

Le ministère de l'Intérieur
au Forum international
de la cybersécurité (FIC)
les 22 et 23 janvier 2019 à Lille

fiers.new

rror_ob

ck the des

= modifier

b)) # modifier

ts[0]

t = 1

two objects

object""

one

LE MOT DU MINISTRE

.....

Face aux nouvelles menaces, le ministère de l'Intérieur apporte de **nouvelles protections**.



Pour sa onzième édition et pour la sixième année consécutive, le ministère de l'Intérieur est partenaire du FIC. Il y est présent pour exposer au public les grands axes de sa stratégie de réponse aux risques et aux enjeux nés de la **révolution numérique**.

Les cybermenaces nous concernent tous, acteurs du public comme du privé, citoyens et institutions et les enjeux sont immenses : souveraineté, défense des intérêts fondamentaux de l'État, lutte contre le terrorisme, développement économique, proximité du service public et, avant tout, protection de nos concitoyens.

Au titre de ses différentes missions et de sa proximité avec les usagers sur le territoire national, le ministère de l'Intérieur s'est doté de longue date d'un dispositif complet de lutte contre ces risques dans leur ensemble. Pour tenir compte de l'évolution de la cybercriminalité, **la gendarmerie, la police et les services de renseignement ont renforcé leur action sur le web**, en développant des techniques et des moyens d'investigation appropriés. Sur le terrain, des policiers et des gendarmes spécialement formés poursuivent les auteurs d'infractions. Parallèlement, des personnels interviennent de manière préventive auprès d'enfants, d'adultes, d'entreprises et de collectivités.

Notre ministère a pour mission d'**apporter la confiance et la sécurité dans l'usage du numérique des citoyens**, par une réponse collective et coordonnée face à des pratiques criminelles, délictuelles ou déloyales qui ne cessent de se développer : cybercriminalité, espionnage, propagande, sabotage ou exploitation excessive de données personnelles.

L'action du ministère de l'Intérieur s'inscrit dans le contexte d'un changement majeur de la société où la part du numérique dans les services, les objets et les métiers ne cesse de croître. Enjeu national, cette transition numérique est porteuse d'innovation et de croissance. Pour accompagner tous les usagers et répondre à leurs attentes, **le ministère développe de nouveaux outils dans le domaine des «civic tech»** : le répertoire électoral unique, la plateforme de signalement des violences sexuelles et sexistes, des outils dédiés à l'automobiliste et à l'automobile, un chatbot pour faciliter la recherche d'informations et les démarches administratives.

Et c'est en plaçant la sécurité comme garantie des libertés dès la conception de ces nouvelles technologies que nous préserverons la confiance de nos concitoyens. Thème de cette année, la **«security and privacy by design»** est ainsi l'un des préalables indispensables pour anticiper et prévenir les risques cyber de demain, en intégrant dès la conception la sécurité de nos systèmes d'information et des outils qui sont mis au service des usagers, tout en protégeant l'exercice des libertés fondamentales.

Les innovations présentées cette année au FIC marquent la volonté du ministère de faire des technologies du numérique des outils de modernisation de nos missions au service du citoyen.

Christophe Castaner

LA STRATÉGIE DU MINISTÈRE CONTRE LES CYBERMENACES

La stratégie ministérielle de lutte contre les cybermenaces, publiée en 2017, définit les objectifs spécifiques du ministère de l'Intérieur au regard du cadre fixé par la stratégie nationale de sécurité du numérique.

Elle s'inscrit dans le cadre des 5 objectifs définis par le Premier ministre.

1 – Défendre les intérêts fondamentaux de la Nation :

- organiser la réponse face aux cybermenaces ;
- anticiper et diffuser les évolutions du droit relatif aux cybermenaces ;
- protéger ses systèmes d'information ;
- contribuer à la sensibilisation et aux enjeux de protection des infrastructures stratégiques ;
- intégrer les cybermenaces dans la gestion de crise ;
- coopérer avec les acteurs économiques.

2 – Assurer la confiance numérique des utilisateurs et la protection de leurs données :

- renforcer l'efficacité de la lutte contre la cybercriminalité ;
- assurer une prise en charge des victimes de cybermalveillances ;
- garantir aux usagers une identité numérique forte en mettant en oeuvre des services électroniques de confiance.

3 – Assurer la prévention par la sensibilisation et la formation sur les territoires :

- sensibiliser l'ensemble des personnels du ministère et former des personnels spécialisés ;
- généraliser les actions de sensibilisation au sein de la société civile.

4 – Favoriser la politique industrielle de sécurité du numérique :

- soutenir l'offre industrielle de cybersécurité ;
- préparer l'avenir par le soutien de la recherche et du développement.

5 – Contribuer à la souveraineté numérique nationale et européenne ainsi qu'à la stabilité du cyberspace :

- influencer et diffuser la parole du ministère au niveau international ;
- promouvoir le renforcement des capacités de lutte contre les cybermenaces ;
- soutenir l'autonomie stratégique de la France et de l'Union européenne en matière de sécurité du numérique.

La cybercriminalité suscite désormais la mobilisation des institutions internationales (Conseil de l'Europe, Union Européenne, ONU, Interpol, Europol...). Dans ce contexte, le ministère de l'Intérieur renforce depuis plusieurs années son dispositif dans le cadre d'une démarche stratégique d'ensemble. Une grande partie des approches implique la coopération internationale, essentielle pour contrer une criminalité par essence transfrontière. La direction de la coopération internationale (DCI) décline cet effort par un plan de mesures et une doctrine qui soutiennent de nombreuses actions à l'international, appuyées par l'ensemble de nos 74 services de sécurité intérieure à l'étranger.

LES SERVICES PRÉSENTS SUR LE STAND DU MINISTÈRE DE L'INTÉRIEUR

Plus de 35 experts cyber du ministère sont à la disposition du public pour présenter leurs missions et engager le dialogue.

Le stand est organisé en cinq pôles thématiques où sont présentés divers outils et animations :

• Le pôle Cybercriminalité :

La sous-direction de la lutte contre la cybercriminalité (SDLC) de la direction centrale de la police judiciaire présente la plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (**PHAROS**) ainsi que **RISE**, logiciel permettant de tester l'empreinte numérique des usagers du web.

La gendarmerie nationale quant à elle propose une démonstration de la plateforme PERCEVAL pour les victimes d'usage frauduleux des cartes bancaires sur internet et une présentation, par le centre de lutte contre la cybercriminalité numérique (C3N), de son **Réseau Cybergend** (réseau de gendarmes spécialistes des nouvelles technologies, dédiés à la lutte contre la cybercriminalité).

La police nationale et la gendarmerie nationale, à travers le service des technologies et des systèmes d'information de la sécurité intérieure (ST-SI²) aborde le thème de la **sécurité des postes de travail** et la mobilité.

La brigade d'enquêtes sur les fraudes aux technologies de l'information de la préfecture de Police de PARIS est présente pour conseiller et sensibiliser le public aux **risques d'Internet**.

• Le pôle Innovation :

La SDLC présente le réseau des référents cybermenaces qui coordonne les actions de lutte, de sensibilisation et de prévention dans le domaine de la **cybercriminalité**.

Plusieurs animations sont proposées par la gendarmerie nationale : la **brigade numérique** qui permet de joindre en ligne la gendarmerie 24h/24, la **photogrammétrie 3D** et le traitement automatisé des traces d'outils par l'Institut de recherche criminelle de la gendarmerie (IRCGN).

La solution de radiocommunication et le **déploiement de réseaux tactiques** pour les besoins des unités d'intervention du ministère de l'Intérieur est exposée par le ST-SI².

La mission prospective et management de l'innovation (**MPMI**) de la **DOSTL** (direction opérationnelle du transports et de la logistique) de la préfecture de Police présentera des exemples d'**applications de l'intelligence artificielle** : Le traitement de la **vidéo verbalisation**, **les lunettes connectées**...

• Le pôle Civic Tech :

La Direction des Systèmes d'Information et de Communication propose la démonstration de plusieurs outils dont :

- **Histovec** qui permet de retracer l'historique d'un véhicule d'occasion lors de son achat.
- **Candilib** : outil permettant de préparer le passage du permis de conduire en candidat libre.

L'utilisation de la plateforme de **signalement des violences sexuelles et sexistes** est présentée conjointement par la gendarmerie nationale et la police nationale.

La délégation à l'information et à la communication propose de découvrir en avant-première son **chatbot** dont la mission est de faciliter la recherche d'informations et les démarches administratives.

• Le pôle Coopération internationale :

La direction de la coopération internationale présente ses actions dans le domaine cyber : mission de **coopération technique** et développement de compétences en matière de lutte contre la cybercriminalité, promotion au niveau international et européen d'une vision stratégique cyber globale en phase avec les besoins du ministère de l'Intérieur, appui aux entreprises françaises à l'export.

• Le pôle recrutement :

Les services du ministère (direction des systèmes d'information et de communication, police judiciaire, gendarmerie nationale et service du haut fonctionnaire de défense) recrutent **des analystes en cybermenaces**, des chargés de stratégie de détection, des responsables qualité et sécurité, des ingénieurs cybersécurité, des ingénieurs et techniciens SIC, des enquêteurs...

Pour une vision d'ensemble des services du ministère de l'Intérieur compétents en matière de cybersécurité, consultez notre brochure sur www.interieur.gouv.fr/FIC

L'ACTION DU MINISTÈRE EN CHIFFRES

- **Près de 3 101 signalements de contenus illicites reçus par semaine** sur internet-signalement.gouv.fr en 2018 ;
- **978 millions de personnes au monde sont concernées par une cyberattaque chaque année ;**
- **146 appels reçus par jour** par la plateforme téléphonique *Info-Escroqueries* (0805 805 817, du lundi au vendredi de 9h à 18h30 – appel gratuit) ;
- **Près de 140 spécialistes cyber, policiers et gendarmes, mobilisés au sein de la sous-direction de la lutte contre la cybercriminalité** (Direction centrale de la police judiciaire), qui regroupe notamment la plate-forme de signalement de contenus illicites (PHAROS) et la ligne téléphonique INFO-ESCROQUERIES ;
- **508 policiers investigateurs en cybercriminalité (ICC)** répartis partout en France ;
- **60 gendarmes experts en applications innovantes**, regroupés dans la division criminalistique ingénierie et numérique, au sein de l'institut de recherche criminelle de la gendarmerie nationale (IRCGN), qui relève du pôle judiciaire de la gendarmerie nationale (PJGN) ;
- **150 enquêteurs numériques de la gendarmerie chargés des investigations sur Internet et 110 N'Tech** spécialisés dans la criminalistique numérique au sein du réseau Cybergend ;
- **4 300 enquêteurs numériques de proximité de la gendarmerie** qualifiés pour appréhender le volet cyber dans la prévention et la lutte contre la délinquance sur lesquels s'appuie le réseau Cybergend ;
- **35 gendarmes chargés de l'analyse de la cybercriminalité** au sein du centre de lutte contre les criminalités numériques (C3N) ;
- **1 400 000 enfants de CM2 sensibilisés aux dangers de l'internet depuis 2013** grâce à l'opération de prévention « Permis Internet pour les enfants » ;
- **74 services de sécurité intérieure rattachés à la Direction de la coopération internationale (DCI)** soit 291 personnels de la police et la gendarmerie dont 4 experts techniques internationaux spécialisés dans le domaine cyber et un dispositif de suivi des questions cyber en direction centrale ;



- **92 actions d'envergure menées en 2018 par la Direction de la coopération internationale**, soit 14 visites, séminaires et stages en France ainsi que 78 actions de formation à l'étranger;
- **70 investigateurs en cybercriminalité (ICC) exercent leurs missions au sein de la préfecture de Police de Paris** (dont 19 à la brigade d'enquêtes sur les fraudes aux technologies et à l'information - BEFTI);
- **La BEFTI traite 250 saisines par an sur le ressort de Paris et des 3 départements de la petite couronne;**
- **1 500 conférences de prévention assurées par la Direction générale de la sécurité intérieure (DGSI) auprès des entreprises.**
- **Depuis son lancement en juin 2018, Perceval, la plateforme de signalement des fraudes à la carte bancaire a reçu près de 63 000 signalements** (pour 246 000 usages frauduleux représentant un préjudice total de plus de 30M€) soit 300 signalements par jour en moyenne (record atteint sur la période des achats de Noël - du 1^{er} au 17 décembre 2018 – avec 466 signalements par jour).



LE SAVIEZ-VOUS ?

- Pour déposer plainte en cas d'actes de cybercriminalité ou de cybermalveillance, les internautes peuvent se rendre dans le commissariat ou la brigade de gendarmerie de leur choix. C'est le principe du guichet unique qui s'applique, comme pour tout acte délictueux ou criminel.

Astuce : pour gagner du temps et prendre rendez-vous, il est possible de déposer une préplainte en ligne; cela permet de prendre rendez-vous :

Site : <https://www.pre-plainte-en-ligne.gouv.fr>

<https://www.prefecturedepolice.interieur.gouv.fr/Vous-aider/Vous-etes-victime/Deposer-plainte/Plainte-et-pre-plainte>

- Alors que le permis internet est proposé par les gendarmes depuis 2013 aux élèves de CM2, au titre de la prévention des risques sur internet, ces actions sont également assurées par les forces de police depuis septembre 2015 (sur tout le territoire national, à Paris et dans la petite couronne).
- Un état de la menace liée au numérique, établi par l'ensemble des services du ministère de l'Intérieur sous la coordination de la délégation ministérielle aux industries de sécurité et à la lutte contre le cybermenaces (DMISC), dresse un panorama complet des enjeux, des menaces et des réponses apportées par le ministère en matière de cybersécurité.
Il est téléchargeable à l'adresse suivante : <https://www.ladocumentationfrancaise.fr/rapports-publics/184000391/index.shtml>

LES OUTILS À CONNAÎTRE

Info-escroqueries

Créée en 2009, la plateforme téléphonique d'information et de prévention sur les escroqueries sur Internet est destinée aux victimes d'escroqueries, qui peuvent recevoir des conseils en termes d'information et de prévention.

0805 805 811 (Du lundi au vendredi de 9h à 18h 30, appel gratuit).

PHAROS

Lancée le 6 janvier 2009, la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) permet aux internautes de signaler les contenus ou les comportements présumés illicites au regard du droit pénal (courriels, sites d'escroqueries), quel que soit le type d'infraction.

www.internet-signalement.gouv.fr.

Dispositif d'aide aux victimes de cybermalveillance

(en collaboration avec le Secrétariat d'État chargé du Numérique)

www.cybermalveillance.gouv.fr

Victime d'un usage frauduleux de votre carte bancaire sur internet?

(Vous n'êtes pas à l'origine de la transaction et êtes toujours en possession de la carte)

Plateforme PERCEV@L de recueil de signalement : téléservice accessible sur le site en ligne servicepublic.fr

Portail de signalement de violences sexuelles et sexistes :

Victime ou témoin d'un acte de violence sexuelle ou sexiste, sur le lieu de travail, dans l'espace public, ou dans le cadre familial, une plateforme d'écoute animée par des policiers et des gendarmes sont à votre écoute sous la forme d'un tchat anonyme et gratuit.

www.signalement-violences-sexuelles-sexistes.gouv.fr

Autres outils

- Spams : www.signal-spam.fr
- Phishing : www.phishing-initiative.com
- SIGNALER LES CONTENUS ILLICITES notamment pédopornographiques : <https://www.pointdecontact.net/>

POUR EN SAVOIR PLUS

contacts :

Ministère de l'Intérieur / Délégation à l'information et à la communication Unité du porte-parolat et des relations presse:

unitemedias-dicom@interieur.gouv.fr

01 40 07 26 78

Gendarmerie nationale - Service d'information et de relations publiques des armées (SIRPA):

sirpag-dggn@gendarmerie.interieur.gouv.fr

06 88 65 18 50

Police nationale - Service d'information et de communication de la police nationale (SICoP):

sicopmedia@interieur.gouv.fr

01 40 07 60 70

Préfecture de Police de Paris:

Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC):

<https://www.interieur.gouv.fr/Le-ministere/Organisation/Delegue-ministeriel-aux-industries-de-securite-et-a-la-lutte-contre-les-cybermenaces>

Plus d'information: interieur.gouv.fr/FIC2019



Twitter@Place_Beauvau
www.facebook.com/ministere.interieur
Partagez avec #FIC2019

Crédits photos: © Adobe Stock © Y.Malenfer © F.Pellier © F.Balsamo © M.Alexandre

