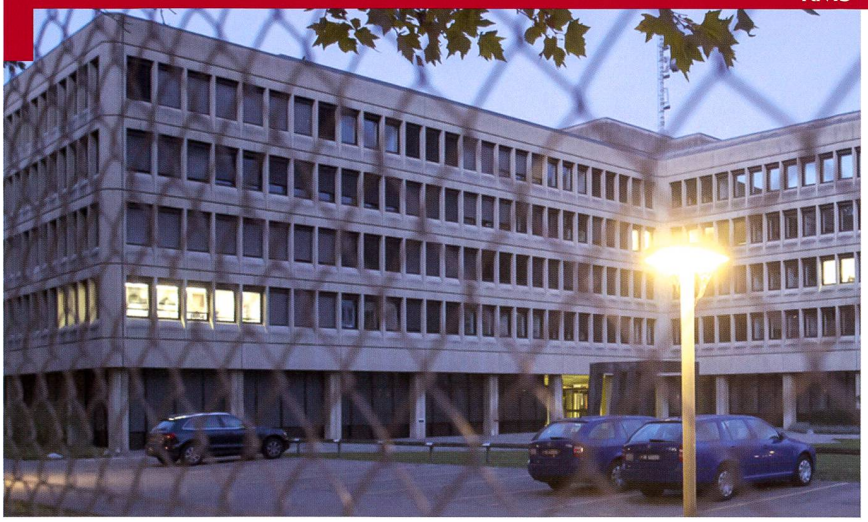
Compétences du SRC en matière d'attribution des cyberattaques



Le siège du Service de renseignement de la Confédération (SRC) à la Papiermühlestrasse 20 à Berne.

Renseignement

Compétences du SRC en matière d'attribution des cyberattaques

Service de renseignement de la Confédération (SRC)

Comme stipulé par la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), adoptée par le Conseil fédéral en 2018, il appartient au Service de renseignement de la Confédération (SRC) d'« *établir l'origine des cyberattaques (attribution) aussi précisément que possible, afin de préserver la marge de manœuvre des autorités politiques et des autorités de poursuite pénale* ». L'accomplissement de cette mission nécessite des compétences très pointues, aussi bien au niveau technique que géopolitique. Le SRC, qui intègre dans ses équipes à la fois des analystes techniques et politiques, est à même de mener à bien ce processus complexe. La tâche de l'attribution nécessite de pouvoir recourir à un large spectre de sources d'informations exclusives, qui sont à disposition du SRC.

En 2019, le SRC a enregistré une hausse sans précédent des cyberattaques d'origine étatique à l'encontre d'intérêts suisses. Alors que de nombreux États déploient des capacités d'espionnage offensives à l'étranger, y compris en Suisse, le SRC se concentre sur les services de renseignement les plus actifs et les plus agressifs contre les intérêts suisses. Dans ce contexte, le processus d'attribution des cyberattaques s'avère primordial, afin de déterminer quels Etats sont à l'origine de cyberattaques sophistiquées, principalement menées à des fins d'espionnage et souvent désignées par l'acronyme APT (« *Advanced Persistent Threats* »). Ces attaques sont conduites directement par des agences de renseignement ou par des groupes guidés et financés par des agences de renseignement.

Dans sa compréhension la plus basique, l'attribution consiste à identifier l'auteur d'un acte et à lui en imputer la responsabilité, autrement dit à répondre à la question « *Who did it* ? ». Concrètement, la réponse à cette question peut résulter de différents niveaux d'analyse. La forme la moins précise d'attribution consiste à désigner un type d'attaquant. On dira par exemple d'une attaque qu'elle est le fait d'un groupe criminel ou d'activistes. A un niveau de précision plus élevé, on cherchera à attribuer une attaque à un groupe d'attaquants (« *Threat actor* »). Un degré d'analyse encore plus pointu permettra de désigner un État comme responsable d'une attaque ou d'une série d'attaques. Parfois même, il sera possible de pointer du doigt une structure organisationnelle spécifique de l'Etat en question, voire des collaborateurs d'une unité spécifique à cet Etat.

Outils à disposition des organes de sécurité suisses

Il est dans la nature humaine de chercher, face à une agression ou à une attaque, à en identifier l'auteur, par curiosité mais également pour comprendre les raisons de cette action. Le processus d'attribution permet de mieux comprendre les motivations des auteurs et leurs modes opératoires, afin de pouvoir se protéger d'attaques ultérieures, de comprendre les stratégies géopolitiques des autres pays et d'engager des mesures de rétorsion.

En Suisse, les organes de sécurité disposent d'une marge de manœuvre pouvant se traduire en fonction du contexte par quatre types de mesures en guise de riposte à une cyberattaque:

- **Mesures basées sur la loi fédérale sur le renseignement:** il s'agit ici de mesures de recherches soumises ou non à autorisation, dirigées contre les entités ayant été identifiées, ou de mesures visant à perturber des systèmes informatiques basés à l'étranger utilisés pour attaquer des infrastructures critiques en Suisse.
- **Mesures judiciaires:** le travail d'attribution, lorsqu'il permet d'identifier précisément des entités ou

personnes, peut conduire à l'ouverture d'une procédure pénale. Le Ministère public de la Confédération (MPC) peut par exemple, sur la base d'un rapport officiel du SRC, décider d'ouvrir une enquête qui sera confiée à la police judiciaire fédérale, en particulier dans des cas d'espionnage politique ou économique.

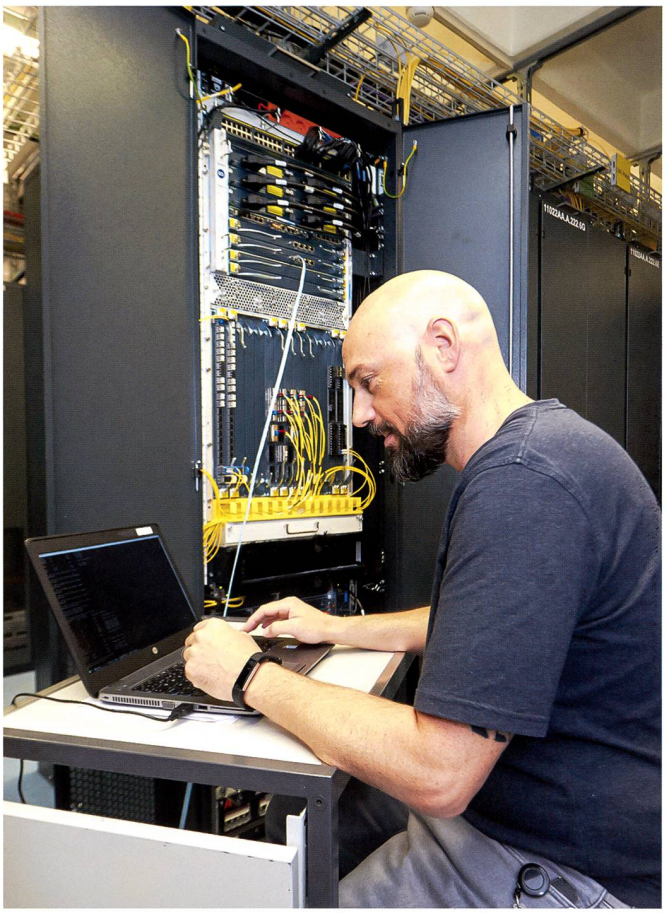
- **Mesures administratives:** toute une série de mesures peuvent être prises contre des individus (principalement des diplomates) ayant été identifiés comme participant à des activités d'espionnage. Il s'agira par exemple d'interdictions d'entrée, de refus de visa ou d'accréditations.
- **Mesures politiques:** un dernier type de mesures est de nature purement politique. Il s'agit par exemple de thématiser la question des cyberattaques ou d'un incident spécifique lors d'une rencontre entre chefs d'Etats ou de convoquer directement un ambassadeur dans ce but. Il peut également être décidé de rendre publique une attribution, c'est-à-dire de désigner par une annonce officielle (par exemple une conférence de presse) un acteur étatique ou un pays comme responsable d'un incident, en fournissant éventuellement les détails techniques et le mode opératoire d'une attaque.

Comment procéder à une attribution

Les méthodes permettant de procéder à l'attribution d'une cyberattaque ont donné lieu à une abondante littérature. S'il n'existe pas à ce jour une unité de doctrine absolue en la matière, les experts s'accordent tout de même sur un certain nombre de points. En premier lieu, l'attribution permet de déterminer un processus, durant lequel différentes compétences et spécialités vont intervenir. Il s'agit tout d'abord d'acquérir des informations, en particulier auprès des victimes, de services partenaires ou encore d'entreprises privées, dont des fournisseurs de service. La majeure partie de ces informations est de nature technique: échantillons de codes malveillants, informations sur l'infrastructure utilisée par l'attaquant (notamment des serveurs de commande et de contrôle), trafic, etc. L'analyse de ces données nécessite des compétences techniques pointues. Il s'agit en particulier de pouvoir relier des indicateurs entre eux et de les associer à des attaques ou à des campagnes déjà connues.

Le travail d'attribution ne se limite toutefois pas à ces aspects techniques. De nombreuses informations utiles peuvent être de nature géopolitique ou concernent les motivations de l'attaquant. Les «*Advanced Persistent Threats*» (APT) sont en effet alignées de manière significative sur les intérêts stratégiques des pays qui les initient, c'est pourquoi il s'agira souvent de partir des victimes pour en déduire les motivations d'un acteur précis, en considérant le contexte géopolitique (conflits, intérêts stratégiques, politique économique, etc.). Pour ce travail, c'est un autre type de compétence qui sera mobilisée, avec des analyses géopolitiques.

SRC



Le SRC exerce des compétences clés en matière d'attribution des cyberattaques. (Photo prétexte)

Rapport de situation 2020 du SRC

La politique internationale en matière de sécurité est aujourd'hui marquée par les rivalités entre plusieurs acteurs qui veulent gagner en influence. Dans ce contexte, les capacités d'anticipation et d'identification précoce du SRC jouent un rôle prépondérant, afin de déceler à temps les menaces et les évaluer, pour ensuite prendre les mesures préventives qui s'imposent. Le rapport annuel du SRC présente les principales évolutions de la situation du point de vue du renseignement. Le code QR ci-dessous vous permettra de télécharger le rapport de situation 2020 du SRC.