08/03/2021

DOCUMENT DE CONCLUSION

Évènement en petit comité du RAN - Les acteurs isolés numériques
24 février 2021, 15h00-18h00 ECT, en ligne

Terroristes numériques et «acteurs isolés»

Principaux résultats

Comment détecter et identifier les «acteurs isolés» du terrorisme numérique avant qu'ils ne commettent des actes de violence, telle était la principale question de cette réunion d'experts. Un accent particulier a été mis sur le rôle et les fonctions des plateformes de médias sociaux et des plateformes de jeux. Le terme «acteur isolé du terrorisme» est devenu au fil du temps un concept controversé et déroutant. Bien que certains individus puissent agir seuls au niveau opérationnel, ils font, et se perçoivent généralement comme faisant partie d'un groupe ou d'un mouvement spécifique. En particulier à l'ère du numérique, ces soi-disant «acteurs isolés» ne sont et ne se sentent généralement ni isolés, ni seuls. Si certains «acteurs isolés» et auteurs d'attaques n'adhéraient à aucun groupe par crainte d'être placés sous surveillance par le gouvernement, ils se percevaient comme faisant partie d'un collectif uni par des valeurs, des actions et des ennemis partagés. Le procès de l'auteur de l'attaque de Halle (2020) et le rapport de la commission de Christchurch(2020) ont fait ressortir que ni les services de renseignement, ni les forces de l'ordre, ni l'industrie de la technologie ne savaient où chercher ces acteurs isolés numériques ou comment les identifier en ligne. Les connaissances sur les fonctionnalités de base (et les abus) des plateformes, des sites Internet et autres services en ligne utilisés par les auteurs en dehors de Facebook, YouTube et Twitter, étaient à l'époque limitées.

Certaines des principales conclusions de la réunion sont les suivantes:

- Les acteurs dits isolés ne sont ni ne se sentent généralement isolés ou seuls. Le mythe du «loup solitaire» est ici inexact et potentiellement nuisible car il sous-estime les milieux et les réseaux informels qui fournissent un soutien idéologique, moral et parfois logistique aux auteurs d'attaques.

- Recherchez les signes avant-coureurs significatifs qui auraient pu indiquer qu'un individu se préparait à commettre un acte violent, par exemple la publication de contenus relayant le discours haineux ou de manifestes décrivant une menace existentielle pour son groupe et justifiant ou appelant à la violence; le partage ou la recherche active d'instructions de fabrication d'armes artisanales; l'expression d'un «besoin d'agir»; l'interruption de relations avec des personnes que l'individu considère inférieures en raison de leur couleur de peau, de leurs croyances, de leur sexe ou d'autres attributs.

- Il est nécessaire de financer des recherches (à court terme) orientées sur l'élaboration de politiques ainsi que des projets axés sur les groupuscules numériques au sein desquels des acteurs isolés numériques potentiels pourraient être actifs.

Cet article décrit dans un premier temps les défis qui ont été discutés à partir des différentes perspectives partagées. Dans un deuxième temps, il expose plusieurs recommandations à l'attention des praticiens et des décideurs.

Points forts de la discussion

Les experts sur le sujet ont présenté les défis suivants:

- **Les acteurs isolés ne sont pas seuls:** Les acteurs dits isolés ne sont ni ne se sentent généralement isolés ou seuls. Le mythe du «loup solitaire» est ici inexact et potentiellement nuisible car il sous-estime les milieux et les réseaux informels qui fournissent un soutien idéologique, moral et parfois logistique aux auteurs d'attaques. Dans plusieurs cas, des auteurs qui avaient été qualifiés d'acteur isolé/loup solitaire se sont en fait avérés faire partie d'un mouvement ou d'un collectif non organisé. Une interprétation erronée de ce phénomène peut conduire à une mauvaise compréhension de l'ampleur et de la portée de la menace.

- **"La désinformation n'est pas un phénomène nouveau:** Le rôle de la ludification dans le contexte des actes de terrorisme commis par des acteurs isolés est potentiellement surfait, dans la mesure où le cadre psychologique qui entoure la promotion et les récompenses dans un climat de concurrence est une pratique courante dans ces groupes (extrémistes/terroristes). Il n'existe jusqu'à présent aucune preuve scientifique d'un lien entre les jeux en ligne (y compris les jeux de tir en vue subjective) et la violence physique ou des comportements extrémistes/terroristes.

- **Le manque de gouvernance sur les plateformes de jeu crée un espace pour les extrémistes:** Certaines plateformes/forums de jeux font office de lieux de rencontre, de relais de propagande et de terrains de recrutement pour les extrémistes et les terroristes. La plupart de ces services ne disposent pas de systèmes de gouvernance et de modération efficaces, ce qui en fait des cibles faciles pour les acteurs extrémistes et terroristes, ainsi capables d'atteindre des publics spécifiques.

- **Marge d'amélioration pour les entreprises de médias sociaux:** Les grandes plateformes de médias sociaux soulignent l'importance de leur investissement dans des outils et des procédures de modération de contenu, mais avertissent qu'en raison des questions relatives à la liberté d'opinion et de la quantité de données, leur efficacité reste limitée. Dans le même temps, toutes les données des utilisateurs sont constamment traitées et analysées, servant le modèle commercial global de la plateforme qui consiste, à des fins publicitaires, à vendre l'accès aux profils d'utilisateurs à des tiers. Cela indique que les entreprises de médias sociaux pourraient «en savoir» plus (ou en apprendre plus) qu'ils ne le font actuellement sur les acteurs extrémistes et terroristes qui font une utilisation abusive de leurs services.

- **Peut-on prévoir un comportement violent?** La question de savoir quel comportement en ligne pourrait signaler ou indiquer de futurs actes violents de la part d'individus qui expriment un comportement extrémiste en ligne, par rapport à ceux qui ne font que «faire semblant», a été abordée sous différents aspects:

    - «La fuite» - De nombreux acteurs isolés avaient prévenu de leurs actes leur famille et leurs amis ou sur des plateformes de médias sociaux ou des sites Internet spécifiques. Comment pourrait-on traiter ces informations plus rapidement?

    - Les outils d'évaluation des risques - L'utilité des outils d'évaluation des risques, conçus principalement pour intervenir auprès de personnes déjà connues, tels que VERA-2R, TRAP-18, ERG22+, et de l'outil RADAR-iTE, qui vise l'identification d'acteurs isolés numériques «inconnus», devrait être explorée plus avant.

- Tirer profit des outils d'évaluation des risques d'automutilation (expériences psychiatriques) - Les expériences tirées des outils d'évaluation des risques d'automutilation pourraient permettre une identification précoce de comportements potentiellement violents. Cela n'implique pas que les acteurs isolés ont nécessairement des problèmes de santé mentale et, s'ils en ont, que ceux-ci sont liés de manière causale aux actes terroristes qu'ils commettent.

- La désintégration des facteurs de protection - Le monde en ligne peut aider les «acteurs isolés» à établir des liens sociaux numériques les maintenant dans un espace émotionnellement sûr. Un sentiment d'urgence à agir peut survenir suite à une rupture des facteurs de protection ou être déclenché par des récits apocalyptiques véhiculant l'existence d'une menace existentielle (par exemple le «grand remplacement»/le «génocide blanc»/la «guerre contre les musulmans»), motivant l'individu à passer de victime à auteur ou à se percevoir comme étant un «héros».

- **La surcharge d'informations:** Faire la différence entre le bruit et les signaux pertinents est de plus en plus difficile, car les paysages numériques extrémistes se diversifient et le rôle des organisations s'affaiblit, en particulier dans le cas de l'extrémisme violent de droite, comparé à l'extrémisme et au terrorisme islamistes.

- **Des paysages numériques changeants:** La déplatformation des contenus extrémistes/terroristes par les grandes plateformes de médias sociaux conduit à une perpétuelle évolution des paysages numériques. Les acteurs extrémistes/terroristes se dirigent souvent vers les petits médias sociaux et les plateformes de partage de vidéos ou les services de messagerie tels que les forums Telegram et Chan, entre lesquels ils se déplacent. Ces services numériques sont souvent moins pris en compte dans les entreprises de prévention et la lutte contre l'extrémisme violent par les praticiens.

- **Un support spécialisé:** De nombreux praticiens de la P/CVE opérant en ligne peuvent ne pas avoir la compréhension approfondie nécessaire des diverses sous-cultures (potentiellement) extrémistes, de leur utilisation du langage, de l'humour, des mèmes et d'autres types de «signalisation tribale». Les organisations de la société civile (OSC) spécialisées peuvent fournir les informations nécessaires à l'analyse et à la sensibilisation numérique (par exemple concernant le travail de rue numérique).

Recommandations

Les recommandations adressées aux praticiens sont les suivantes:

- Lorsque vous travaillez avec un individu, ou la famille d'un individu signalé comme étant un acteur isolé, **assurez-vous de faire les recherches et d'acquérir la compréhension nécessaires sur leur environnement social (en ligne)** et de leurs pairs, pour éviter toute erreur d'interprétation concernant leurs motivations, leurs valeurs et la structure qui les soutient. **Tirez des enseignements des débriefings, des essais et des recherches** sur les éléments à explorer afin d'avoir une vue d'ensemble. Idéalement, certains praticiens (sources crédibles) devraient avoir la possibilité de **prendre part aux conversations**.

- Assurez-vous de **bien comprendre les tendances, les sujets, les mèmes, les insignes et les marques pertinents actuellement utilisés dans les milieux extrémistes (en ligne)** avec lesquels vous interagissez, en contactant des organisations de la société civile et des chercheurs spécialisés dotés de l'expertise et de l'expérience nécessaires. Il est important de former les praticiens, tels que les policiers et les éducateurs, à la compréhension de l'humour et du langage spécifiques utilisés en ligne.

- Recherchez les **signes avant-coureurs particuliers** pouvant indiquer qu'une personne se prépare à commettre un acte violent, tels que:

    - la publication de contenus relayant le discours haineux ou de manifestes décrivant une menace existentielle pour son groupe et justifiant ou appelant à la violence;

    - le partage ou la recherche active d'instructions de fabrication d'armes artisanales;

    - l'expression d'un «besoin d'agir»;

    - l'interruption de relations avec des personnes que l'individu considère inférieures en raison de leur couleur de peau, de leurs croyances, de leur sexe ou d'autres attributs.

Aux fins de l'identification des signaux numériques d'acteurs isolés potentiels, **vérifiez** si les **outils d'évaluation des risques** existants tels que VERA-2R, TRAP-18, ERG22 + ou RADAR-iTE pourraient être utiles ou devraient être modifiés. Les recommandations adressées aux décideurs sont les suivantes:

- **Assurez-vous que les milieux et mouvements extrémistes/terroristes numériques susceptibles de guider et de motiver un acteur isolé sont appréciés avec discernement et bien compris.** Une incompréhension des attaques d'acteurs isolés comme des actions déconnectées et isolées d'individus peut conduire à des statistiques trompeuses et à une évaluation incomplète des menaces.

- **Donnez la priorité au financement de recherches (à court terme) orientées sur l'élaboration de politiques** ainsi que de projets axés sur l'identification des groupuscules numériques au sein desquels des «acteurs isolés» numériques potentiels pourraient être actifs, c'est-à-dire sur la cartographie des acteurs permettant de comprendre les connexions internationales et l'examen des conversations sur différentes plateformes pour identifier les «acteurs isolés» potentiels et repérer les discours importants, significatifs et pertinents pour ces acteurs en ligne. Ces recherches peuvent être menées de manière anonyme, afin d'identifier les tendances et les conversations sur ces plateformes.

- **Poursuivez le dialogue et faites pression sur les entreprises de médias sociaux, de partage de vidéos et de jeux en ligne** non seulement en matière de déplatformation des contenus terroristes, mais aussi d'identification proactive des potentiels acteurs isolés du terrorisme. Les plateformes et les chercheurs en ligne devraient mettre au point des indicateurs, notamment des signaux de discours haineux, permettant de prédire les comportements, et examiner leur interaction avec d'autres indicateurs

afin d'étudier des modèles de comportement au fil du temps, c'est-à-dire une éventuelle escalade de ces comportements permettant d'identifier des acteurs isolés.

Investissez dans des **modules d'apprentissage entre pairs** structurés et continus qui facilitent l'échange des enseignements tirés entre les acteurs concernés (OCS/chercheurs/gouvernement/entreprises).

Pratiques pertinentes

Plusieurs pratiques ont été présentées:

Les interventions en ligne 1-2-1 de l'Institute for Strategic Dialogue constituent une approche expérimentale conçue pour combler les lacunes en matière de tentatives systématiques de soutien des efforts de contre-discours par le recours à la messagerie instantanée et à des interventions à grande échelle. Actuellement disponible sur Facebook et axé sur les idéologies d'extrême droite et islamistes, ce programme offre aux individus montrant des signes clairs de radicalisation l'occasion de rencontrer et de s'entretenir avec un intervenant apte à les aider à se sortir de cette spirale haineuse.

La méthode de redirection développée par MoonshotCVE et employée par Facebook et Google peut servir d'inspiration. Cette méthode est conçue pour lutter contre l'extrémisme violent et les organisations dangereuses en redirigeant vers des ressources éducatives et des groupes de sensibilisation les utilisateurs ayant saisi des termes de recherche liés à la haine ou à la violence. Un projet pilote du programme a été lancé avec les partenaires de prestation Life After Hate (États-Unis) en mai 2019 et avec Exit Australia en septembre 2019.

Le projet «Good Gaming - Well Played Democracy» de la Fondation Amadeo-Antonio en Allemagne combine l'analyse des sous-cultures de jeu du point de vue de la P/CVE avec un travail de rue numérique, par l'établissement de contacts avec des joueurs en ligne afin de les sensibiliser à l'effet préjudiciable des mythes du complot. Ce projet forme également des enseignants, des travailleurs sociaux et des influenceurs sur ces questions.

Suivi

Un échange structuré et continu entre les experts travaillant sur les milieux des acteurs isolés numériques et les agents du travail de sortie, expérimentés dans les interventions en ligne, pourrait permettre de réunir des informations pratiques supplémentaires sur la façon de comprendre, de prévenir et de lutter contre ce phénomène en développement et en évolution. Un événement transversal intitulé «Lone actors – jointly taking stock of recent developments and combining knowledg» («Acteurs isolés - bilan conjoint des développements récents et combinaison des connaissances») et un webinaire sur intitulé «Digital Terrorist/Lone Actors » («Terroristes numériques/acteurs solitaires») assureront le suivi de cette réunion en vue de stimuler davantage la sensibilisation à cette thématique.