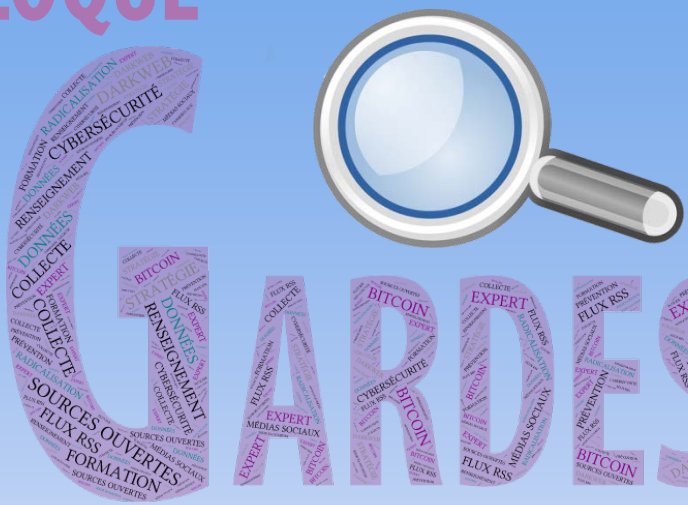
3e édition

COLLOQUE



Groupe sur l'Analyse, la Recherche et le Développement en Source Ouverte

Jeudi 14 juin 2018

8 h 00 – 16 h 00

Université de Montréal
Pavillon Lionel-Groulx, 3150, rue Jean-Brillant
Montréal
Salle C-3061 (3e étage)

En collaboration avec :

JLR 30 ans de solutions foncières

COMMISSIONNAIRES
FIABLE · EN TOUT TEMPS · EN TOUT LIEU

GARDESO · CiCC · serene risc · Université de Montréal

Remerciements

Le comité organisateur désire remercier les partenaires commerciaux de l'événement pour leur contribution à faire de cet événement un succès !

Partenaires principaux

JLR 30 ANS DE SOLUTIONS FONCIÈRES

COMMISSIONNAIRES
FIABLE · EN TOUT TEMPS · EN TOUT LIEU

Partenaires

GARDESO

CICC
Centre international de criminologie comparée

Université de Montréal

serene-risc
RÉSEAU INTÉGRÉ SUR LA CYBERSÉCURITÉ

HORAIRE DE LA JOURNÉE

8h00	Accueil (Salle C-3061)
8h30	Mots d'accueil et présentation des dignitaires
9h00	Médias sociaux et Tribunaux – Marie-Christine Robert
10h00	Pause / Réseautage
10h30	Conférences: • Vers une veille systématique des sites web hébergés sur le Darknet – David Décary-Hétu • Surveillance et indexation du Web invisible et du Web profond – Olivier Bilodeau et Félix Lehoux
11h30	Présentations des commanditaires : JLR et Commissionnaires
12h00	Dîner (Cafétéria)

HORAIRE DE LA JOURNÉE (SUITE)

13h15	Ateliers			
	Piste 1 **Débutant**	**Piste 2** **Intermédiaire**	**Piste 3** **Expert**	**Piste 4** **Enjeux**
13h15	(1 et 2) **Cybersec101: Un programme québécois de sensibilisation et de formation à la cybersécurité** (Présentation d'une heure) Benoit Dupont (C-1017-02)	(3) **Facebook: Outils et Astuces** Jocelyn April (C-3061)	(5) **Exploration des utilisations criminelles des cryptomonnaies** Mathieu Guillot (C-2059)	
13h45		(4) **Analyse de données Facebook** Julie Delle Donne (C-3061)	(6) **Traçabilité des transactions illicites dans l'écosystème du Bitcoin** Masarah Paquet-Clouston (C-2059)	
14h15	Pause / Réseautage			
14h30	(9) **La cyberenquête: un outil de plus dans la lutte au braconnage** Éric Champagne (C-1017-13)	(11) **Al-Canadi et compagnie : Portrait du rôle des Canadiens dans la propagande jihadiste** Maxime Bérubé (C-1017-02)	(13) **Buscador: un outil puissant et polyvalent** Philippe Lefebvre (C-3061)	(15) **Les défis de la mise en preuve des documents électroniques de sources ouvertes (R. c. *Hamdam* 2017 BCSC 676)** Maxime Laroche (C-2059)
15h00	(10) **Traces numériques et application de la loi** Francis Fortin (C-1017-13)	(12) **Vers une typologie des «contre-mesures» visant le jihadisme en ligne : Le cas du Canada** Benjamin Ducol (C-1017-02)	(14) **XL-Whois: l'automatisation et le classement d'un registre de données sur les sites Web** Alain Rioux (C-3061)	(16) **Un pas vers l'«Evidence Based Policing» Table ronde sur les bonnes pratiques en matière de médias sociaux** Brigitte Poirier et Julie Delle Donne (C-2059)
15h30	Mot de la fin (Salle C-3061)			
16h00	4 @ 7 (Salle C-2081/2083)			

8h00 Accueil (C-3061)

8h30 Mots d'accueil et présentation des dignitaires

Francis Fortin, Professeur adjoint, École de criminologie de l'Université de Montréal

Maxime Grenier, Superviseur d'équipe, Division des enquêtes en cybercriminalité, Sûreté du Québec

Jean-Philippe Dehaes, Lieutenant-détective, Division du renseignement, module liaison-sécurité, Service de Police de la Ville de Montréal

Manon Tremblay, Responsable Analyse stratégique et tactique, Division Renseignement, Service de police de Laval

9h00 Médias sociaux et Tribunaux

Revue jurisprudentielle en matière de médias sociaux. Très populaires, les Facebook, Instagram, Pinterest et YouTube de ce monde, sont de véritables mines d'or d'informations. À la fois outils d'enquête et « scènes de crime » les médias sociaux font partie intégrante du quotidien d'une grande partie de la population et par conséquent, également du paysage judiciaire. Se retrouvant ainsi de plus en plus devant les tribunaux, comment toutes ces informations provenant de sources dites « ouvertes » sont-elles accueillies par ces derniers ? Constituant une opportunité unique, l'utilisation de ces sites accessibles apporte également son lot de défis, notamment pour que ces éléments de preuve soient acceptés par la cour. Réalité du web 2.0 et maintenant du web 3.0, les médias sociaux ont été au cœur de nombreuses décisions dans les dernières années, offrant ainsi un portrait de plus en plus clair de ce qui est maintenant possible d'obtenir avec ces outils numériques.

Marie-Christine Robert, Avocate, Ministère de la Justice du Québec

10h00 Pause / Réseautage

10h30 Conférences
Vers une veille systématique des sites web hébergés sur le Darknet

L'internet est souvent présenté comme un environnement virtuel où la désinhibition envers des comportements déviants et l'impunité sont élevées. Cela est d'autant plus vrai pour le darknet, la sous-section d'internet où toutes les communications entre des internautes et des serveurs hébergeant des sites web sont chiffrées. Ce chiffrement permet d'anonymiser les communications et de rendre difficile la localisation des internautes et des serveurs actifs sur le darknet. Plusieurs études ont indexé de manière partielle les sites web hébergés sur le darknet afin de mieux comprendre la proportion de contenu illicite véritablement présente sur le darknet. Ces études ont démontré qu'une proportion importante de sites web hébergés sur le darknet distribuaient ou facilitaient la distribution de pornographie juvénile, de drogues illicites, d'outils de piratage informatiques et de données personnelles et financières volées. L'objectif de cette présentation est de bâtir sur ces recherches passées en réalisant une veille beaucoup plus importante des sites web hébergés sur le darknet. Cette activité nous a permis d'augmenter la proportion de sites web du darknet étudiés et de mieux comprendre leur contenu. Cette présentation visera aussi à cartographier à l'aide de technique d'analyse de réseaux les liens entre les différents sites web hébergés sur le darknet. Ces analyses visent à comprendre la structure, la cohésion et la présence d'acteurs clés dans ce réseau de sites web.

David Décary-Hétu, Professeur, École de Criminologie de l'Université de Montréal

10h30 Conférences (suite)
Surveillance et indexation du Web invisible et du Web profond

De nos jours, la posture de cybersécurité d'une organisation ne dépend plus seulement de sa surface d'attaque extérieure, mais aussi des fuites d'informations la concernant. Ces fuites peuvent être volontaires ou non, sur le Web invisible ou bien cachées sur le Web "régulier". Elles sont généralement le fruit d'un employé ou d'un pirate informatique. Afin de mieux protéger nos clients, nous avons mis à l'essai deux outils de surveillance et d'indexation du Web invisible et profond.

Cette présentation introduira le Web invisible (Darknet), fera un survol de son contenu et montrera comment y accéder. De plus, nous aborderons le Web profond (sites réguliers mal indexés par Google) qui est sous-estimé quant à son contenu de fuites intéressantes. Nous terminerons avec une démonstration de ces outils pour lesquels l'accès sera partagé gratuitement à la communauté de Gardeso, qui pourra l'utiliser à des fins policières.

Olivier Bilodeau et Félix Lehoux, Chercheurs en cybersécurité, GoSecure Inc.

11h30 Présentations des commanditaires JLR et Commissionnaires

12h00 Dîner (Cafétéria)

Ateliers en après-midi – première partie

Piste 1 Débutant (C-1017-02)

13h15 (1 et 2) Cybersec101: Un programme québécois de sensibilisation et de formation à la cybersécurité

Cette présentation a pour objectif de décrire la structure et le contenu du programme de sensibilisation et de formation cybersec101 destiné au grand public. Élaboré par le Réseau intégré sur la cybersécurité, en partenariat avec le Centre canadien anti-fraude et avec le soutien financier de Sécurité publique Canada, ce programme est disponible selon deux modalités de diffusion: en ligne sur le principe de l'auto-formation et en mode présentiel dispensé par des formateurs à de petits groupes selon des modalités interactives. Cette présentation abordera la philosophie générale du programme, ses contenus, les expériences de diffusion menées en collaboration avec de grands réseaux de bibliothèques publiques et discutera des possibilités pour les organisations policières québécoises de l'offrir à leurs citoyens.

Benoit Dupont, Professeur, École de criminologie de l'Université de Montréal

Piste 2 Intermédiaire (C-3061)

13h15 (3) Facebook: Outils et Astuces

Dans cette présentation, il sera question de mettre à jour les différents outils utiles dans le cadre de la recherche en source ouverte et particulièrement dans le cadre d'enquêtes de tous types. En utilisant des études de cas et des exemples en ligne, la présentation abordera les divers médias sociaux ainsi que des méthodes de recherche permettant d'établir le profil virtuel d'un individu. Il sera aussi question de certains outils et techniques pour effectuer des recherches plus complètes dans les sources ouvertes. L'accent sera mis sur les nouveaux outils et les meilleures pratiques dans le domaine.

Jocelyn April, Retraité de la Sûreté du Québec

13h45 (4) Analyse de données Facebook

Chaque jour, que ce soit sur des profils, des pages ou encore des groupes, une multitude d'informations, accessibles à tous, circule sur Facebook. Ces informations sont parfois indispensables aux membres des organisations policières. Or, la façon dont est conçu Facebook peut rendre leurs recherches et leurs collectes fastidieuses. Le présent atelier aura donc pour objectif d'aider les participants à comprendre le fonctionnement de certains outils reliés à la recherche et à la collecte d'information sur Facebook. Pour se faire, des démonstrations de l'utilisation d'outils, tels que le Graph Facebook, FacePager et ExtractFace, seront réalisées. La présentation des informations obtenues par les requêtes transmises dans les outils permettra également d'aborder quel outil a la capacité de répondre à quels types de besoins, tel que créer le portrait d'un réseau, trouver des informations sur un individu, ou encore, comprendre un mouvement social.

Julie Delle Donne, Candidate au doctorat, École de Criminologie de l'Université de Montréal

Piste 3 Expert (C-2059)

13h15 (5) Exploration des utilisations criminelles des cryptomonnaies

Cette présentation s'intéressera aux différents types de criminalité pouvant utiliser les cryptomonnaies comme agent facilitateur. Nous décrirons chacun de ces types en proposant d'explorer l'impact des cryptomonnaies sur leurs commissions, ainsi qu'en fournissant des exemples d'évènement ayant été rendus publics qui relatent l'utilisation de cryptomonnaies. Au cours de la deuxième partie, nous décrirons les caractéristiques des cryptomonnaies qui sont (ou seront) profitables aux criminels et nous proposerons de comparer le fonctionnement de certaines d'entre elles afin de soupeser cette profitabilité. Ces constats permettront de souligner les défis inhérents à l'investigation sur les transactions effectuées en cryptomonnaie, mais aussi de mettre en avant des pistes de solutions ayant été utilisées par le passé.

Mathieu Guillot, Candidat à la maîtrise, École de Criminologie de l'Université de Montréal

13h45 (6) Traçabilité des transactions illicites dans l'écosystème du Bitcoin

Cette conférence présente les résultats d'une étude ayant développé une méthode pour suivre les transactions reliées à des activités illicites dans l'écosystème du Bitcoin. La méthode va au-delà des heuristiques de 'clustering' présentées au cours des dernières éditions de Gardeso puisqu'elle réussit, lorsque possible, à trouver les endroits où l'argent est encaissé. Elle capitalise également sur une plateforme en source ouverte, GraphSense, qui offre une interface graphique. La méthode est appliquée, à des fins de démonstration, sur les transactions bitcoin de 35 familles de rançongiciels.

Suite à l'analyse, l'étude estime l'impact financier direct des 35 familles de rançongiciels et montre les différentes plateformes, lorsque possible, ou l'argent obtenu par extorsion est encaissé.

Masarah Paquet-Clouston, Chercheure, GoSecure Inc.

14h15 Pause

Piste 1 Débutant (C-1017-13)

14h30 (9) La cyberenquête: un outil de plus dans la lutte au braconnage

Cette conférence vous présente comment les sources ouvertes transforment le métier d'agent de protection de la faune et comment son unité de renseignement doit s'adapter à l'arrivé des réseaux sociaux sur le territoire québécois.

Tout d'abord, le fonctionnement et les réalisations du Service de Renseignement et du Soutien aux Enquêtes (SRSE) seront présentés. Cette unité, peu connue en dehors du cercle restreint des agents de protection de la faune, fait son travail dans l'ombre. Leur pain quotidien est constitué d'infiltration, de surveillance et de soutien aux enquêtes courantes. Derrière chaque grande opération, on retrouve la trace de ces enquêteurs spécialisés.

Ensuite, l'impact des réseaux sociaux sur le travail des agents de protection de la faune se fait de plus en plus sentir et ceux-ci doivent se réinventer pour rattraper le train. Parmi ces changements, la décentralisation de la collecte de donnée, la normalisation de la méthode et le développement d'un réseau d'avatars pour traquer les braconniers.

Éric Champagne, Lieutenant, Service du renseignement et du soutien aux Enquêtes, Ministère des Forêts, de la Faune et des Parcs

15h00 (10) Traces numériques et application de la loi

Depuis l'arrivée d'Internet, il a toujours été possible de tracer la provenance de l'information. Au cours des dernières années, des outils plus avancés et subtils sont apparus afin de suivre les utilisateurs d'Internet. À l'instar de la trace traditionnelle, la trace numérique est constituée à partir d'empreintes numériques qui seraient laissées volontairement ou involontairement dans l'environnement informatique à l'occasion d'une activité informatique (Mille, 2013). Bien que l'intention initiale était de suivre les individus pour des fins de marketing, on se sert depuis longtemps des traces informatiques comme objet d'analyse de tendance, mais aussi afin de cibler des marchés. Dans cet atelier de vulgarisation, nous aborderons la question de la trace numérique que laissent les interactions en ligne et ce, que ce soit pour le public en général ou les agences d'application de la loi. À l'aide d'exemple, nous démontrerons les possibilités de découverte d'information à partir d'opérations simples sur Internet. Ainsi, nous verrons des exemples de Google Analytics, de profilage de navigateurs, de suivi de liens (urls shorteners). Des mesures de précaution pour des opérations en ligne seront présentées en guise de conclusion.

Francis Fortin, Professeur adjoint, École de Criminologie de l'Université de Montréal

Piste 2 Intermédiaire (C-1017-02)

14h30 (11) Al-Canadi et compagnie : Portrait du rôle des Canadiens dans la propagande jihadiste

Depuis maintenant plus d'une décennie, les violences associées au jihadisme et à l'islamisme radical sont devenues une préoccupation majeure pour les autorités publiques canadiennes. Ces dernières doivent notamment jongler avec la nature changeante des activités d'influence menées par les organisations jihadistes, surtout en cette ère où les nouvelles technologies offrent de plus vastes opportunités de communication. Bien qu'il faille nuancer les effets directs de ces technologies (Conway, 2017), bon nombre de chercheurs suggèrent que l'exposition aux vidéos et autres matériels de propagande peut agir comme catalyseur et accélérateur d'un processus de radicalisation menant à la violence (p.ex. : von Behr et al., 2013; Gill et al., 2017; Ducol et al., 2016). Afin de contribuer à une meilleure évaluation de la menace jihadiste relative au Canada, cette présentation explore les représentations en sources ouvertes du Canada dans la propagande diffusée par les organisations jihadistes. Elle se concentre entre autres à offrir un portrait détaillé des usages de figures canadiennes à des fins de recrutement et de persuasion en vue d'actions terroristes, ou encore afin de les mobiliser comme symbole du jihadisme global.

Maxime Bérubé, Candidat au doctorat, École de Criminologie de l'Université de Montréal

15h00 (12) Vers une typologie des « contre-mesures » visant le jihadisme en ligne : Le cas du Canada

À l'instar de nombreux États confrontés au phénomène jihadiste et à ses manifestations violentes, le Canada a tenté de développer au cours de la dernière décennie, une série de « contre-mesures » visant à lutter contre la prolifération des contenus de propagande et des discours jihadistes en ligne. Afin de mieux cerner la nature de ces « contre-mesures », nous nous proposons de développer une typologie permettant de catégoriser ces « contre- mesures » selon deux axes principaux : leur nature (répression vs prévention) et les acteurs dont elles émanent (État vs acteurs de la société civile). Cette typologie permet d'entrevoir la diversité des « contre-mesures » existantes à l'heure actuelle au Canada, allant des nouvelles dispositions criminelles introduites par la Loi antiterroriste de 2015 (aussi connu sous le nom de C-51), aux campagnes de sensibilisation en ligne et aux approches dites de « contre-narratifs » en passant par les stratégies de blocage ou de retrait des contenus illégaux sur les médias sociaux et le Web. Cette typologie nous permet en retour d'évaluer l'adéquation des mesures en place pour lutter contre le jihadisme en ligne au regard des constats actuels dans le domaine. Cette présentation est tirée de: Bérubé, M. & Ducol, B. (À paraître en 2018) « Jihadism in the Digital Era. The Canadian context and responses" dans J. Littlewood, L. L. Dawson, & S. Thompson (dir.), Terrorism and Counterterrorism in Canada (Toronto: University of Toronto Press).

Benjamin Ducol, Responsable de la recherche et de l'appui à l'innovation, Centre de prévention de la radicalisation menant à la violence

Piste 3 Expert (C-3061)

14h30 (13) Buscador : un outil puissant et polyvalent

Buscador (qui en espagnol signifie Chercheur), est un système d'exploitation conçu spécifiquement pour l'enquête en ligne à partir des sources ouvertes. Le système d'exploitation basé en Linux, contient les principales applications et des extensions utilisées couramment par les cyberenquêteurs pour notamment l'analyse de profils dans les médias sociaux (Twitter, Instagram), l'analyse de nom de domaine et sous-domaines, le téléchargement et la conversion de vidéos ainsi que l'extraction de métadonnées. L'objectif de cette présentation est de passer en revue ces applications à l'aide d'exemples concrets.

Philippe Lefebvre, Conseiller sécurité industrielle, Hydro-Québec

15h00 (14) XL-Whois: l'automatisation et le classement d'un registre de données sur les sites Web

Les outils de WHOIS sont utiles, mais est-ce que les gens comprennent vraiment d'où vient l'information et ce qu'elle signifie ? Dans cette présentation, il sera question de domain WHOIS, network WHOIS, dns records, ICANN, IANA, les registraires, les serveurs de WHOIS, les requêtes avancées, etc. Des notions de base et des concepts plus avancés. En bonus, une présentation de XL-Whois (le-tools.com).

Alain Rioux, Enquêteur, Sûreté du Québec

Piste 4 Enjeux (C-2059)

14h30 (15) Les défis de la mise en preuve des documents électroniques de sources ouvertes (R. c. *Hamdam* 2017 BCSC 676)

En 2015, M. Othman Ayed Hamdan est accusé de trois chefs d'accusation pour avoir conseillé de commettre des actes criminels au profit, sous la direction ou en association avec une organisation terroriste. Il est également accusé d'avoir chargé, directement ou indirectement, des personnes à mener des activités terroristes. Les accusations se rapportent à une série de messages Facebook créés par M. Hamdan qui semblaient soutenir le groupe terroriste État islamique (« EI »). La série de messages a été obtenue par le biais de deux membres d'une Équipe intégrée de la sécurité nationale (EISN) qui œuvrait à la cybersurveillance de sources ouvertes.

Or, la mise en preuve des documents électroniques (messages) n'a pas été de tout repos lors du procès. En défense, on s'oppose à leur production et on allègue également que la méthode de travail des policiers dans la conservation de la preuve a mené à une destruction de celle-ci qui nuit de manière irrémédiable la défense pleine et entière de M. Hamdam, contrairement à l'article 7 de la Charte canadienne. La communication proposée vise à analyser les balises et commentaires du tribunal pour la mise en preuve efficace de documents provenant de sources ouvertes.

Maxime Laroche, Expert-conseil juridique (ENPQ), Procureur aux poursuites criminelles et pénales

15h00 (16) Un pas vers l'« Evidence Based Policing »

Table ronde sur les bonnes pratiques en matière de médias sociaux

Les médias sociaux sont de plus en plus utilisés par les organisations policières, et ce dans divers pays. Cette augmentation de l'utilisation d'outils tels que Facebook, YouTube ou encore Twitter, a mené plusieurs organisations et chercheurs à évaluer l'efficacité ainsi que les avantages et désavantages qu'entrainent les diverses formes d'utilisation de ces plates-formes par les organisations policières. Par diverses formes d'utilisation, on peut penser par exemple au policier qui voudrait utiliser Facebook pour solliciter l'aide du public alors que dans un tout autre contexte ce dernier pourrait vouloir utiliser Facebook pour collecter des informations permettant de localiser un individu. Au sein même de ces formes particulières d'utilisation, plusieurs variantes peuvent exister. Par exemple, est-il plus profitable de mettre la photo d'un individu recherché sur une publication qui sera diffusée sur le compte Facebook de l'organisation ou est-il préférable de mettre uniquement un lien référant vers le site Web de l'organisation ? Dans un tout autre contexte, vaut-il mieux centraliser l'OSINT ou le décentraliser ? Les conclusions qui découlent de ce type d'études seront présentées.

*Une période sera réservée aux gestionnaires et responsables de l'intégration des médias sociaux dans les pratiques pour faire part des enjeux qu'ils rencontrent et avoir l'avis des autres participants (mise en place des directives, choix relatif à l'accessibilité, etc.). Les conférencières présenteront également certains concepts de l' «Evidence Based Policing» permettant de comprendre comment il est possible d'évaluer l'efficacité, les avantages et les désavantages qu'entraine une pratique particulière.

Brigitte Poirier et Julie Delle Donne, Candidates au doctorat, École de Criminologie de l'Université de Montréal

15h30 Mot de la fin (Salle C-3061)

16h00 4 @ 7 (Salle C-2081/2083)

Session de présentation d'affiches scientifiques

« jvais me faire un dossier sur lui et jvais le tuer staprem » : En quoi un tweet est-il menaçant?

Jessica Rioux-Turcotte[1,2], Marty Laforest[1,2], Francis Fortin[3,4] et Geneviève Bernard Barbeau[1,2]

[1]Université du Québec à Trois-Rivières, [2]Centre de recherche interuniversitaire sur le français en usage au Québec (CRIFUQ), [3]Université de Montréal, [4]Centre international de criminologie comparée (CICC)

L'utilisation du « *machine learning* » dans la détection de menace sur *Twitter*.

Sébastien Meloche, Francis Fortin, Rajat Bhateja et Benjamin Fung

Suivez le CICC

https://www.facebook.com/CICCUdeM

www.youtube.com/user/cicctv

www.fr.twitter.com/CICCTweet