**Criminologie**

# Nouvelles technologies et cyberharcèlement : l'exemple du *swatting*

## New technologies and cyberstalking: Swatting as an example

## Nuevas tecnologías y ciberacoso: el ejemplo del *swatting*

Nicolas Estano

La criminologie de l'information : état des lieux et perspectives
Volume 52, numéro 2, automne 2019

URI : https://id.erudit.org/iderudit/1065854ar
DOI : https://doi.org/10.7202/1065854ar

Aller au sommaire du numéro

Éditeur(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (imprimé)
1492-1367 (numérique)

Découvrir la revue

Citer cet article

Estano, N. (2019). Nouvelles technologies et cyberharcèlement : l'exemple du *swatting*. *Criminologie*, *52* (2), 13–32. https://doi.org/10.7202/1065854ar

Résumé de l'article

Cette contribution tentera d'établir un état des lieux d'un phénomène qui s'est développé au cours des cinq dernières années en Europe, mais qui existe depuis une quinzaine d'années aux États-Unis, notamment chez les utilisateurs de jeux en ligne, à savoir le *swatting*. Les faits survenus en décembre 2017 à Wichita, au Kansas (États-Unis), où un homme trouva la mort viendront illustrer les potentialités dramatiques de cette pratique, présentée généralement par les auteurs comme un simple canular téléphonique. Nous tenterons à travers cet article de définir ce qu'est le *swatting*, ce que cela recouvre, quelles sont ses implications en termes de sécurité, les risques et enjeux qui y sont liés ainsi que les types de conduite qui y sont associés.

# Nouvelles technologies et cyberharcèlement : l'exemple du *swatting*

Nicolas Estano[1]
*Psychologue clinicien*
*Unité de psychiatrie et de psychologie légales*
*C.R.I.A.V.S. Pôle Paris Nord-Est*
*Expert près la Cour d'appel de Paris, France*
*nicolas.estano@gmail.com*

**RÉSUMÉ** • *Cette contribution tentera d'établir un état des lieux d'un phénomène qui s'est développé au cours des cinq dernières années en Europe, mais qui existe depuis une quinzaine d'années aux États-Unis, notamment chez les utilisateurs de jeux en ligne, à savoir le* swatting. *Les faits survenus en décembre 2017 à Wichita, au Kansas (États-Unis), où un homme trouva la mort viendront illustrer les potentialités dramatiques de cette pratique, présentée généralement par les auteurs comme un simple canular téléphonique. Nous tenterons à travers cet article de définir ce qu'est le* swatting, *ce que cela recouvre, quelles sont ses implications en termes de sécurité, les risques et enjeux qui y sont liés ainsi que les types de conduite qui y sont associés.*

**MOTS CLÉS** • Swatting, *cyberharcèlement, tétrade noire,* spoofing.

## Introduction

L'Union internationale des télécommunications (UIT) évaluait en 2018 à 51,2 % la part de la population mondiale à utiliser Internet. Dans les pays dits développés, cette proportion serait de 80,9 %, tandis que seulement 45,3 % de la population des pays en voie de développement aurait accès à Internet. En tout, près de 96 % de la population mondiale serait couverte par des réseaux cellulaires permettant l'usage de téléphones intelligents et d'autres objets connectés. L'augmentation de la population utilisatrice a cependant entraîné un accroissement des

1. EPS de Ville-Evrard, 202, avenue Jean Jaurès, 93332 Neuilly-sur-Marne, France.

données partagées et attiré les délinquants à l'affût de nouvelles opportunités. Celles-ci peuvent prendre la forme d'activités criminelles classiques comme, par exemple, l'observation des statuts estivaux des utilisateurs de réseaux sociaux qui facilite la planification de cambriolages (Roberts, 2010). Le partage de données soutient également une cybercriminalité financièrement motivée (*phishing*, fraude, etc.), voire l'exploitation sexuelle à des fins mercantiles et pornographiques de femmes et d'enfants. La toile est aussi le lieu de comportements hétéroagressifs comme le *trolling*, les conflits entre célébrités cherchant à faire parler d'elles, et les situations plus problématiques de cyberharcèlement qui prolongent dans la sphère virtuelle les comportements de brimades vécues dans le réel au sein des établissements scolaires.

Nous nous intéresserons dans cette communication à un type de cyberharcèlement particulier, le *swatting* (Jaffe, 2016). Présent aux États-Unis depuis le début des années 2000 et apparu au cours des cinq dernières années en Europe, le *swatting* consiste à faire un appel téléphonique à une unité de police ou à la gendarmerie pour y signaler la survenue d'un événement (p. ex. : une prise d'otages ou une situation impliquant un forcené retranché) au domicile d'un individu (la cible de l'usurpation d'identité) dans le but qu'une unité d'intervention s'y rende et y intervienne.

## 1. Définition et état des lieux

Une recherche du terme *swatting* dans les bases de données en libre accès, dans le domaine des sciences humaines (notamment Medline, Cairn Info, ResearchGate, ScienceDirect, etc.), n'offre que très peu de résultats, et même aucun résultat en langue française. Que désigne-t-on par ce phénomène, visiblement peu investigué par les chercheurs, et présenté par leurs auteurs comme un canular ?

Le terme *swatting* fait référence à « SWAT » (pour Special Weapons and Tactics), le service d'intervention policier aux États-Unis, dont l'équivalent en France est le Groupe d'intervention de la gendarmerie nationale (GIGN) ou la Brigade de recherche et d'intervention (BRI), et au Canada, le Groupe tactique d'intervention (GTI). À la suite de l'appel d'urgence fait par l'auteur du *swatting*, les forces de l'ordre dépêchent une unité d'intervention sur les lieux. La fausse situation d'urgence et la non-nécessité d'y avoir dépêché une équipe d'intervention sont constatées sur place. La personne visée par ce canular, quant

à elle, voit une unité policière arriver chez elle, la mettre en joue et la maîtriser avant que la dimension factice de l'appel ne soit finalement découverte.

Pour réaliser ce canular téléphonique, l'auteur doit d'abord obtenir les informations personnelles de la personne visée. Il peut y parvenir grâce à ses compétences techniques, notamment par l'utilisation de l'ingénierie sociale, soit la manipulation d'autrui dans le but d'obtenir des informations sur une personne (mots de passe, données, etc.) et le piratage, ou grâce à des compétences technologiques lui permettant de réaliser une usurpation d'identité (*spoofing*). Cela consiste, pour le pirate informatique, à s'intercaler entre deux parties, au moyen de la mystification de l'identité de l'appelant (*Caller ID spoofing*), et à modifier le numéro d'appel de l'émetteur. L'usurpation de l'identité de la personne ciblée, qui sera perçue par le récepteur (généralement un service d'urgence) comme étant authentique, provoquera le dépêchement sur les lieux de l'équipe d'intervention. Auparavant coûteuses en termes de matériel et de connaissances techniques, ces actions qui visent à usurper des lignes d'appel sont maintenant largement diffusées et accessibles grâce à des logiciels en source ouverte. Il arrive même que des pirates informatiques louent leurs compétences dans des cas de harcèlement par procuration.

Dans le milieu des joueurs en ligne, l'imminence d'un *swatting* serait désignée par le nom de code « livrer des pizzas »[2]. Cette livraison, parfois diffusée en ligne à la future victime et à l'auditoire, lui laisserait savoir qu'elle est « mat ». L'intervention des forces de l'ordre au domicile d'un adversaire a ainsi pour but d'établir une domination symbolique. S'il arrive que l'intervention (et la terreur de la personne) soit diffusée en direct à l'intention des autres membres de la communauté, ces activités ne sont pas l'apanage des joueurs en ligne. Plusieurs artistes ont en effet été victimes de *swatting* aux États-Unis (dont Miley Cyrus, Ashton Kutcher, et Justin Timberlake) (Duke, 2013).

Les conséquences psychologiques du *swatting* chez les victimes et les proches présents sont variables. Ceux-ci peuvent, après avoir vu les forces de l'ordre intervenir comme si un preneur d'otage était réellement sur les lieux, avoir la perception de s'être fait avoir mais aussi vivre un

2. Les vidéos et forums évoquant ces canulars font référence à la livraison de pizza (chez des personnes qui n'ont rien demandé), laquelle est historiquement le premier type d'usurpation d'identité (*spoofing*). Ce terme est resté mais désignerait désormais le *swatting* (Sellami, 2016).

réel traumatisme psychologique. Être confronté à un danger de mort qui fait irruption dans l'espace intime et bien réel du sujet est susceptible d'engendrer un (psycho)traumatisme.

Les conséquences de ce type de canular peuvent être importantes. Si la plupart des interventions se terminent par un bris de porte ou une frayeur, on rapporte dans certains cas des blessures plus sérieuses[3]. Les événements de Wichita, au Kansas (États-Unis), survenus le 28 décembre 2017, ont même entraîné la mort d'une personne. Les répercussions observées sur le plan humain vont donc du psychotraumatisme à la mort de la personne *swattée*, abattue au cours de l'intervention.

Les intervenants policiers peuvent aussi être considérés comme des victimes secondaires. En effet, la prise de conscience d'avoir été manipulés et d'avoir potentiellement mis en danger la vie d'un civil peut engendrer une situation fragilisante chez les policiers.

Mais quels sont les objectifs des auteurs de ces canulars téléphoniques ? Les médias avancent notamment un désir de démontrer leur habileté technique en multipliant les fausses alertes et en causant subséquemment l'engorgement des services d'urgence (Sellami, 2016), ou encore celui d'être spectateurs, auditifs ou visuels, de la stupéfaction des protagonistes, tant du côté de la victime que des forces de l'ordre[4]. Cela renverrait à une forme de pulsion scopique, le plaisir fondé sur la vue (lorsque des webcaméras sont disponibles) et sur l'audition (lorsque les micros des téléphones ou des ordinateurs sont activés). Les réactions positives de la communauté des joueurs pourraient contribuer au trait de personnalité « renarcissisant » des auteurs, qui cherchent à prouver leur maîtrise à un auditoire plus ou moins acquis à leur cause ou, en tous les cas, en attente de ces « affrontements ». Il s'agirait possiblement d'une vengeance ou d'une tentative de nuire à la personne ciblée, ce qui leur procurerait du plaisir devant les émotions ou la sidération affichées par les victimes et à entendre les policiers se rendre compte de la supercherie. Le cas de la fausse alerte de l'attentat du 17 septembre 2016 à l'église Saint-Leu de Paris (Burel, 2016) en est l'illustration parfaite, l'auteur des faits et ses complices s'étant réjouis sur les réseaux sociaux du nombre de policiers mobilisés ce jour-là.

3. Voir, par exemple, les cas de Tyran Dobbs ou de Nathan Hanshaw dans Jaffe (2016).

4. Voir Spacebound (2016) pour des illustrations de *swatting* réalisé aux États-Unis chez des joueurs en ligne.

En France, l'ampleur du phénomène est difficile à estimer[5] en l'absence de collectes de statistiques précises sur le sujet, mais il a déjà conduit à des interpellations et à des condamnations (voir les études de cas plus loin). Aux États-Unis, le Federal Bureau of Investigation (FBI) a émis dès 2008 des recommandations sur les précautions à prendre si l'on suspecte être la cible de *swatting* (FBI, 2008). De 2002 à 2006, l'organisation américaine rapporte que cinq *swatters* ont appelé le 911 dans plus de soixante villes, et que le coût imputé aux premiers répondants a atteint 250 000 $. En 2013, les situations de *swatting* étaient évaluées à environ 400 par an, le coût financier de chacune de ces interventions étant estimé à 10 000 $ (Jeffries, 2013). Les poursuites, pour ce qui est considéré comme un délit et non un crime, se font sur le plan local et non fédéral, ce qui explique l'absence de statistiques précises du FBI. Entre 2015 et 2017, Katherine Clark, une élue à la Chambre des représentants des États-Unis, propose le projet de loi « Interstate Swatting Hoax Act ». Celui-ci, qui visait à faire du *swatting* un crime de ressort fédéral, compte tenu du fait que ces actions se déroulent dans différents États, n'est toutefois pas adopté. En France, le *swatting* est passible de poursuites dans le cadre d'un délit de fausse alerte, les auteurs encourant jusqu'à deux ans de prison et 30 000 € d'amende (Ministère de l'Intérieur, 2018), selon l'article 322-14 du Code pénal, sur « le fait de communiquer ou divulguer une fausse information dans le but de faire croire qu'une destruction, dégradation ou détérioration dangereuse pour les personnes va être ou a été commise ».

## 2. Ancrage théorique

La rareté des données sur le sujet nous amène à nous concentrer principalement sur des études de cas à partir des éléments parus dans la presse et des quelques décisions de justice rendues relatives à ces infractions. Mais avant de présenter ces études de cas, nous aborderons les notions et les conduites qui y sont intrinsèquement liées et pour lesquelles des publications existent.

Le développement d'Internet ces dix dernières années a offert au plus grand nombre un accès illimité à des produits et services, à des boîtes courriel et au stockage de données. Une quantité impressionnante de

5. Une sollicitation faite dans le cadre de cet article auprès du secrétaire d'État, qui a transmis la demande aux directions centrales de la police et à la gendarmerie, est restée sans réponse.

données personnelles s'est ainsi retrouvée disséminée sur la toile, permettant par conséquent l'apparition du cybercrime. Les éléments facilitant les infractions sont nombreux : du côté de la victime, la non-protection de ses données et les fragilités des systèmes ; du point de vue de l'auteur, la perception de la distance entre la cybervictime et lui, et l'immatérialité de l'action qui peuvent créer une forme de déresponsabilisation. Et comme il a été mentionné précédemment, l'auteur du *swatting* a la capacité de récupérer un grand nombre de données relatives à sa future victime par différents moyens à sa disposition. Sur le plan technologique, notons également l'automatisation de certaines infractions, comme le vol d'une somme minime répété sur plusieurs machines, qui passe inaperçue et qui maximise les gains (Herzog-Evans, 2010). En outre, la mondialisation du cybercrime soulève la question des compétences territoriales spécifiques[6].

Le développement des sites de réseautage social (SRS) a été témoin de nouvelles atteintes, comme le cyberharcèlement[7] (cyberintimidation) et la manipulation à visée sexuelle ou pédopiégeage. Les notions de harcèlement et de cyberharcèlement permettent-elles de comprendre la dynamique à l'œuvre dans le *swatting* ? Selon Meloy (1998), le *stalking*[8] comprend trois critères : 1) des comportements intrusifs sur un tiers qui ne le désire pas ; 2) des comportements implicitement ou explicitement menaçants ; et 3) les conséquences de ces conduites sur la personne visée, qui éprouve une peur importante et régulière (p. 2). Ce comportement reposerait sur des mécanismes de suivi obsessionnel mal intentionné, des menaces et du harcèlement à long terme (Meloy et Gothard, 1995). Bien que son ouvrage soit limité à la technologie en vigueur à l'époque de sa rédaction, lequel consistait surtout en l'envoi de courriels et d'appels obscènes, Meloy (1998) décrit avec justesse les mécanismes psychodynamiques du *cyberstalking*. Dans le cadre du cyberharcèlement, Internet favoriserait la communication avec une autre personne sans aucune des contraintes de la réalité sociale.

> Premièrement, le manque de restrictions sociales signifie que l'anxiété, particulièrement en tant qu'inhibiteur de l'agressivité, est inexistante (…)

6. Pour une discussion juridique, qui ne fait pas l'objet de cette communication, voir Bernstein (2016), Blanch et Hsu (2016) et Brumfield (2014).

7. En anglais : *cyberstalking*, *cyberbullying*, *cyberharassment* et *grooming*.

8. Meloy (1998) emploie le verbe « *to stalk* », qui définit une action ou une conduite comportementale. La traduction la plus proche serait la traque ou la chasse, mais le concept de *stalking* se rapproche de la notion de harcèlement en France.

> les pulsions agressives que cela engendre à déprécier, humilier ou insulter peuvent être grossièrement et directement exprimées à la cible. Deuxièmement, l'absence de stimuli sensoriperceptifs de la personne réelle signifie que le fantasme peut jouer un rôle d'autant plus expansif dans l'origine des comportements du harceleur. Les cibles deviennent facilement accessibles et des réceptacles pour ses projections, les fantasmes narcissiques faisant le lien peuvent être la scène d'un rejet du monde réel, l'humiliation et la rage. (Meloy, 1998, p. 11, notre traduction)

Suler (2004) énumère plusieurs facteurs psychologiques pouvant conduire à cette désinhibition de l'agressivité en ligne : l'anonymat (plus ou moins réel) que procure un pseudonyme, l'invisibilité face aux autres, le court laps de temps entre l'envoi du message et la réception du *feedback*, le sens exagéré de soi du fait d'être seul à son clavier et le manque d'une figure d'autorité en ligne. Il précise que « les différentes modalités de communication en ligne (chat, email, vidéo) et différents environnements (sociaux, fantasmatiques, professionnels) peuvent faciliter les différentes expressions du Soi » (p. 325).

Quelles seraient les principales caractéristiques de la personnalité des individus s'adonnant à des rapports conflictuels sur Internet ? Le développement des moyens de communication de type chat et l'expansion des réseaux sociaux ont créé de nouvelles attentes chez les utilisateurs. La réputation numérique devient une part de la réputation générale de l'individu, qui peut être considérée comme une « prothèse narcissique ». Celle-ci comblerait les failles de l'image de soi par l'intermédiaire des approbations obtenues par les likes et les retweets (Gozlan, 2013). La valeur conférée à cette opinion partagée en ligne permettrait de lutter contre de possibles éléments dépressifs. Mais de nouvelles opportunités s'offrent aussi aux auteurs de comportements déviants. Le cyberharceleur se sert d'Internet pour harceler, observer et susciter l'angoisse chez sa ou ses victimes. Il a désormais la possibilité de voir leurs réactions en direct. Selon Bocij et McFarlane (2002), le cyberharcèlement est le fait pour un individu :

> d'utiliser les technologies de l'information et de la communication dans le but de harceler une ou plusieurs personnes. Les comportements de l'individu peuvent inclure (…) des menaces et des allégations mensongères, le vol d'identité et de données, des atteintes aux équipements ou aux données, la surveillance des équipements (…). Le harcèlement est un ensemble de conduites et de moyens d'action qu'une personne raisonnable, en possession de telles informations sur une tierce personne, sait qu'elle lui causerait une grande détresse émotionnelle. (p. 38, notre traduction)

Pittaro (2007) a relevé, dans sa revue de la littérature scientifique, que les *cyberstalkers* sont équivalents aux harceleurs « hors ligne » et qu'ils sont motivés par la colère, la rage et un besoin de contrôle et de pouvoir. Ils auraient des antécédents judiciaires, de consommation de substances psychoactives ou un trouble de la personnalité qui, directement ou en partie, contribueraient à la probabilité de conduites antisociales et l'augmenteraient même. Il précise toutefois que la plupart des crimes n'étant pas découverts ou rapportés aux autorités, ces éléments devraient donc être pondérés. Il effectue une comparaison entre les *stalkers* hors ligne et en ligne : le premier aurait un lien interpersonnel significatif avec la victime (le plus souvent un ex-partenaire amoureux), alors que le second aurait, dans la moitié des cas, tendance à choisir une victime sans lien d'intimité interpersonnelle, mais sur laquelle il peut facilement recueillir de l'information auparavant privée mais maintenant disponible sur les sites de réseautage professionnel (p. ex. : LinkedIn) (Bocij et McFarlane, 2002). Les recherches mentionnent même que des *cyberstalkers* peuvent faire équipe ou harceler par procuration, encouragés par d'autres dans cette tâche de harcèlement (Pittaro, 2007). Il en ressortirait que les « swatters agissent rarement seuls (…) les coconspirateurs peuvent se « rencontrer » sur un forum en ligne et agir de concert pour choisir, rechercher et localiser les victimes. Pendant qu'un des coauteurs passe l'appel, les autres peuvent l'écouter, encourageant son action et suivant les réponses des services d'urgences » (Bernstein, 2016, p. 52, notre traduction). À cet égard, les révélations récentes autour de la ligue du LOL illustrent bien la dynamique de groupe sous-jacente à ces harcèlements. D'autres suiveurs que le harceleur principal peuvent en effet se saisir d'une personne désignée[9].

En ce qui concerne le *swatting* au sens propre, nous pourrions supposer que l'émergence de cette pratique surviendrait assez régulièrement dans le milieu interconnecté du jeu en ligne. C'est du moins ce que laisse entendre Bernstein (2016), dont l'étude indique que les protagonistes peuvent se connaître par réputation numérique, dans un contexte de rivalités, floutant ainsi la démarcation en ligne / hors ligne sur la nature du lien entre l'auteur et sa victime. Nous avons toutefois pu constater que les victimes de *swatting* n'appartenaient pas toujours au milieu des joueurs en ligne puisque des stars du cinéma, des médias,

9. Pour en savoir plus, voir Durand et Sénécat (2019).

voire des politiciens considérés comme des opposants[10] peuvent aussi être ciblés. L'exposition médiatique de ces figures pourrait attirer des auteurs en recherche de gloire personnelle étant donné la médiatisation des faits.

> Une étude menée par Hoffman, Meloy et Sheridan (2013) sur un échantillon de 271 harceleurs de célébrités (hors ligne cette fois) révélait que les harcèlements duraient généralement en moyenne 26 mois et qu'un nombre substantiel de harceleurs ayant des troubles mentaux se retrouvait dans l'échantillon, que 27 % d'entre eux étaient psychotiques au moment des faits, 17 % s'étaient déjà vu prescrire une médication psychotrope, 7 % avaient commis des tentatives de suicide, 29 % étaient sans emploi et 29 % aussi avaient des antécédents judiciaires (…), 8 % insultaient et 6 % proféraient des menaces. (p. 164, notre traduction)

Mais l'un des points intéressants de cette étude concerne le harcèlement visant les membres de familles royales européennes. En effet, 32 % des *stalkers* (N = 107) présentaient les éléments d'une fixation pathologique envers ces familles :

> des préoccupations obsédantes (…). De telles fixations se focalisent sur une personne ou une cause, cette dernière est souvent en lien avec un grief personnel intense ou une quête de justice (…). Les recherches en Europe indiquent que la fixation sur une cause est reliée à un risque accru d'actions violentes. (p. 169, notre traduction)

Enfin, 36 % présentaient des éléments de grandiosité en lien avec des troubles narcissiques de la personnalité.

## 3. Méthodologie et connaissances apportées par les études de cas

Le sujet du *swatting* n'ayant jusqu'alors pas fait l'objet de publication en langue française, nous appuierons notre réflexion sur des thématiques connexes et conduites, pouvant se rapprocher de celle étudiée, notamment le cyberharcèlement, et des publications (principalement juridiques et anglo-saxonnes) qui couvrent ce phénomène ayant pris ces dernières années « des proportions quasi épidémiques en Californie » (Brumfield, 2014, p. 575, notre traduction). En l'absence de données statistiques,

10. Voir le cas d'un membre de l'assemblée américaine, Paul Moriarty, qui voulait faire passer une loi augmentant les peines de prison en 2014 pour des auteurs de *swatting* et qui fut lui-même victime d'un *swatting* le 13 novembre 2014 (Jaffe, 2016).

des études de cas seront utilisées pour illustrer notre réflexion relative aux mécanismes psychologiques sous-jacents au *swatting*. Nous détaillerons certains éléments nécessaires à sa réalisation, dont les techniques employées qui demandent des compétences dans différents domaines de la cybercriminalité et qui appartiennent à des catégories d'infractions condamnables pour lesquelles il existe une littérature scientifique. Nous aborderons les notions de mystification, de harcèlement et de piratage[11] et proposerons des pistes de réflexion dans le but d'intéresser les chercheurs au phénomène du *swatting* et les encourager à recueillir des données permettant une appréhension plus fine de celui-ci.

Du fait des délais judiciaires, certaines affaires non jugées à l'heure actuelle ne peuvent pas être utilisées à des fins de publication. Cela contribue malheureusement au faible nombre d'écrits sur le sujet. Dans cet article, nous développerons notre argument autour de trois cas ayant été déjà jugés ou médiatisés : les cas de Paris, Wichita et Créteil. Ces illustrations concrètes du *swatting* et de ses répercussions de même que cette partie documentée et les éléments contenus dans la presse éclaireront certains des concepts déjà abordés.

### *Étude de cas : Paris*

Le 17 septembre 2016, à Paris (France), une « alerte attentat » est déclenchée dans le quartier des Halles pour une prise d'otages se déroulant à l'église Saint-Leu. Dans le contexte post-attentat de 2015, et après l'attentat de Saint-Étienne-du-Rouvray de juillet 2016, un important dispositif de 300 policiers est dépêché sur les lieux. Mais les policiers mobilisés ce jour-là se rendent rapidement compte de la supercherie, au grand plaisir d'un des auteurs de ce *swatting*. Celui-ci s'en vanta sur les réseaux sociaux en écrivant : « *j'ai fais le pire SWATT, j'ai fait déplacé des hélico, le gouvernement, 50 voiture de flic j'suis passer en premier sur twitter, j'suis passer sur périscope, j'suis passer sur facebook, j'suis passer sur BFMTV et 10 journal hihi. #eglisefuck #flicKO* ».

Le principal suspect, Dylan, alias Tylers Swatting, est interpellé quelques jours plus tard dans son lycée où il était en seconde professionnelle. Il s'avérait être impliqué dans une série d'appels malveillants pour une fausse alerte à la bombe dans un lycée à Draveil. L'un de ses coauteurs avait diffusé de fausses alertes à la bombe dans des centres

11. En anglais : *spoofing*, *stalking* et *hacking*.

commerciaux. Au total, trois adolescents âgés de 14 à 17 ans ont été poursuivis pour ces faits. Les camarades de classe de Dylan l'ont décrit comme un jeune homme replié sur lui-même, passant ses nuits à pirater et à jouer en ligne (Goinard, Lombart et Sellami, 2016).

### *Étude de cas : Wichita*

Le 28 décembre 2017, à Wichita, au Kansas (États-Unis), une dispute éclate entre Casey Viner et Shane Gaskill au sujet d'une mise de 2 $ au cours d'une partie de *Call Of Duty : WWII* (Blankstein et Johnson, 2018 ; Swenson, 2018). Alors que le ton serait monté entre les deux joueurs, Viner, un résident de l'Ohio, aurait contacté un troisième individu, Tyler Barris de Los Angeles, afin de *swatter* Gaskill. Ce dernier, se rendant compte de l'activité sur son fil Twitter, aurait constaté que Barris suivait ses notifications et, dans une attitude de prestance, l'aurait contacté : « Essaie de faire un truc de fou. Tu vas essayer de me swatter, c'est hilarant… Je t'attends mon pote. » Barris aurait obtenu, lors de son échange avec Gaskill, une adresse qui correspondait à une ancienne adresse occupée par ce dernier avant d'en être expulsé deux ans auparavant. Barris se trouva ainsi en possession, au moyen de la mystification de l'identité de l'appelant, d'un indicatif d'appel à Wichita. Usurpant l'identité de Gaskill, il contacta le commissariat local et déclara qu'il avait tué son père, tenait en joue son frère et sa mère et envisageait de réduire la maison en cendres et de se suicider. Selon Blankstein et Johnson (2018), « L'attente ne fut pas longue, une quarantaine de minutes après le message reçu sur Twitter, la police de Wichita lança un raid sur une habitation en réponse à une situation d'otage. Andrew Finch, 28 ans, [nouvel occupant de l'adresse, n.d.a] est abattu par les forces de l'ordre… » (notre traduction).

L'occupant de l'ancienne adresse de Gaskill a ainsi été abattu sans être lié à ce qui se déroulait entre les trois jeunes hommes. Gaskill, Viner et Barris ont tous les trois étés inculpés, mais les deux premiers plaidèrent non coupables des charges d'homicide involontaire au deuxième degré. Barris, connu des forces de l'ordre pour des antécédents de fausses alertes à la bombe en 2015 et 2016, avait déjà été condamné à 32 mois de prison en mai 2016. Les deux accusés se sont vu notifier lors de l'audition de juin 2018 les chefs d'accusation auxquels ils faisaient face. En novembre 2018, à la suite d'une négociation de plaidoyer, Barris plaide coupable pour le compte d'une cinquantaine de faux

appels d'alertes pouvant amener à une condamnation de 20 à 25 ans de prison (Wolf, 2018). Le 29 mars 2019, la Cour de Californie condamne Barris à 20 ans de réclusion criminelle (Brice-Saddler, 2019). Le deuxième coaccusé n'a pas encore reçu de verdict. Quant à la nièce du défunt qui vivait avec lui au domicile et qui a assisté à la fusillade, elle s'est suicidée en début d'année, la mère de la victime liant ce geste à ce dont elle avait été témoin.

### *Étude de cas : Créteil*

Le 30 juin 2016, le Tribunal correctionnel de Créteil (France) condamne trois adolescents à des peines allant de six mois avec sursis à deux ans ferme à la suite d'un *swatting* survenu dans la nuit du 10 au 11 février 2015 (*Le Monde*, 2016)[12]. Hubert S. (alias Bibix) se filmait en direct sur la plateforme Twitch en jouant au jeu vidéo *DayZ* quand des policiers de la brigade anticriminalité (BAC) firent irruption dans son appartement et le menottèrent, ainsi que sa compagne. Ceux-ci avaient été avertis par téléphone d'un meurtre qui serait survenu à cette adresse. *Le Monde* (2016) rapporte à la suite de l'événement que la fausse dénonciation :

> était l'œuvre d'un groupe de trois jeunes Français passés par une plateforme spécialisée dans ce genre de canular, « ViolVocal », utilisée par les proches du hacker Ulcan, accusé de multiples appels malveillants et de menaces ces dernières années. Les trois condamnés étaient également inculpés pour recel – ils avaient utilisé des numéros de cartes bleues volées pour créer leur compte sur la plateforme.

L'avocat de la partie civile déclara sa surprise quant à la sévérité nouvelle des sanctions, puisqu'une affaire similaire en France avait abouti à une condamnation de six mois ferme, durée généralement aménageable. Bibix a été contraint de déménager, car son adresse a été diffusée sur Internet (une pratique appelée divulgation de données personnelles ou *doxing*).

## 4. Discussion : regard psychologique et criminologique

Ces trois cas montrent l'intrication qui existe entre les réseaux sociaux et la communauté en ligne. Ces sites de réseautage social (SRS) se sont

12. Voir le jugement rendu par le Tribunal de grande instance de Créteil le 30 juin 2016.

multipliés au cours des vingt dernières années. D'abord sortes de blogues améliorés, ils sont devenus aujourd'hui des plateformes de communication (Facebook Live, Périscope, Twitch) qui placent l'utilisateur comme un « producteur de contenu » partageant des moments de sa vie et interagissant par des chats valorisants avec ses suiveurs. Gozlan (2013) décrit dans sa thèse les enjeux psychiques et la construction identitaire chez l'adolescent. À travers son rapport aux SRS, le regard sur soi de l'adolescent s'inscrit dans une recherche narcissique qui confirme son sentiment d'exister, « faisant écho à cette recherche de l'objet perdu, le regard, première vérité sur soi » (Gozlan, 2013).

L'étude de O'Keeffe et Clarke-Pearson (2011) a mis au jour une corrélation entre le temps consacré aux SRS et le développement de signes dépressifs. Boudreault, Fournier et Beaulieu (2014) évoquent également un lien entre une utilisation supérieure à 10 heures par semaine de SRS et la présence de problèmes affectifs. L'identité numérique deviendrait ainsi pour certains une extension de leur personnalité, et une atteinte causée à cette « néo-identité » pourrait avoir des répercussions dans la vie réelle, soit en causant une perte de l'estime de soi, soit en entraînant une réaction agressive aux fins de préservation de celle-ci. On notera qu'« une relation intime antérieure entre le harceleur et la victime fut constamment repérée et corrélée positivement à des taux élevés de violence » (Scalora, 2014, p. 217, notre traduction).

D'autres comportements observables sur ces SRS sont les déchaînements de violence et d'agressivité, favorisés par le sentiment d'anonymat ou d'impunité sur la toile et désignés par le terme trollage (*trolling*), lequel est parfaitement décrit par Suler (2004). Seigfried-Spellar, Villacís-Vukadinović et Lynam (2017) associent les comportements de cybercriminalité à certains traits de personnalité psychopathique, dont l'absence de considération pour autrui et la désinhibition des conduites agressives. Leur étude laisse supposer une corrélation entre le faible contrôle comportemental et les actes de *hacking* et de piratage de données.

Le concept de *trolling* sur Internet a été interrogé en recourant au concept de « tétrade noire », évolution du concept de « triade noire » regroupant le machiavélisme, la psychopathie et le narcissisme, et incluant désormais les conduites « du sadisme quotidien » (Buckels, Jones, Paulhus, 2013). Quelles sont les attentes de l'auteur du *trolling* ? Il s'agit dans la plupart des cas d'obtenir l'approbation des autres (Craker et March, 2016). Ces récompenses sociales sont soit prosociales

et acceptées par la majorité des individus, soit atypiques, autrement dit valorisées, mais au sein d'une sous-culture à laquelle s'identifieraient les individus :

> la « puissance sociale négative » était positivement corrélée avec les traits de personnalité appartenant à la triade noire (machiavélisme, psychopathie et narcissisme) et des objectifs interpersonnels hostiles. Cela laisserait entendre que les personnes qui recherchent la « nuisance sociale » sont plus enclines à prendre plaisir à infliger à autrui une souffrance psychologique ou de la détresse en exerçant une influence sociale négative, ou en usant de leurs capacités et de leur « pouvoir ». (Craker et March, 2016, p. 80, notre traduction)

Si les études de Chabrol, Melioli, Van Leeuwen, Rodgers et Goutaudier (2015), Craker et March (2016) et Buckels *et al.* (2014) portent principalement sur le trollage et les conduites agressives sur les réseaux sociaux, nous pourrions extrapoler certains de leurs résultats au *swatting*, puisque, *in fine,* il s'agit d'activités se déroulant en ligne, entre des personnes entrant en contact par Internet, se connaissant parfois très succinctement, et hautement agressives dans leurs visées. Favorisés par l'anonymat d'Internet, qui offre alors la possibilité à des individus aux traits antisociaux d'aller explorer les « niches d'autrui » (parfois les plus secrètes), les auteurs cherchent à nuire par des pratiques plus variées qu'avant l'avènement d'Internet (Buckels *et al.*, 2014). Le contenu connaissant une forte popularité sur le Web renvoie généralement à trois thématiques : l'humour, le sexe et la violence. Les pratiques du *swatting* en réunissent au moins deux dans l'esprit des auteurs : l'humour et la violence.

Le cas de Wichita est particulièrement représentatif à cet égard. Une dispute survient entre deux joueurs en réseaux, au motif d'une somme dérisoire de deux dollars. Le ton serait monté entre les deux personnes et l'on pourrait supposer une question sous-jacente d'ego ou de narcissisme. L'étude de Rosenfeld (2003) évoque que les troubles de la personnalité les plus fréquents chez les harceleurs appartiennent au Cluster B du DSM IV, à savoir le trouble de la personnalité antisociale, le trouble de la personnalité narcissique et le trouble de la personnalité limite. L'atteinte narcissique pourrait être le déclencheur dans la mise en œuvre de conduites agressives. « Jones et Paulhus (…) trouvèrent une corrélation entre le narcissisme et l'agression lorsqu'il y a eu une provocation portant atteinte à l'intégrité de l'image de soi » (Gammon, Converse, Lee et Griffith, 2011 p. 367).

Outre le harcèlement, le harcèlement par procuration est également mentionné dans les études sur le sujet. Le « recrutement » de Barris par Viner dans les événements de Wichita en est une illustration.

Plusieurs hypothèses, qui sont à confirmer ou à infirmer puisqu'elles se fondent sur un petit nombre de cas, peuvent être posées. Notamment, nous pouvons nous questionner sur la présence d'antécédents de condamnation (ou du moins de mises en accusation) pour des faits rattachés à de la cybercriminalité au sens large. Le jeune Dylan-Tylers avait déjà commis des faits similaires et s'identifiait, avec ses coauteurs, au *swatter* Gregory Chelli (connu sous le pseudonyme Ulcan) qui les désavoua immédiatement en donnant leurs coordonnées. Par ailleurs, le choix de son pseudo évoque le nom du principal accusé de Wichita. Barris avait déjà été condamné et mis en cause à quatre reprises. Concernant le cas jugé à Créteil, parmi les trois Français condamnés, l'un avait des antécédents judiciaires pour vols et dégradation, outrage, et vol en réunion, l'un n'avait pas de condamnation et le troisième bénéficia d'une « altération du discernement[13] » à la suite de l'expertise psychiatrique. Une coopération avec les services de justice pourrait permettre d'isoler d'autres caractéristiques plus spécifiques, notamment la prévalence d'actes hétéroagressifs « dans la vie réelle » parmi les auteurs de ce type d'infraction. Est-ce que, de la même manière que dans les cas de téléchargeurs de vidéos pédopornographiques, les auteurs les plus à même de passer à l'acte et de se montrer violents dans la vie réelle seraient ceux possédant des condamnations pour des violences physiques interpersonnelles et des traits de personnalité antisociale, voire nettement psychopathique (Babchishin, Paquette et Fortin, 2017) ? Est-ce que l'aspect sans contact, présent entre les protagonistes, conférerait à ces infractions une absence de prise en considération du risque encouru ? Une minimisation à un simple canular entre joueurs ? Des études supplémentaires, prenant en compte les caractéristiques de la personnalité, les antécédents de troubles de l'humeur, la présence ou l'absence de traits de personnalité psychopathique, les antécédents de violences physiques ou non, ainsi que les caractéristiques principales du fonc-

13. Le Code de procédure pénale français indique que « La personne qui était atteinte, au moment des faits, d'un trouble psychique ou neuropsychique ayant altéré son discernement ou entravé le contrôle de ses actes demeure punissable. Toutefois, la juridiction tient compte de cette circonstance lorsqu'elle détermine la peine et en fixe le régime. Si est encourue une peine privative de liberté, celle-ci est réduite du tiers. »

tionnement social chez l'auteur de *swatting*, seront nécessaires pour confirmer ou infirmer ces hypothèses.

## Conclusion

Comme cet article traite d'un sujet nouveau, il soulève *de facto* des limites liées en premier lieu à l'absence de données statistiques précises. La deuxième limite est l'absence d'éléments cliniques de première main, puisque la majorité des cas de *swatting* ne donnent pas lieu à l'ouverture d'une procédure criminelle, nécessaire en France pour qu'une expertise psychologique et psychiatrique soit ordonnée par le juge d'instruction. La troisième limite provient du délai judiciaire, qui s'étend du début des poursuites jusqu'au jugement. Relevons en dernier lieu la principale limite, le nombre restreint de cas, qui devrait inciter à la prudence pour ne pas surgénéraliser ce phénomène nouveau.

Le *swatting* entraîne des coûts financiers importants en termes de déploiement des unités spéciales et d'engorgement de ces services, qui ne seraient alors plus opérationnels en cas de nécessité réelle d'intervention. Si le risque est généralement minimisé par les auteurs, le *swatting* est toutefois assez éloigné du canular téléphonique traditionnel compte tenu des compétences techniques mobilisées et de ses conséquences. L'exemple de Wichita a montré que la mobilisation d'unités d'intervention sur un site envisagé comme étant hostile par les forces de l'ordre peut se révéler dramatique. La question qui se pose à propos des SRS et de l'identité numérique est la suivante : serait-ce pour le sujet une tentative d'affirmation de soi, une démonstration de ses compétences techniques ou une manipulation en vue d'obtenir une valorisation par des pairs – lui procurant une visée antidépressive –, l'expression d'une agressivité qu'il ne pourrait forcément pas se permettre hors ligne ? La notion d'une dilution de la responsabilité observée y serait présente compte tenu du fait que l'auteur ne se sent pas toujours responsable, estimant que ce n'est « pas réel »[14] et que la victime, d'une certaine manière, se voit dépossédée d'une partie de l'infraction, pour citer Gozlan (2013), qui parle « d'altérité virale », avec un élément d'elle qui lui échappera totalement par sa diffusion et son partage à grande échelle sur le Web ou parmi un groupe de pairs.

14. Dans la mesure où l'atteinte causée à la cible n'est pas directement et physiquement causée par l'auteur.

## Références


Babchishin, K. M., Paquette, S. et Fortin, F. (2017). Les consommateurs de pédopornographie. Dans F. Cortoni et T. H. Pham (dir.), *Traité de l'agression sexuelle : théories explicatives, évaluation et traitement des agresseurs sexuels* (p. 251-270). Bruxelles, Belgique : Éditions Mardaga.

Bernstein, L.-K. (2016). Investigating and prosecuting "swatting" crimes. *United States Attorneys' Bulletin, 64*(3), 51-56.

Blanch, J. L. et Hsu, W. L. (2016). An introduction to violent crimes on the Internet. *United States Attorneys' Bulletin, 64*(3), 2-11.

Blankstein, A. et Johnson, A. (2018, 3 janvier). Suspect in Kansas 'swatting' death served time for false bomb reports. NBC News. Repéré à https://www.nbcnews.com/news/us-news/suspect-kansas-swatting-death-served-time-false-bomb-reports-n834201

Bocij, P. et McFarlane, L. (2002). Online harassment : Towards a definition of cyberstalking. *Prison Service Journal, 139*, 31-38.

Boudreault, A., Fournier, S. et Beaulieu, J. (2014). *La relation entre le temps consacré aux réseaux sociaux et les problèmes affectifs chez les adolescents.* Affiche présentée au 82e congrès de l'ACFAS, Montréal, Québec.

Brice-Saddler, M. (2019, 29 mars). Man to serve 20 years in fatal 'swatting case'. *The Washington Post.* Repéré à https://www.washingtonpost.com/national/a-california-man-is-sentenced-to-20-years-in-fatal-false-hostage-swatting-hoax/2019/03/29/7ae18a90-4d14-11e9-9663-00ac73f49662_story.html? noredirect=on&utm_term=.028c553967d1

Brumfield, E. (2014). Deterring and paying for prank 911 calls that generate a SWAT team response. *McGeorge Law Review, 45*(3), 585-594.

Buckels, E. E., Jones, D. N. et Paulhus, D. L. (2013). Behavioral confirmation of everyday sadism. *Psychological science, 24*(11), 2201-2209.

Buckels, E. E., Trapnell, P. D. et Paulhus, D. L. (2014). Trolls just want to have fun. *Personality and individual Differences, 67*, 97-102.

Burel, L. (2016, 18 septembre). L'appel irresponsable qui a provoqué l'alerte attentat à Paris samedi. *L'Obs.* Repéré à https://www.nouvelobs.com/societe/20160917.OBS8237/info-obs-l-appel-irresponsable-qui-a-provoque-l-alerte-attentat-a-paris-samedi.html

Chabrol, H., Melioli, T., Van Leeuwen, N., Rodgers, R. et Goutaudier, N. (2015). The Dark Tetrad : Identifying personality profiles in high-school students. *Personality and Individual Differences, 83*, 97-101.

Craker, N. et March, E. (2016). The dark side of Facebook® : The Dark Tetrad, negative social potency, and trolling behaviours. *Personality and Individual Differences, 102*, 79-84.

Duke, A. (2013, 12 mars). Boys admits 'swatting Ashton Kutcher, Justin Bieber. *CNN.* Repéré à https://edition.cnn.com/2013/03/11/showbiz/kutcher-swatting-conviction/index.html

Durand, A.-A. et Sénécat, A. (2019, 12 février). Ligue du LOL : cinq questions pour comprendre l'affaire et ses enjeux. *Le Monde.* Repéré à https://www.lemonde.fr/les-decodeurs/article/2019/02/12/ligue-du-lol-cinq-questions-pour-comprendre-l-affaire-et-ses-enjeux_5422639_4355770.html

Federal Bureau of Investigation. (2008). Don't make the call : The new phenomenon of 'swatting'. Repéré à https://archives.fbi.gov/archives/news/stories/2008/february/swatting020408

Gammon, A. R., Converse, P. D., Lee, L. M. et Griffith, R. L. (2011). A personality process model of cyber harassment. *International Journal of Management and Decision Making, 11*(5-6), 358-378.

Goinard, N., Lombart, G. et Sellami, S. (2016, 21 septembre). Fausse alerte attentat : Tylers Swatting n'était pas un inconnu. *Le Parisien*. Repéré à http://www.leparisien.fr/faits-divers/tylers-swatting-n-etait-pas-un-inconnu-21-09-2016-6137359.php

Gozlan, A. (2013). La machine virtuelle : une désintimité à l'oeuvre. *Recherches en psychanalyse, 2*(16), 185-193.

Herzog-Evans, M. (dir.). (2010). *Transnational criminology manual* (vol. 1). Nijmegen, Pays-Bas : Wolf Legal Publishers.

Hoffmann, J., Meloy, J. R. et Sheridan, L. (2013). Contemporary research on stalking, threatening, and attacking public figures. Dans J. R. Meloy et J. Hoffmann (dir.), *International Handbook of Threat Assessment* (p. 160-177). New York, NY : Oxford University Press.

Jaffe, E. M. (2016). Swatting : the new cyberbullying frontier after *Elonis v. United States. Drake L. Rev., 64*(2), 455-483

Jeffries, A. (2013, 23 avril). Meet 'swatting', the dangerous prank that could get someone killed. *The Verge.* Repéré à https://www.theverge.com/2013/4/23/4253014/swatting-911-prank-wont-stop-hackers-celebrities

Le Monde. (2016, 1er juillet). "Swatting" : prison ferme pour un canular dangereux. Repéré à https://www.lemonde.fr/pixels/article/2016/07/01/prison-ferme-pour-les-auteurs-d-un-canular-en-pleine-partie-de-jeu-video_4961831_4408996.html

Meloy, R. J. (1998). *The psychology of stalking : Clinical and forensic perspectives.* San Diego, CA : Academic Press.

Meloy, R. J. et Gothard, S. (1995). Demographic and clinical comparison of obsessional followers and offenders with mental disorders. *Am J Psychiatry, 152*(2), 258-263.

Ministère de l'Intérieur. (2018). *État de la menace liée au numérique en 2018 : la réponse du ministère de l'Intérieur. Rapport nº 2.* Repéré à https://www.interieur.gouv.fr/content/download/110309/879759/file/rapport-2-cybermenaces.pdf

Mishra, A. et Mishra, D. (2007). Cyber stalking : A challenge for web security. Dans L. Janczewski et A. Colarik (dir.), *Cyber Warfare and Cyber Terrorism* (p. 216-226). IGI Global.

O'Keeffe, G. S. et Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *Pediatrics, 127*(4), 800-804.

Pittaro, M. L. (2007). Cyber stalking : An analysis of online harassment and intimidation. *International Journal of Cyber Criminology, 1*(2), 180-197.

Roberts, L. (2010, 23 décembre). Police warn of burglary risk from social media sites. *BBC News.* Repéré à https://www.bbc.com/news/av/uk-12070679/police-warn-of-burglary-risk-from-social-media-sites

Rosenfeld, B. (2003). Recidivism in stalking and obsessional harassment. *Law and Human Behavior*, *27*(3), 251-265.

Scalora, M. (2014). Electronic threats and harassment. Dans J. R. Meloy et J. Hoffmann (dir.), *International Handbook of Threat Assessment* (p. 214-223). New York, NY : Oxford University Press.

Seigfried-Spellar, K. C., Villacís-Vukadinović, N. et Lynam, D. R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. *Journal of Criminal Justice*, *51*, 67-73.

Sellami, S. (2016, 20 septembre). L'objectif final des canulars : la paralysie des services de l'État. *Le Parisien*. Repéré à http://www.leparisien.fr/faits-divers/l-objectif-final-la-paralysie-des-services-de-l-etat-20-09-2016-6134265.php

Spacebound. (2016, 21 janvier). Top 10 gamers swatted on live stream [Fichier vidéo]. Repéré à https://www.youtube.com/watch ? v=gedVHbgIt7c&ab_channel=Spacebound

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & behavior*, *7*(3), 321-326.

Swenson, K. (2018, 14 juin). Two rival gamers allegedly involved in Kansas 'swatting' death plead not guilty in federal court. *The Washington Post*. Repéré à https://www.washingtonpost.com/news/morning-mix/wp/2018/06/14/two-rival-gamers-allegedly-involved-in-kansas-swatting-death-plead-not-guilty-in-federal-court/?noredirect=on&utm_term=.3d1ddcb1650a

Union internationale des télécommunications. (2018). L'UIT publie des estimations régionales et mondiales concernant les TIC pour l'année 2018. Repéré à https://www.itu.int/fr/mediacentre/Pages/2018-PR40.aspx

Wolf, J. (2018, 4 novembre). Tyler Bariss pleads guilty to 'swatting' hoax, gets 20 to 25 years. *ESPN*. Repéré à https://www.espn.com/esports/story/_/id/25271573/tyler-barriss-pleads-guilty-gets-20-25-years-swatting-case

**Jurisprudence**

Tribunal de Grande Instance de Crétail. (2016, 30 juin). Jugement du 30 juin 2016. Repéré à https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-creteil-12e-ch-corr-jugement-du-30-juin-2016/

## New technologies and cyberstalking : Swatting as an example

**ABSTRACT** • *This paper focuses on the internet phenomenon known as swatting, which has existed in the United States for over fifteen years but only recently appeared in Europe. Often described by its perpetrators – online gamers – as a "hoax" or a "phone prank", swatting can have dramatic consequences, as demonstrated by a case in Wichita, Kansas, in December 2017, in which a man was killed during the event. The aim of this paper is to define what is swatting, what are its implications for security, what are the risks and issues it poses, and what types of behavior it includes.*

**KEYWORDS** • *Swatting, cyberstalking, dark tetrad, spoofing.*

## Nuevas tecnologías y ciberacoso : el ejemplo del *swatting*

**RESUMEN** • *Esta contribución tratará de hacer un balance de un fenómeno que se ha desarrollado estos últimos cinco años en Europa, pero que existe desde hace unos quince años en los Estados Unidos, sobre todo entre los usuarios de juegos en línea, es decir el* swatting. *Los hechos que tuvieron lugar en Wichita, Kansas, Estados Unidos, en diciembre del 2017, resultando en la muerte de un hombre, muestran las consecuencias dramáticas, considerado como un engaño telefónico. Trataremos a lo largo de este artículo de definir el* swatting*, lo cual pasa por preguntarse por las implicaciones en términos de seguridad, por los riesgos y dilemas que están ligados y por los tipos de conductas asociadas a este.*

**PALABRAS CLAVE** • Swatting*, cibercriminalidad, tétrada negra,* spoofing.