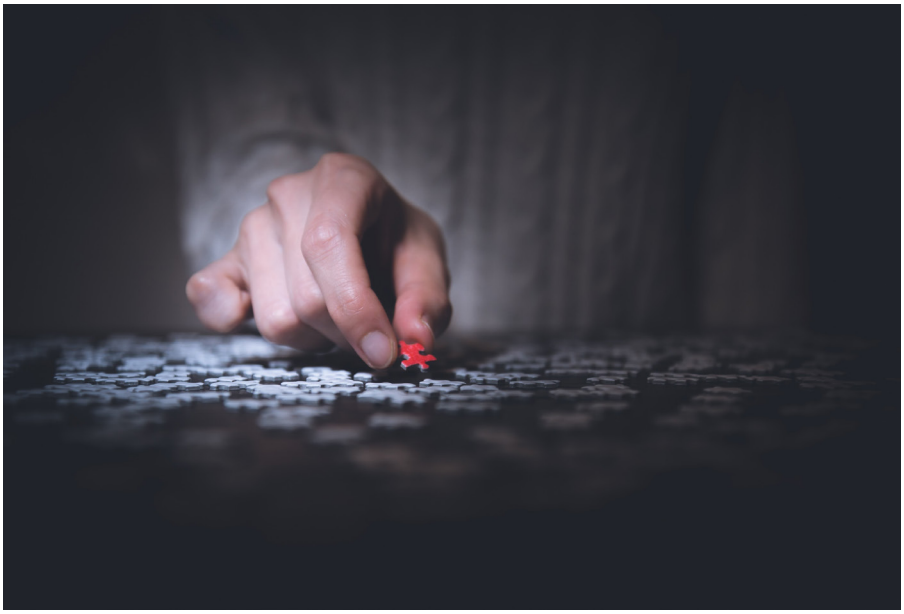
L'attribution publique d'incidents cybernétiques

De plus en plus de d'incidents cybernétiques sont publiquement attribués aux responsables. Mais souvent, les informations communiquées par les États et les entreprises de cybersécurité sont peu transparentes et difficiles à comprendre. Pour renforcer la confiance dans ces attributions publiques, il faut des mécanismes institutionnels au niveau international et l'engagement des États, des entreprises et de la société.

Par Florian J. Egloff et Andreas Wenger



L'attribution est un processus long et complexe qui consiste à rechercher des indices afin de débusquer les responsables d'incidents cybernétiques. *Ryoji Iwata / Unsplash*

Qui est à l'origine d'un incident cybernétique? Répondre à cette question a longtemps été, et reste encore aujourd'hui, parmi les défis techniques des plus exigeants. Du fait de la structure même d'Internet, il est relativement facile de conserver un certain anonymat technique. Les auteurs d'attaques ont avantage, car la partie touchée ignore souvent dans un premier qui se cache derrière un incident cybernétique. La recherche scientifique longue et complexe qui consiste à rechercher des indices pour débusquer le coupable est appelée «processus d'attribution». Lorsque la partie touchée pense connaître le responsable de l'incident cybernétique, elle doit ensuite décider si elle doit réagir et comment. L'une des options à sa disposition est l'attribution publique, c'est-à-dire que l'incident cybernétiqueest publiquement imputé à un auteur précis.

Le nombre d'attributions publiques d'incidents cybernétiquespar les États et les entreprises est en augmentation depuis quelques années. Du côté des gouvernements, les États-Unis sont très actifs en la matière. L'acte d'attribution peut prendre diverses formes allant de la prise de position publique aux poursuites judiciaires, en passant par la déclaration commune avec des partenaires de coalition. Dans le secteur privé, ce sont essentiellement les entreprises de cybersécurité qui désignent les responsables des incidents cybernétiques, individuellement ou en groupe, dans des rapports publics. Elles établissent parfois des liens directs entre les groupes d'auteurs et certains États.

Ces deux types d'attribution publique jouent un grand rôle politique, en particulier dans les démocraties. La divulgation au public des interactions numériques entre les auteurs et les victimes d'un incident cybernétique est une condition essentielle pour garantir la formation de la volonté démocratique et la légitimité politique des options d'action au niveau national et international – allant des questions d'assurance aux procédures pénales, tout en passant par les préoccupations liées à la guerre et à la paix. Le manque de transparence et de responsabilité laisse les sociétés dans l'ignorance quant à la manière dont les États et les entreprises de cybersécurité

parviennent à leurs conclusions publiques et quant à leurs motivations. Les propositions visant à instaurer une gouvernance internationale et à renforcer la confiance dans les processus d'attribution montrent que pour lutter plus efficacement contre les incidents cybernétiques, il faut la contribution des États, des entreprises et de la société civile – y compris les universités.

Légitimité politique

Dans les démocraties, la légitimité politique repose sur la transparence des agissements de l'État. Dans le domaine de la cybersécurité, un minimum d'attribution publique est donc nécessaire pour assurer la transparence de l'action gouvernementale. S'il est possible de prendre des mesures préventives et passives pour renforcer sa propre cybersécurité, même sans connaître les agresseurs potentiels, il est nécessaire de pouvoir déterminer qui est responsable de l'incident pour agir contre des agresseurs spécifiques. Une autre question se pose ensuite: faut-il rendre publiques les informations acquises?

Une attribution est une condition indispensable pour assurer la coopération internationale dans le cyberespace.

Les réponses varient selon les systèmes politiques. Au niveau national, on attend généralement plus de transparence dans les démocraties que dans les autocraties pour légitimer certaines mesures à caractère coercitif (poursuite pénale, guerre). Mais même dans les démocraties, les informations ne seront pas rendues publiques si les conflits cybernétiques sont perçus comme relevant en premier lieu des services de renseignement. Sur le terrain de la cybersécurité, tous les acteurs étatiques ont deux visages: d'un côté, ils protègent, de l'autre, ils peuvent être responsables d'attaques. Du fait de cette double casquette, l'attribution publique des incidents cybernétiques est une question très controversée. Les débats nationaux sur les menaces diffèrent selon les systèmes politiques, ce qui offre aux États autoritaires des angles d'attaque potentiels. Néanmoins, en raison de l'interconnexion des systèmes techniques, les effets stratégiques sont difficilement contrôlables pour toutes les parties prenantes.

Dans ce contexte, la retenue stratégique que l'on observe de la part des acteurs étatiques est à considérer à la lumière du fait que certaines opérations cybernétiques sont délibérément exécutées à des fins coercitives. Au niveau international, il est important de maintenir un minimum de stabilité stratégique. Dans ce cadre, il est essentiel d'avoir la possibilité d'identifier les responsables des incidents cybernétiques et de prendre des contre-mesures. Sans cette capacité, les mécanismes de sécurité classiques, notamment la dissuasion et le contrôle de l'escalade, risquent de ne pas être opérants. Une attribution compréhensible pour le public est également une condition indispensable pour assurer la coopération internationale dans le cyberespace. Si les normes cybernétiques doivent servir de cadre à une action responsable dans le cyberespace, cela suppose que leur respect ou leur mépris soit identifié par les autres acteurs. Dans une telle situation, l'attribution publique peut être un moyen de proscrire les violations de ces normes.

Asymétrie des connaissances

Les attributions publiques d'incidents cybernétiques ont augmenté ces dernières années. Au niveau des États, la cybersécurité est devenue une question politique centrale. Les gouvernements focalisent de plus en plus leurs services de renseignement sur le sujet et investissent dans des capacités d'attribution. Dans un même temps, l'option de l'attribution publique fait désormais partie des instruments de politique étrangère et de sécurité à disposition. Les entreprises, elles aussi, ont rapidement développé leurs capacités dans ce domaine. De nouvelles possibilités techniques en matière de cybercriminalistique et de nouvelles méthodes d'identification des auteurs ont été mises au point. Aujourd'hui, les entreprises de cybersécurité publient des rapports réguliers sur les *Advanced Persistent Threats (APT),* c'est-à-dire des groupes de hackers professionnels qui mènent en continu des opérations ciblées mobilisant beaucoup de ressources.

Cependant, peu d'États et d'entreprises privées possèdent des capacités et des processus d'attribution professionnels qui leur permettent d'identifier les acteurs politiques qui se cachent derrière les incidents cybernétiques. Il s'agit essentiellement de pays dotés de systèmes très performants dans le renseignement électromagnétique (en anglais *Signals Intelligence* ou SIGINT) et de quelques entreprises qui exploitent leurs propres réseaux mondiaux de capteurs ou dont le modèle économique leur donne une vue d'ensemble des flux de données mondiaux. Les autres acteurs étatiques ou privés n'ont, pour la plupart, ni la capacité de mener des processus d'attribution, ni les moyens de s'acheter ces connaissances. Au regard de la légitimité politique et de l'exigence de véracité de l'attribution publique, cette asymétrie des connaissances pose problème. En effet, des informations impossibles à vérifier de façon indépendante sont sujettes à manipulation – à la fois par ceux qui savent et par ceux qui ne savent pas.

Manque de transparence

En règle générale, les attributions publiques des incidents cybernétiques par les États et les entreprises de cybersécurité sont peu transparentes. Les informations publiées ne permettent pas de vérifier en détail les accusations portées. Cet état de fait reflète l'absence de normes internationales sur la question. Les techniques de cybercriminalistiques approuvées à l'échelle internationale n'ont pas encore été pleinement mise en place. D'autre part, il y a souvent plus de consensus entre les experts qu'il n'y paraît. Mais pour des raisons structurelles, les États et les entreprises n'ont pas d'intérêts à révéler toutes les informations au public.

Les États mettent en balance plusieurs intérêts en matière de cybersécurité: ils disposent de moyens offensifs et défensifs et agissent sans connaître précisément les motivations et les capacités de leurs concurrents. Malgré leur retenue stratégique, ils sont responsables, de façon directe ou indirecte, d'une grande partie des activités offensives dans le cyberespace. Pour des raisons d'ordre structurel, la confidentialité des capacités techniques et des sources est la réponse standard apportée par les États aux incidents cybernétiques. Cependant, les attributions publiques restent l'exception. Lorsqu'un incident cybernétique est publiquement imputé à un auteur précis, ce choix répond donc à des motivations politiques complexes. La plupart des attributions publiques réalisées à ce jour semblent servir des intérêts liés à la politique étrangère et à la sécurité. Elles poursuivent aussi, dans une moindre mesure, des intérêts politiques nationaux.

Les entreprises de cybersécurité, en revanche, ont intérêt à démontrer au grand public qu'elles disposent de capacités d'analyse indépendantes. Leurs rapports leur font une belle publicité dans un marché en pleine croissance. Cependant, elles ont aussi de bonnes motivations structurelles pour

ne pas révéler les informations sur toutes leurs sources de données. D'une part, la base de données d'une entreprise de cybersécurité est un secret commercial à forte valeur économique. D'autre part, les meilleures données proviennent souvent de réseaux de clients qui sont soumis à des accords de confidentialité. Enfin, les entreprises de cybersécurité ont une compréhension des conflits cybernétiques qui se limite aux technologies qu'elles proposent et aux marchés sur lesquelles elles opèrent. En résumé, elles possèdent une connaissance détaillée de certains acteurs, dont une partie seulement est divulguée au public.

Le processus d'attribution

L'attribution des incidents cybernétiques est, par nature, une mission interdisciplinaire. Elle nécessite des connaissances fondamentales en informatique, en particulier dans les domaines de l'investigation criminalistique, de la sécurité des réseaux et de l'analyse des logiciels malveillants. Mais d'autres dimensions telles que la politique, l'économie, la psychologie, la science administrative et le droit apportent également une contribution importante au processus d'attribution et aident à comprendre les attributions publiques.

Le processus d'attribution génère des connaissances sur l'origine d'un incident cybernétique. On peut analyser cette démarche sur trois niveaux. Au niveau tactique, elle permet de déterminer précisément ce qui s'est produit et comment les auteurs ont procédé. Au niveau opérationnel, elle permet d'acquérir des connaissances supplémentaires sur les responsables en intégrant toutes les sources de renseignement. Au niveau stratégique, elle permet d'évaluer l'incident sous l'angle politique. Il s'agit notamment d'identifier ses causes dans le contexte d'autres incidents.

À l'échelle internationale, il n'existe pas de mécanisme institutionnalisé d'attribution publique.

À la fin du processus, il faut ensuite décider si l'on va tirer des conséquences politiques de l'incident et si oui, lesquelles. L'une des nombreuses options est l'attribution publique.

Ces trois niveaux mobilisent des acteurs différents. Au niveau tactique, les États, les entreprises ou les particuliers font appel à des entreprises de cybersécurité spécialisées dans la gestion des incidents. L'intervention des autorités est surtout indiquée lorsqu'il y a un lien avec la sécurité nationale ou lorsque l'affaire risque d'être portée au tribunal. Au niveau opérationnel, les processus d'attribution se déroulent généralement au sein des services de renseignement, mais peuvent également relever de la police ou du ministère public dans le cadre d'enquêtes judiciaires. Au niveau stratégique, les options d'action sont le plus souvent définies par les instances nationales de sécurité. Les incidents cybernétiques font l'objet d'une évaluation exhaustive dans le contexte plus large de la politique étrangère et de sécurité. Les options d'action n'ont alors aucun lien avec le cyberespace et englobent tout l'éventail des instruments politiques.

Les mécanismes institutionnels

À l'échelle internationale, il n'existe pas de mécanisme institutionnalisé d'attribution publique dans le domaine de la cybersécurité. Cependant, les partisans d'un tel mécanisme sont de plus en plus nombreux. Quels acteurs doivent participer à un processus d'attribution international et selon quelles modalités? Aucun consensus n'a encore été trouvé sur cette question. Les propositions quant au degré d'implication des États, des entreprises et de la société civile, à la nature et au contexte des incidents cybernétiques, à la forme d'organisation et au caractère contraignant des règles fixées sont très divergentes. L'aspect décisif pour la crédibilité de l'attribution publique est de savoir quels acteurs (l'industrie, les États ou la société civile) seront au centre des mécanismes proposés.

Les approches centrées sur l'industrie se concentrent sur l'attribution des incidents cybernétiques soutenus par des États, ce qui peut aller à l'encontre des intérêts d'entreprises internationales. Par exemple, *Microsoft* a proposé dès 2017 la création d'une organisation indépendante pour permettre la coopération entre les entreprises technologiques dans le domaine de l'attribution. Le premier objectif d'une telle organisation serait d'assurer une identification et une attribution politiquement neutres des incidents cybernétiques émanant d'États. En favorisant la coopération internationale d'experts de la cybersécurité et la transparence des données et des conclusions, *Microsoft* espère combler le déficit de confiance actuel vis-à-vis de l'attribution publique.

Lectures conseillées

Deibert, R. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs, 32* (4), p. 411–424. Le *CitizenLab* a également conduit des recherches sur le sujet des cyberattaques visant la société civile.

Grindal, K., Kuerbis, B., Badiei, F. & Mueller, M. (2018). Is it time to institutionalize cyber-attribution? *Internet Governance Project White Paper.*

Rid, T. & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies, 38* (1–2), p. 4–37.

Schulzke, M. (2018). The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty. *Perspectives on Politics, 16* (4), p. 954–968.

Les États-Unis ont créé une certaine transparence concernant leurs méthodes d'attribution avec le document suivant: Office of the Director of National Intelligence (ODNI) (2018). «A Guide to Cyber Attribution». *U.S. Office of the Director of National Intelligence Publication.*

Les approches centrées sur les États se focalisent également sur l'attribution des conflits cybernétiques étatiques. Un groupe de réflexion russe a ainsi proposé la création d'un tribunal international indépendant d'arbitrage pour les conflits cybernétiques entre États. Dans le même ordre d'idée, le *think tank* américain *Atlantic Council* recommande la mise en place d'un conseil d'arbitrage multilatéral pour les incidents cybernétiques qui dépassent le seuil de violence d'un conflit armé. Les États dotés de capacités d'attribution avancées les mettraient à la disposition de cette instance, tandis que ceux dépourvus de telles capacités pourraient la saisir. Le conseil communiquerait les éléments de preuve et ses recommandations aux organes de sécurité internationaux ou régionaux, qui décideraient des éventuelles sanctions.

Certaines approches centrées sur la société civile ont déjà été lancées. *AccessNow* déplore la trop grande place accordée à la création d'organisations. L'ONG propose de se concentrer davantage sur le développement de lignes directrices et de normes en matière de preuve. Ronald J. Deibert, directeur du *CitizenLab* à Toronto, a déposé l'idée d'un réseau d'instituts universitaires qui mènerait des recherches distribuées, transparentes et scientifiquement évaluées sur les incidents cybernétiques. Le *think tank* américain *RAND* Corporation suggère une troisième voie: il recommande

la création d'un consortium mondial permanent d'acteurs non étatiques chargés d'attribuer les incidents cybernétiques les plus importants.

Toutes ces recommandations visent à réduire l'asymétrie des connaissances en matière d'attribution publique et à lutter contre la méfiance qui en découle. Elles reposent sur l'hypothèse que l'on fait confiance aux attributions publiques lorsqu'elles sont évaluées de façon transparente par un réseau international d'experts. D'un point de vue politique, cependant, la situation est différente selon que l'incident émane ou non d'un État. En cas de conflit cybernétique étatique, il est impératif d'impliquer les acteurs publics pour apporter une réponse politique. Si l'incident n'est pas imputable à un État, les interactions peuvent se limiter à un échange avec les autorités nationales. Il faudrait donc un réseau de mécanismes internationaux au sein duquel les approches centrées sur l'industrie, sur les États et sur la société civile se complèteraient. Les capacités d'attribution sont développées de façon décentralisée et reposent sur des structures de confiance nationales et régionales, étatiques et non étatiques. Or, pour pouvoir apporter une réponse politique, résoudre la question des sanctions et assurer la stabilité internationale, ces structures décentralisées doivent absolument être rattachées aux institutions de sécurité régionales et mondiales existantes.

Le rôle des universités

Pour élaborer un cadre de gouvernance viable concernant l'attribution publique des incidents cybernétiques, il faut l'engagement de l'État, des entreprises et de la société. Mais les universités peuvent aussi jouer un rôle important pour renforcer cette confiance. Elles développent et transmettent des connaissances publiques, transparentes et évaluées et peuvent ainsi contrecarrer l'asymétrie des connaissances qui caractérise l'attribution des incidents cybernétiques. Elles interviennent sur deux tableaux: la recherche et la création de réseaux.

> Un consortium d'institutions universitaires menant des recherches autonomes pourrait aider au développement de connaissances publiques.

D'une part, les universités peuvent mener des recherches interdisciplinaires et évaluées par des pairs sur les problèmes d'attribution. Pour étudier les processus d'attribution publique, il convient d'intégrer une expertise technique, politique et organisationnelle. La recherche fondamentale peut servir de base à l'élaboration et à la vérification de normes internationales en matière de preuve. La recherche peut expliquer comment le travail pratique d'attribution a débouché sur ces normes. Elle peut également aider à expliquer comment façonner concrètement des mécanismes internationaux d'attribution publique et des réseaux de gouvernance associés pour combler le manque de confiance.

D'autre part, les universités peuvent aussi participer à l'étude des conflits numériques. Les laboratoires universitaires qui possèdent une expertise interdisciplinaire dans le domaine de l'attribution et leur propre base de données pourraient explorer les réalités complexes des conflits cybernétiques. Un consortium d'institutions universitaires menant des recherches autonomes sur le sujet pourrait aider au développement de connaissances publiques sur cette question importante du point de vue social et politique. L'acquisition de connaissances interdisciplinaires dans le domaine de l'attribution et l'intégration de ces connaissances dans la formation de la prochaine génération d'analystes sont deux aspects essentiels pour améliorer la compréhension des conflits numériques.

Florian J. Egloff est chercheur senior en cybersécurité au Center for Security Studies (CSS), intégré à l'ETH de Zurich, et Research Associate au Centre for Technology & Global Affairs de l'université d'Oxford.

Le **Prof. Andreas Wenger** enseigne la politique de sécurité suisse et internationale à l'ETH de Zurich et dirige le Center for Security Studies (CSS), intégré à l'ETH de Zurich.

Les analyses de politique de sécurité du CSS sont publiées par le Center for Security Studies (CSS) de l'ETH Zurich. Deux analyses paraissent chaque mois en allemand, français et anglais. Le CSS est un centre de compétence en matière de politique de sécurité suisse et internationale.

Editeurs: Lisa Watanabe, Fabien Merz, Benno Zogg
Traduction: Interserv; Relecture: Marie Baezner
Layout et graphiques: Miriam Dahinden-Ganzoni
ISSN: 2296-0228; DOI: 10.3929/ethz-b-000340840

Feedback et commentaires: analysen@sipo.gess.ethz.ch
Téléchargement et abonnement: www.css.ethz.ch/cssanalysen

Parus précédemment:

Réduire la complexité du processus de paix en Ukraine No 243
La guerre en Ukraine et la stratégie militaire occidentale No 242
La coopération d'armement PESCO: potentiel et failles No 241
Le rapprochement des deux Corées No 240
Congo: l'alternance dans la continuité No 239
La diffusion des technologies militaires: mythes et réalités No 238