ARTICLE EX-POST

Le rôle de la police en ligne dans la prévention et la lutte contre l'extrémisme violent

Vaincre un réseau extrémiste par un autre réseau

Nous ne pouvons pas abandonner le cyberespace aux réseaux extrémistes. Les services de police, déjà très actifs dans la lutte contre l'extrémisme hors ligne, doivent élargir leurs activités au monde en ligne. Les unités de référence sur Internet, l'Unité norvégienne de patrouille en ligne et les agents de surveillance de Facebook montrent aux autres pays la voie à suivre en associant le travail en ligne et hors ligne.

Il s'agit d'un jeu de «notification et d'action», dans lequel l'action ne se limite pas à un démantèlement. Elle recouvre également l'analyse stratégique, la communication et la prévention, et notamment les campagnes contre la haine.

Il est impératif de contrer, interrompre et supprimer les messages qui poussent les individus vers la radicalisation. Dans le même temps, nous avons besoin de messages alternatifs et aussi de messages positifs.

Les services de police bénéficieront largement d'un investissement dans des réseaux associant des ONG et l'industrie de l'Internet.

Cet article a été rédigé par **Steven Lenos et Lieke Wouterse**, membres du Centre d'excellence du RAN.

Introduction

Les réseaux sociaux constituent une force majeure pour les extrémistes. Les services de police qui cherchent à prévenir et à lutter contre l'extrémisme ont tout intérêt à se concentrer sur les activités en ligne. Mais quelles sont les possibilités qui s'offrent à eux? Nous présentons dans ce document certaines approches que les services de police pourraient employer pour contribuer en ligne à la prévention et à la lutte contre l'extrémisme violent sur les réseaux sociaux.

Le présent document s'adresse aux services de police désireux de connaître les moyens dont ils disposent en ligne pour prévenir et lutter contre l'extrémisme violent; il est le fruit de la réunion de RAN POL sur «Le rôle de la police en ligne» qui s'est tenue les 1er et 2 mars, à Oslo.

Après une mise en situation qui insiste sur la nécessité de lutter contre les extrémistes en ligne, ce document aborde les différentes dimensions de la détection et de l'action, ainsi que la compréhension et la prévention. Dans la mesure où les services de police ne peuvent agir seuls, la question de la coopération avec les ONG et l'industrie de l'Internet est également soulevée.

Les enjeux de l'Internet

Plusieurs raisons expliquent l'importance de la présence policière en ligne. Même si le soi-disant califat a perdu son territoire, les idées extrémistes djihadistes se sont répandues et se maintiennent en vie dans le cyber-Califat. Pour Daesh, le djihadisme sur Internet est aussi important que le champ de bataille. En ligne, il soutient le djihadisme physique. Daesh, de même qu'Al-Qaida, utilisent Internet pour propager leur idéologie et diffuser un message de terreur afin de polariser les communautés et de mobiliser, recruter et radicaliser leurs sympathisants.

Les réseaux djihadistes mondiaux ne sont pas les seuls à avoir démontré leur capacité à utiliser les médias sociaux à leur avantage. Les extrémistes de droite aussi. Depuis des décennies, Stormfront, Daily Stormer et d'autres plateformes abritent les clubs numériques et les chambres d'écho des idéologues d'extrême droite et des individus en colère et vulnérables. L'infosphère d'extrême droite est efficace pour faire tourner et encadrer l'information et créer des bulles qui propagent de fausses nouvelles et toute autre propagande mensongère.

L'Internet permet aux groupes et aux individus d'établir des réseaux de personnes partageant les mêmes idées, qui peuvent s'inspirer et se former mutuellement.

L'Institut pour le dialogue stratégique (ISD) a récemment publié un document de recherche intitulé *«The fringe insurgency»* [1] (L'insurrection marginale) qui fait état des réseaux internationaux d'extrême droite: *«Les réseaux d'extrême droite utilisent des ressources militaires et des services du renseignement, comme les documents de communication stratégique du GCHQ et de l'OTAN, pour mener des campagnes contre leurs propres gouvernements. En organisant des opérations sophistiquées à la manière d'opérations psychologiques militaires (ou «psy-ops»), ils cherchent à perturber les processus démocratiques en Europe (...).»*

Les attaques terroristes sont également le fait d'acteurs isolés. Mais ces individus sont en réalité intégrés dans une infosphère et un réseau d'extrémisme. Internet est un vecteur important de radicalisation et d'autoradicalisation. Certains acteurs solitaires commettent leurs atrocités sur instruction, mais d'autres ont simplement été inspirés et agissent plus ou moins seuls. Cette résistance sans chef de file est menée de l'intérieur de la sphère en ligne, parallèlement aux appels à l'action lancés pour les loups solitaires. Les individus peuvent trouver des suggestions de cibles ainsi que des conseils sur la façon d'exécuter des attaques.

https://www.isdglobal.org/wp-content/uploads/2017/10/The-Fringe-Insurgency-221017.pdf

[1] The fringe insurgency. La connectivité, la convergence et l'intégration de l'extrême droite (2018) qui caractérisent les

En place: la surveillance Internet

Les unités de l'UE chargées du signalement des contenus sur l'Internet jouent un rôle central dans l'approche de la police en matière de surveillance en ligne. Les IRU se concentrent sur deux aspects importants de la propagande en ligne: la diffusion et les messages. Il est important de surveiller, de comprendre et d'agir. La surveillance est essentielle pour connaître l'activité des terroristes en ligne, elle aide la police à comprendre ce qui se passe sur Internet et ce qui pourrait se passer dans le monde réel dans un avenir proche.

L'IRU d'Europol est l'un des principaux contributeurs à la base de données des contenus à caractère terroriste connus «Database of Hashes» du Forum de l'UE sur l'Internet, aux côtés des acteurs de l'Internet.

Pour comprendre et référencer les contenus extrémistes ou terroristes en ligne, les IRU utilisent des systèmes semi-automatisés associés à une évaluation humaine. Les investissements dans le développement technologique sont constants. La «buttonologie», c'est-à-dire les outils tels que les programmes de grattage, de balayage et d'évaluation des réseaux, des utilisateurs et des contenus, qui sont nécessaires pour prévenir et lutter contre l'extrémisme violent sur Internet, doit suivre la complexité croissante de l'Internet et des plateformes et technologies utilisées. Mais la technologie seule ne peut pas y parvenir, nous avons aussi besoin de l'intelligence et de l'évaluation humaines, tant pour le développement des outils que pour l'évaluation du matériel en ligne.

Lorsque l'IRU détecte sur Internet des messages ou des personnes attirant son attention, elle peut ouvrir une enquête judiciaire ou demander aux fournisseurs d'accès à Internet de supprimer certains contenus ou de fermer un compte. Les

partenariats public-privé et la coopération avec l'industrie ou d'autres organismes sont donc essentiels en matière de prévention et de lutte contre l'extrémisme violent en ligne.

L'accès à l'expertise d'EUROPOL est possible grâce au portail restreint «Check the Web».

Réduire l'écart entre les activités en ligne et hors ligne

Il existe une interaction continue entre les activités en ligne et hors ligne. Cette constatation se retrouve dans les deux axes de travail de l'IRU Europol, ainsi que dans ceux des IRU nationales. L'un des axes de travail se concentre sur la surveillance et la recherche sur Internet, et sur la prise de mesures lorsque quelque chose est détecté. Il peut s'agir d'une réponse urgente si une menace est imminente, d'un retrait de contenu ou d'une enquête et de poursuites. Le travail d'Europol est accompli de telle manière qu'il peut être exploité dans le cadre de poursuites judiciaires.

L'autre volet de travail consiste à répondre aux demandes de soutien de la part des services de police qui ont besoin d'expertise, d'information ou d'aide en ce qui concerne les activités numériques du suspect pour avoir une meilleure compréhension des messages et de leur diffusion.

La Norvège dispose d'une approche intéressante en matière de réduction de l'écart entre les services de police en ligne et hors ligne. Le Service national des enquêtes criminelles (NCIS) a établi une présence en ligne sur plusieurs plateformes et a mis en place une Cyber patrouille sur Facebook. Celle-ci est dotée d'une page de police Facebook et d'un profil de police Facebook. La page est actuellement active sur Facebook, alors que le profil fait actuellement l'objet de tests.

Cette page Facebook représente une présence policière en uniforme qui mobilise le public de différentes façons. La police apparaît dans un manoir ouvert, en uniforme, préventif, qui peut être comparé à un poste de police physique, où les gens peuvent contacter la police. La page a deux fonctions principales:

1) répondre aux questions et évaluer les renseignements envoyés par le public au moyen de messages personnels.
2) publier des articles avec du contenu sur divers sujets, tels que la prévention de l'extrémisme violent et des conseils pour les jeunes, les parents et les adultes.

Le contenu atteint des milliers de personnes. L'objectif global du projet est de créer une méthode et des orientations pour la police préventive en ligne de Norvège. Sur la base de l'expérience acquise jusqu'à présent, les 12 districts de police de Norvège mettront en place une présence policière préventive en ligne en 2018.

Le profil Facebook consistera en une patrouille de police opérationnelle en ligne. L'objectif est d'assurer une présence ouverte, en uniforme et préventive en ligne. La lutte contre la radicalisation et l'extrémisme violent figurera parmi les domaines prioritaires. Le profil vise à sensibiliser le public aux comportements criminels et/ou inquiétants des groupes fermés et à encourager les administrateurs et/ou les propriétaires de plateformes (en l'occurrence Facebook) à supprimer les contenus illégaux. Le profil de la police fait actuellement l'objet de tests.

La nécessité de comprendre: analyse stratégique et communications stratégiques

Europol et les services de police ont pour ambition de réduire l'écart entre la prévention et les enquêtes. De quelle manière ces deux missions peuvent-elles se soutenir mutuellement? L'observation et la prise de

mesures constituent le cœur de l'activité policière sur Internet. Mais l'effort d'analyse et de compréhension des développements en ligne est tout aussi important. Les extrémistes ont évolué dans leurs façons d'utiliser les messages, mais également dans la technologie utilisée pour les diffuser. Ces changements appellent une prise de conscience de la part des services de police, et ces derniers se doivent au minimum de se tenir au fait des évolutions, voire de prendre une longueur d'avance sur les extrémistes.

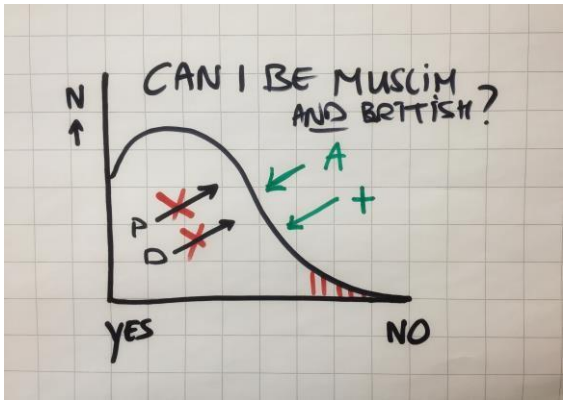
La compréhension des évolutions en ligne passe par la compréhension des évolutions des messages et de leur diffusion. Europol utilise différents

«Le problème de la radicalisation est un problème de communication. C'est une question de perception et de leur transfert vers la réalité par la communication.»
(Hugo McPherson, SCN)

outils d'évaluation technique pour surveiller le cyberespace. Ils sont élaborés grâce au renseignement humain et en coopération avec les entreprises, les unités de référence locales et les universités.

L'analyse des téléphones portables et des ordinateurs portables confisqués appartenant à des individus radicalisés a permis de trouver principalement des contenus non violents, y compris la propagande de Daesh sur la fraternité, l'appartenance et les perspectives dans le califat. Ce qui suggère que ce sont les sentiments d'appartenance et non la séparation qui sont recherchés, ce qui permet de mieux comprendre le type de contenu qui contribue à la radicalisation. Cette connaissance joue un rôle essentiel dans les efforts de prévention, notamment dans la conception de messages alternatifs et de contre-messages.

Comme l'a suggéré le CSN lors de la réunion d'Oslo, la radicalisation peut être appréhendée comme un problème de communication. Les gens adhèrent au djihadisme ou à d'autres formes de propagande en raison de leur perception du monde et du rôle qu'ils y jouent. Nous devrions être en mesure, grâce à la communication, de transformer cette perception en réalité. Un exemple:



La figure ci-dessus illustre de quelle manière une population imaginaire est susceptible d'avoir un éventail d'opinions. À gauche, se trouvent des individus qui sont parfaitement d'accord avec l'idée que quelqu'un puisse être britannique et musulman en même temps [2]. Mais il existe aussi une partie qui pourrait parfois avoir du mal à combiner les deux identités. Et à droite, se trouvent ceux qui croient fermement à la propagande de Daesh qu'il faut choisir: vous ne pouvez pas combiner ces deux identités et vous êtes soit avec Daesh, soit contre Daesh, vous êtes un vrai musulman ou non. De ce côté du spectre, se trouvent les personnes vulnérables à la radicalisation ou au recrutement. L'enjeu que posent non seulement la propagande, mais également les discours haineux et autres messages négatifs et de division, tient au fait qu'ils poussent certaines parties du public cible vers la droite du graphique. Nous devons donc contrer, interrompre et supprimer les messages qui poussent les gens dans la

[2] Cette image peut également être lue comme quelqu'un (mon voisin) pouvant être britannique et musulman en même temps.

mauvaise direction. Parallèlement, il est indispensable de diffuser des messages alternatifs et d'autres messages positifs qui contribuent au glissement vers la gauche du graphique.

Investir dans la résilience en ligne = prévention du crime

Nous ne pourrons jamais supprimer tous les contenus extrémistes en ligne et bloquer toutes les formes de partage entre pairs, qu'ils soient cryptés ou non, sur des forums ouverts ou fermés (sur invitation uniquement). Il est difficile de prouver l'illégalité ou le caractère radicalisateur de certains contenus. Et pourtant, les agents de la radicalisation s'en servent pour guider les individus vers l'extrémisme. De surcroît, en raison de la valeur démocratique fondamentale de la liberté d'expression, il existera toujours des documents en ligne contestés, que certains estiment devoir être supprimés. Pour résumer: des contenus extrémistes resteront toujours disponibles, pour une période plus ou moins longue.

C'est pourquoi, tout en se concentrant sur les contenus et les messagers extrémistes, il est important de travailler du côté du destinataire. Nous devons rendre la société et les personnes vulnérables résilientes. Ce n'est qu'une autre forme de prévention du crime. Ces activités pourraient se dérouler au sein de l'espace précriminel, par exemple dans le domaine de l'éducation aux médias, de la sécurité sur Internet et des communautés résilientes en ligne, avec des messages alternatifs et des contre messages. Et dans cet espace pré-criminel, la police a besoin de partenaires.

L'éducation aux médias et la sécurité en ligne sont des domaines dans lesquels les policiers chargés de la prévention peuvent obtenir des résultats avec les jeunes, leurs parents et leurs enseignants. Les risques qui nécessitent une sensibilisation des parents, des enseignants et des autres personnes qui travaillent avec les jeunes se recoupent énormément. Ainsi, par exemple, la reconnaissance de la propagande, des fausses nouvelles et des théories du complot sont des compétences nouvelles que les jeunes doivent acquérir aujourd'hui. La protection contre la radicalisation et le recrutement pourrait être intégrée dans les formes de prévention reconnues.

Combattre les discours haineux et renforcer la résilience

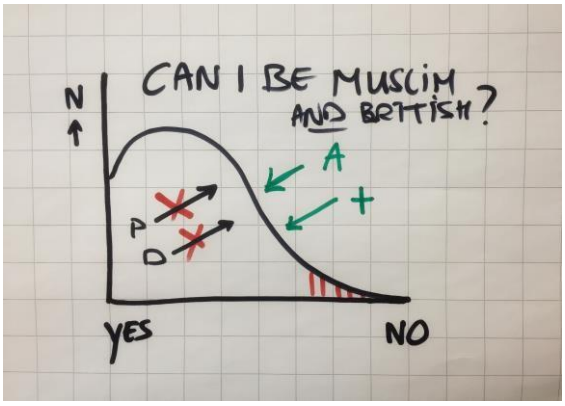
Le discours haineux couvre toute forme d'expression qui répand ou justifie la haine raciale, la xénophobie, l'antisémitisme ou toute forme de haine basée sur l'intolérance, y incite ou en fait l'apologie (définition du Conseil de l'Europe [3]).

La prévention du crime passe par le soutien ou l'engagement dans la lutte contre le discours haineux. Le programme allemand *Helden statt Trolle* (des héros au lieu de trolls) est un projet intéressant sur le thème du discours haineux. Financé par l'UE, il a été lancé par la police du Mecklembourg-Poméranie-Occidentale en coopération avec un institut de la citoyenneté soutenu par l'État. Le projet comprenait des activités en ligne et hors ligne et visait à sensibiliser la police et la société aux discours haineux et aux fausses informations en développant et en formant des méthodes pour contre-réagir. Il a ainsi encouragé la création de communautés en ligne et hors ligne pour lutter contre les discours haineux. Le soutien des services de police aux communautés en ligne qui luttent contre la propagande haineuse équivaut au soutien des services de police aux quartiers et aux propriétaires de

[3] https://www.coe.int/en/web/freedomexpression/hate-speech

magasins qui cherchent à créer un environnement plus sûr et plus résilient.

Combattre et lutter contre le discours haineux soutient les forces qui repoussent la courbe en cloche présentée ci-dessous dans la direction souhaitée: vers la gauche. Nous avons besoin de moins de propagande (P) et moins de messages qui divisent (D) et plus de messages alternatifs (A) et positifs (+).



Une campagne de lutte contre le discours haineux peut mobiliser la résilience de la société et entraîner un plus grand nombre de signalements de ce genre de message et leur retrait des plateformes Internet. Cette mesure assainit le terrain fertile qui est exploité par les recruteurs et les agents de la radicalisation.

Travailler avec les ONG

Les programmes de lutte contre la propagande haineuse illustrent la coopération policière avec les ONG. L'organisation allemande **Jugendschutz.net** va encore plus loin. Cette ONG cherche à protéger les jeunes allemands des contenus dangereux. Cette définition large garantit plus de possibilités d'intervention que celles offertes par les organes juridictionnels. Et alors qu'Europol a pour seul mandat de travailler sur le djihadisme, Jugendschutz peut agir contre tout contenu préjudiciable aux jeunes.

Le projet a été lancé en 2011 avec des activités de lutte contre l'extrémisme de droite; le djihadisme est venu se greffer postérieurement, mais avant que Daesh ne fasse son apparition. L'ONG se concentre sur la surveillance générale et la recherche ciblée. Les individus peuvent également se référer au contenu de Jugendschutz qui leur offre de multiples options. Une ligne d'assistance téléphonique est mise à la disposition pour contacter les services de police, mais des personnes ressources sont également joignables par le biais des fournisseurs de services Internet et des procédures convenues avec les partenaires dans ce domaine. Jugendschutz affiche un taux de réussite de 90 % en ce qui concerne la suppression du contenu après un contact direct avec le délinquant. La police et Jugendschutz se tiennent mutuellement informés des questions opérationnelles.

Pour Jugendschutz, il est plus facile de travailler dans la «zone grise». À quel moment l'humour offensant constitue-t-il officiellement un discours de haine? Jugendschutz recherchera des contenus que la police n'a ni le temps ni le mandat de suivre. Les éducateurs et autres praticiens manifestent un grand intérêt pour ce qui se passe en ligne. Jugendschutz est un partenaire très apprécié de la police qui répond aux besoins des éducateurs et des autres intervenants.

En plus des opérations, Jugendschutz coopère également avec la police en matière de recherche. La collaboration entre les unités de surveillance de l'État et cette ONG est un exemple inspirateur de la façon dont la coopération peut avoir un impact significatif et positif sur la société, avec un effet synergique d'accroissement des résultats.

La police en ligne: styles de communication

La présence en ligne ne suffira pas aux services de police pour communiquer avec le public. En Suède, un petit groupe d'agents a été invité à se connecter en ligne et à interagir avec le public. Dans un premier temps, ils ne sont pas

parvenus à former un public. Mais ils ont fait évoluer certaines choses [4].

Plusieurs éléments peuvent faire une réelle différence. L'utilisation d'images attrayantes et de l'humour peut contribuer au succès de la communication en ligne, en compétition visuelle. Les messages doivent aussi faire appel aux émotions et être perçus comme authentiques. Les messages de la presse policière ne deviendront pas viraux; un policier averti reprochant aux parents de ne pas prendre leurs responsabilités le sera.

Travailler avec l'industrie liée à Internet

La coopération entre, d'une part, la police et les forces de l'ordre et, d'autre part, l'industrie de l'Internet, peut se révéler compliqué. Aucun des deux partenaires ne peut se passer de l'autre, mais il arrive qu'ils ne se tolèrent pas l'un l'autre. Lors de la réunion d'Oslo, RAN POL a découvert que Facebook dispose de plus d'informations sur les utilisateurs que ce qu'on imaginait et que le géant de l'Internet est doté de ses propres compétences et de son personnel dédié à la lutte contre l'extrémisme violent, tout comme les gouvernements et les autorités chargées du respect des lois. Ces équipes mixtes sont composées de personnes d'horizons professionnels différents: ONG, gouvernement et police, par exemple. La présence de locuteurs natifs permet d'évaluer les messages signalés ou référencés du fait que les contextes locaux sont importants. Facebook est équipé de son propre appareil pour contrôler et réajuster sa communauté. De cette façon, l'entreprise essaie de devancer les contenus extrémistes et autres contenus malveillants ou importuns. Elle peut signaler le contenu téléchargé et créer l'équivalent d'une empreinte numérique de celui-ci. Lorsqu'il est à nouveau téléchargé, la machine le reconnaît et le supprime rapidement.

Certains diront que les capacités et les options de Facebook dépassent même les possibilités des gouvernements en matière de surveillance et d'intervention. Ce qui justifie amplement la poursuite de la coopération entre les différents acteurs et le secteur de l'Internet.

Facebook dispose également d'un meilleur équipement et d'une plus grande expertise que les petites entreprises du secteur. Il serait bénéfique pour l'industrie, et pour la société en général, que des entreprises plus solides investissent dans la coopération entre les acteurs de l'industrie Internet.

Le partage de l'information et la coopération dans ce domaine ne sont pas toujours faciles, mais peuvent être améliorés en travaillant avec des personnes ressources désignées et des protocoles convenus.

Vaincre un réseau par un autre réseau

Les extrémistes exploitent les réseaux et les utilisent à des fins criminelles. Leurs sympathisants engagés contribuent à diffuser des messages dans des salles d'écho remplies de fidèles. Pour lutter efficacement contre un tel réseau, la police doit se mobiliser et fonctionner au sein d'un réseau qui lui est propre. Dans le milieu des ONG et de l'éducation, la police peut trouver des partenaires capables d'aider à identifier les contenus non désirés et même de lutter contre ceux-ci ou de faire pression pour leur

[4] http://ktar.com/story/228286/swedish-police-toparents-pick-up-your-drunk-kids/

retrait. L'industrie de l'Internet jouit d'une expertise et d'un accès aux utilisateurs.

Collaborer avec les ONG revient à trouver un terrain d'entente et des objectifs communs. Les ONG ne doivent pas se voir forcées d'adopter les objectifs des services de police et de soutenir leurs missions. Ces derniers doivent adopter une attitude telle qu'ils soient perçus comme des partenaires et des alliés du secteur non gouvernemental.

Par ailleurs, la police et les gouvernements doivent insister auprès de l'industrie de l'Internet pour qu'elle prenne ses responsabilités. Cela passe notamment par la garantie que les installations offertes ne servent pas à promouvoir l'extrémisme ou même à préparer des actes terroristes, et qu'elles ne servent pas à publier du contenu qui alimente le terrorisme et la division.

En matière de prévention et de lutte contre l'extrémisme en ligne, le renforcement des partenariats public-privé avec les plates-formes et les fournisseurs d'accès Internet peut faire une réelle différence.

Messages clés

Outre l'accent mis sur les extrémistes, leur contenu et leurs activités, la police doit contribuer à la résilience en ligne.

Vaincre un réseau extrémiste passe par un autre réseau. La police doit établir des partenariats avec les ONG et l'industrie de l'Internet.

Les unités de référence Internet, l'Unité norvégienne de patrouille en ligne et les agents de surveillance de Facebook montrent aux autres pays la voie à suivre en associant le travail en ligne et hors ligne.