

Sur les traces des cybercriminels

CYBERCRIMINALITÉ Les criminels perfectionnent sans cesse les méthodes qu'ils utilisent pour accéder aux biens d'autrui par l'intermédiaire d'Internet. Avec la nouvelle filière de «Master of advanced studies in digital forensics & cyber investigation», la Haute école spécialisée bernoise BFH prend en compte les besoins de l'économie, de l'armée et des autorités judiciaires.

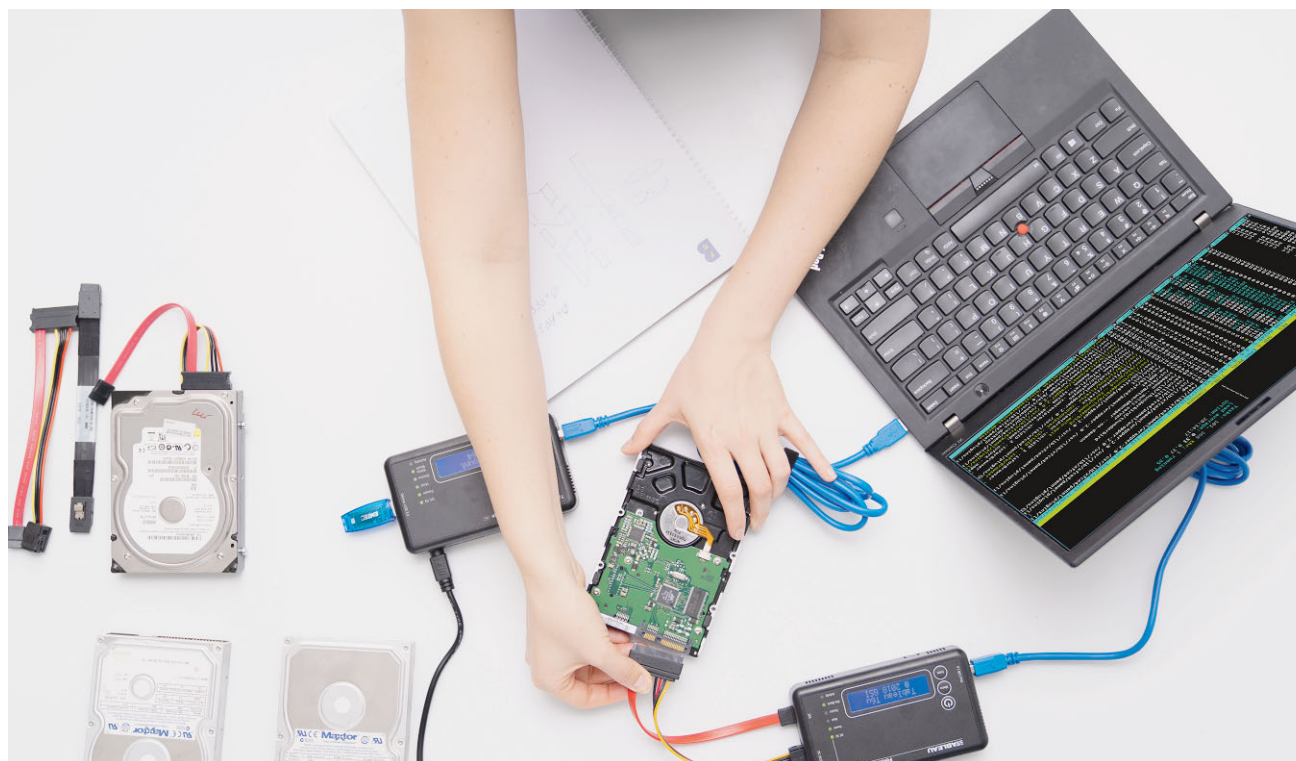
PAR MARC SCHIESS

Les cambrioleurs de banques à l'ancienne ont un gros problème: l'argent circule de plus en plus sous forme numérique et la salle des serveurs remplace désormais le coffre-fort. Bonne nouvelle pour les honnêtes gens: la violence brute ou l'art de creuser des tunnels ne permettent plus d'accéder au butin. Mais il y a aussi une mauvaise nouvelle: des criminels ingénieux s'attaquent désormais non

CAMPUS BIENNE **Page spéciale**
Coup de projecteur sur le département Technique et Informatique

seulement aux grands établissements, mais aussi aux petits poissons comme vous et moi, et cela de manière numérique, sans se salir les mains. Et si les voleurs, il y a dix ans, profitaient essentiellement des points faibles des appareils, ils visent désormais surtout la fragilité humaine.

Tout cela, peu de monde le sait aussi bien que Bruce Nikkel. Ce Canadien travaille depuis plus de 20 ans comme expert en cybersécurité auprès d'une banque suisse. La division de criminalistique qu'il a fondée existe depuis 15 ans. Bruce Nikkel est impressionné par la force avec laquelle Internet a chamboulé le monde au cours des dernières décennies: «Le changement numérique est phénoménal: de toutes nouvelles compétences sont indispensables pour combattre le crime.» Son autre activité d'enseignant au département Technique et informatique TI de la BFH, ainsi que son réseau international, ont ouvert des portes au professeur: la filière de master en criminalistique numérique et cyberenquête, dont Bruce Nikkel est l'initiateur, démarrera en avril 2020 à la BFH. Les cours-blocs d'une semaine seront donnés à Berne en anglais par les meilleur-e-s spécialistes des domaines concernés à l'échelle internationale. L'expert en cybersécurité s'attend à ce que les participant-e-s viennent de toute l'Europe, parce que les compétences proposées sont très particulières: «Les universités européennes ne proposent pas encore ce genre de programmes très ciblés.» Il n'est toutefois pas question de créer un centre



Extraire et analyser des preuves provenant de diverses sources numériques.

de formation pour policiers, souligne le professeur: «La police dispose déjà de ressources et de formations pour la cybercriminalité.» Ce sont surtout des entreprises internationales actives dans le domaine de la finance et de l'assurance qui ont manifesté leur intérêt, ainsi que l'armée et des autorités judiciaires. Dans le cadre du master, on apprend comment traquer, étudier, analyser et reconstruire les actes criminels dans le cyberspace, de manière scientifique et systématique. En cas de crime, l'enquête et l'analyse sont suivies d'une communication à la police.

Jouer au chat et à la souris

Le domaine de la criminalistique numérique est très complexe. Seul-e-s les spécialistes comprennent ce qui se cache derrière des termes tels que «hashing», «anti-forensics», «super timelines» ou «Rekall». «Pour simplifier, on peut dire



Les cybercriminels sont intelligents: c'est comme jouer au chat et à la souris en devant résoudre des énigmes chaque jour.

BRUCE NIKKEL
EXPERT EN CYBERSÉCURITÉ

qu'on apprend, dans le cadre du master, comment faire des recherches dans Internet par exemple avec l'Open Source Intelligence, comment prélever des preuves ou comment analyser un smartphone ou un disque dur», détaille Bruce Nikkel. Lui-même se décrit comme un passionné «typique», qui a attrapé le virus de l'informatique en 1983 en regardant le film «WarGames». Le défi intellectuel le fascine toujours. «Les cybercriminels sont intelligents: c'est comme jouer au chat et à la souris en devant résoudre des énigmes chaque jour.» Le niveau de difficulté de ce jeu très sérieux passe souvent à «extrêmement complexe», puisque contrairement aux actes illicites commis dans le monde réel, ces attaques ne connaissent pas de «lieux du crime». La coopération entre autorités judiciaires du monde entier s'est aussi fortement accrue ces dernières décennies. Europol et Interpol sont devenus des

partenaires importants des enquêteurs, tout comme, en Suisse, le Centre national pour la cybersécurité (qui a succédé à la centrale MELANI). «Le secteur public a compris qu'il valait la peine de se faire aider par le secteur privé pour contrer ce type de criminalité», pense Bruce Nikkel.

Les perspectives de ce domaine professionnel encore relativement jeune sont excellentes. Avec l'évolution technologique, les criminels disposent en effet de nouveaux outils qui peuvent tromper même des personnes à l'esprit très critique. Le professeur considère que les attaques d'ingénierie sociale – notamment à l'aide de la technologie «deep fake» – constituent le plus gros défi. Avec l'intelligence artificielle, elles permettent de créer des vidéos étonnamment réalistes d'une personne: il suffit de disposer de quelques photos de cette dernière. Même la voix peut être imitée si l'on a suffisamment d'enregistrements audio à l'avenir, si l'un de vos proches vous demande par téléphone de lui remettre de l'argent, il peut donc valoir la peine de vous assurer – en lui posant quelques questions sur son passé – que c'est bien votre mari ou votre petite-fille qui est à l'appareil.

LES DÉTAILS DU MASTER

La filière de master en criminalistique numérique et cyberenquête, qui débute en avril 2020, inclut quatre semestres de CAS avec des cours, ainsi qu'un mémoire final de master. Chaque semestre, quatre modules d'une semaine doivent être suivis. Une partie d'entre eux peuvent être choisis individuellement. L'ensemble de la filière correspond à 60 points ECTS et coûte 34 000 francs. Le public visé comprend les criminalistes expérimentés qui souhaitent élargir leurs compétences techniques en criminalistique numérique et cyberenquête, ainsi que les ingénieur-e-s et technicien-ne-s expérimentés qui souhaitent entrer dans le monde professionnel de la cyberenquête. MSC