que des experts puissent comprendre la mutation de la langue textuelle vers une langue visuelle et en informer les pouvoirs publics.

2) La deuxième partie de la réponse est de ne pas participer ou utiliser les mêmes méthodes que l'attaquant. Le réflexe des services de renseignement de riposter directement à la génération malveillante de contenu sur Internet est dangereux .

Fonction opérationnelle à Europol
Après Christchurch, Europol a coordonné la réponse européenne pour endiguer le contenu en temps réel.
De nombreuses communautés, ayant des objectifs complètement différents, ont mené des stratégies différentes pour promouvoir le contenu en question :

- La communauté *far right* a usé de sa capacité technologique pour promouvoir du contenu *far right* suite à l'attentat.
- La communauté djihad dur : promotion du contenu pour appeler à la violence et se venger de l'attentat.
- La communauté de *shit posters*: stratégies de démultiplications du contenu.
- Mainstream médias: promotion du contenu et de l'événement à des fins journalistiques et avec des approches plus ou moins éthiques.

Parce que les communautés ont toutes suivi leur agenda très spécifique, il est impossible de penser sérieusement au fait qu'une opération informationnelle même étatique ne sortira pas de l'écosystème défensif et ne sera pas détourné.

Recommandations

Coopération exigeante et obligatoire avec les plateformes:

- Comprendre le fonctionnement des plateformes ainsi que l'interaction de l'utilisateur avec celles-ci.

Il faut que les législateurs et autres acteurs inclus dans le processus de régulation aient une capacité de compréhension de la plateforme. On ne peut pas discuter avec Facebook ou Instagram si on n'en comprend pas les mécanismes.

De manière plus générale, il faut que des qualités telles que la curiosité et de l'expertise d'Internet soient bien représentées dans les assemblées législatives où les discussions autour de la régulation et de la coopération se déroulent.

- Démontrer une exigence de transparence et une vraie ambition démocratique (*oversight* du Parlement).

Ces plateformes évoluent dans un système global. Il faut leur rappeler que l'Europe est *leadeuse* en matière de régulation (RGPD, TCO, DSA), réaffirmer ses valeurs et le cadre dans lequel ces plateformes s'inscrivent lorsqu'elles s'installent en Europe.

- Exigence technologique : si on demande des données, il faut être en mesure de les comprendre, et être à la hauteur de ses ambitions.
- Responsabiliser l'État en matière industrielle pour qu'il n'achète pas de produits de surveillance de masse (NSO).

La menace numérique se transforme très vite et la loi évolue lentement. Face à ce constat, la tentative de créer de nouvelles lois chaque année est grande. Néanmoins, cette inflation de loi ne doit pas négliger la phase de mise en application concrète (mis en œuvre de moyens conséquents, veiller au respect des règles édictées par la loi) des textes à l'échelle nationale ou européenne.

Les blocages dans la coopération avec les plateformes

Blocages au sein des plateformes

- L'opacité du fonctionnement des plateformes : il est difficile de contrer les opérations et de comprendre comment l'information circule.

Blocages internes aux organes étatiques

- La fragmentation et l'éclatement des informations sur le fonctionnement d'une plateforme entre les différents services français rend les demandes à formuler aux plateformes plus compliquées.

Recommandation: œuvrer pour une centralisation de l'information pour savoir ce qu'il est possible de formuler ou non comme demande.

- Le manque d'indépendance de structures impulsées par les plateformes (GIFCT par ex.) pose problème.

Recommandation: Exigence d'indépendance de la recherche face aux plateformes pour qu'elle ne soit pas entachée de suspicion.

Recommandation: Investir davantage dans les interactions avec les plus petites plateformes numériques ainsi que celles qui émergent, pendant leur phase de *start-up/scale-up*. Cela peut contribuer à un travail de *scouting* qui pourrait constituer la base d'une nouvelle façon de penser l'écosystème informationnel et de le rendre plus vertueux.