

Le ministère de l'Intérieur au Forum international de la cybersécurité (FIC)

Les 25 et 26 janvier 2016 à Lille



MINISTÈRE
DE
L'INTÉRIEUR

LA PRÉSENCE DU MINISTÈRE DE L'INTÉRIEUR AU FIC

- Cette année, le ministère de l'Intérieur est partenaire du FIC pour la 8^e édition et la troisième année consécutive. Chargé d'assurer l'ordre public, le ministère ne limite pas son action au domaine matériel. La gendarmerie, la police et les services de renseignement investissent au quotidien la cybersphère pour lutter contre les menaces tournées vers les internautes.
Depuis les attentats de novembre 2015 et le déclenchement de l'état d'urgence, les services ont renforcé leur action sur le web pour prévenir tout nouveau drame.
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.
- L'action du ministère s'inscrit dans l'évolution 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, mais aussi de risques pour l'État, les acteurs économiques et les citoyens. La confiance et la sécurité dans le numérique appellent une réponse collective et coordonnée pour faire face à des pratiques criminelles, délictuelles ou déloyales — cybercriminalité, espionnage, propagande, sabotage ou exploitation excessive de données personnelles.
- Le ministère de l'Intérieur participe au FIC à plusieurs titres :
 - le discours du ministre, prononcé mardi 26 janvier 2016 à 9 h ;
 - les interventions de personnalités spécialisées dans les ateliers et le plateau TV ;
 - l'animation par 35 experts cyber d'un stand organisé en 4 pôles thématiques (voir rubrique dédiée).



L'action du ministère de l'Intérieur s'inscrit dans la stratégie nationale pour la sécurité du numérique. Annoncée le 16 octobre 2015 par le Premier ministre, celle-ci dispose : « la France développe un usage du cyberspace conforme à ses valeurs et qui protège la vie numérique de ses citoyens. Elle accroît sa lutte contre la cybercriminalité et l'assistance aux victimes d'actes de cyber malveillance ».

Sous le pilotage du préfet chargé de la lutte contre les cybermenaces, la mise en œuvre du plan d'actions ministériel vise à atteindre les 3 objectifs stratégiques suivants :

- **Mieux anticiper le phénomène cyber criminel et accompagner les victimes de cyber malveillance**

Le ministère de l'Intérieur s'attache à améliorer l'accueil des victimes de cyber malveillance, en s'impliquant dans la démarche interministérielle d'accompagnement de ces victimes, notamment les particuliers et les petites et moyennes entreprises, et en mobilisant les réseaux territoriaux de l'État ainsi que les acteurs privés. L'analyse des données recueillies sur le terrain permettra en outre une meilleure perception de l'état réel de la menace et de mieux anticiper sur son évolution.

- **Mieux dialoguer avec les acteurs cyber**

La filière des industries de sécurité est, par définition, un acteur majeur de la lutte contre les cybermenaces. Le ministère de l'Intérieur soutient les nombreuses entreprises qui contribuent à la sécurité numérique et qui développent des solutions innovantes pour la France, mais aussi à la conquête des autres marchés.

Le groupe de contact permanent mis en place avec les grands acteurs de l'Internet après les attentats du début 2015 a démontré l'intérêt d'un travail commun approfondi, tant en termes opérationnels dans le domaine de l'application de la loi, que pour la sensibilisation du public ou la diffusion de messages pendant la crise. De nouveaux groupes de travail seront lancés dans différents secteurs concernés au premier chef par la fraude numérique et la cybercriminalité (banques, assurances, commerce électronique) pour échanger sur ces questions avec les services spécialisés.

- **Adapter le cadre juridique national et international**

L'année 2015 a vu la mise en œuvre de la loi de programmation militaire du 18 décembre 2013 et de la loi du 13 novembre 2014 autorisant le blocage et le déréférencement de sites hébergeant des contenus illicites, ainsi que celle des lois du 24 juillet 2015 relative au renseignement et du 20 novembre 2015 relative à l'état d'urgence, autant de textes contenant des dispositions visant à adapter notre droit à la lutte contre les cybermenaces.

En outre, la dimension transfrontière des cybermenaces impose de définir les mécanismes d'entraide judiciaire les mieux adaptés à l'obtention de la preuve numérique de la part de nos partenaires étrangers, publics ou privés : ainsi, après la récente extension de la possibilité pour les enquêteurs d'intervenir sous pseudonyme aux fins d'identifier puis d'interpeller des criminels, l'adoption d'un nouveau critère de compétence territoriale devrait permettre à la Justice française de connaître des faits de cybermalveillance commis en dehors du territoire national, dès lors que la victime réside en France.

Pour en savoir plus sur le plan d'action ministériel, consultez notre brochure sur www.interieur.gouv.fr/FIC



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 4 pôles thématiques

- **Lutter contre la cybercriminalité**

- Sous direction de lutte contre la cybercriminalité (Direction centrale de la police judiciaire)
- Plate forme de signalement des contenus illicites sur internet (Pharos)
- Plate forme téléphonique de conseils aux particuliers et entreprises victimes sur le net (Info-Escoqueries)
- Brigade d'enquête sur les fraudes aux technologies de l'information et de la communication (Préfecture de police de Paris)
- Réseau Cybergend de la gendarmerie : gendarmes N-TECH (spécialistes des nouvelles technologies) et pôle central : le Centre de lutte contre les cybercriminalités numérique (C3N).

- **Prévenir les risques**

- Gendarmerie : Sous direction de l'anticipation opérationnelle, section intelligence économique et territoriale
- Gendarmes et policiers : le permis internet (prévention auprès d'élèves de CM2 partout en France).
- Sous direction de lutte contre la cybercriminalité, division de l'anticipation et de l'analyse (Direction centrale de la police judiciaire)
- Brigade d'enquête sur les fraudes aux technologies de l'information et de la communication (Préfecture de police de Paris)

- **Innover en cybersécurité**

- Pôle judiciaire de la gendarmerie nationale (Institut de recherche criminelle et service central de renseignement criminel)
- Réseau Cybergend de la gendarmerie : gendarmes N-TECH (spécialistes des nouvelles technologies) et pôle central : le Centre de lutte contre les criminalités numériques (C3N).
- Service des technologies et des systèmes d'information de la sécurité intérieure : ST(SI)²
- Délégation ministérielle aux industries de sécurité

- **S'engager à l'international**

- Direction de la coopération internationale (DCI)

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



- En 2015 : **3 600 signalements de contenus illicites reçus par semaine** sur internet-signalement.gouv.fr ;
- En 2015 : **90 appels reçus par jour** par la plateforme téléphonique *Info-Escroqueries* (0811 02 02 17, du lundi au vendredi de 9h à 18h) ;
- Au 1^{er} octobre 2015 : **plus de 100 spécialistes cyber mobilisés au sein de la sous direction de lutte contre la cybercriminalité** (Direction centrale de la police judiciaire), qui regroupe notamment la plateforme de signalement de contenus illicites et la ligne téléphonique Info-Escroqueries ;
- **1 400 conférences assurées chaque année par la direction générale de la sécurité intérieure (DGSI)** auprès des entreprises sur la protection de l'information et la sécurité numérique ;
- **430 policiers investigateurs en cybercriminalité (ICC)** répartis partout en France ;
- **54 experts de la police technique et scientifique** (service central de l'informatique et des traces technologiques, SCITT) en charge des missions d'analyse et d'exploitation des supports numériques ;
- **59 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 ;
- **Plus de 2 000 enquêteurs spécialisés et réservistes qualifiés pour appréhender le volet cyber** dans la prévention et la lutte contre la délinquance sur lesquels s'appuie le réseau Cybergend ;
- **260 enquêteurs gendarmes N-TECH** spécialisés dans les nouvelles technologies, au sein du réseau Cybergend ;
- **190 référents intelligence économique et 1 600 référents et correspondants sûreté** chargés d'intervenir auprès des commerçants et artisans en zone gendarmerie ;
- **500 gendarmes spécialistes du renseignement cyber répartis partout en France** (réseau des centres d'opération et de renseignement) ;
- **35 gendarmes chargés de l'analyse de la cybercriminalité** au sein du centre de lutte contre les criminalités numériques (C3N) ;
- **450 000 enfants de CM2 sensibilisés aux dangers de l'internet depuis 2013** via des animations pédagogiques assurées par la gendarmerie ;
- Coopération internationale : **74 services de sécurité intérieure** à l'étranger (289 personnels de la police et de la gendarmerie)
- **11 visites, séminaires ou stages dédiés à la lutte contre la cybercriminalité** organisés en France par la direction coopération internationale (DCI) en 2015.
- 28 missions de formation, d'étude ou de dons de matériels **relatives à la lutte contre la cybercriminalité** ont été menées à l'étranger en 2015.



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 criminels.
Astuce : pour gagner du temps, il est possible de faire une pré-plainte en ligne ; cela permet de prendre rdv :
Site : <https://www.pre-plainte-en-ligne.gouv.fr>
- 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 (partout en France, à Paris et dans la petite couronne).

LA PRÉSENCE DU MINISTÈRE DANS LE FORUM

Des représentants du ministère de l'Intérieur participeront à de nombreuses conférences.

	QUAND	QUI	QUOI	OÙ
LUNDI 25 JANVIER 2016	9 H 45	Jean-Yves Latournerie, Préfet chargé de la lutte contre les cybermenaces	Va-t-on vers une crise de confiance des utilisateurs ?	Salle Vauban
	14 H	Général (2S) Marc Watin-Augouard Directeur du centre de recherches de la gendarmerie nationale Chef d'escadron Xavier Leonetti Chef de la section intelligence économique territoriale de la sous-direction de l'anticipation opérationnelle – DGGN	Ethique et cyberspace	Salle Faidherbe
	14 H 30	Lieutenant-colonel Jean-Dominique Nollet (Europol EC3), animateur Commissaire François-Xavier Masson Chef de l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication), Police nationale (DCPJ, Direction centrale de la police judiciaire)	La nouvelle cybercriminalité liée aux données	Salle Artois
	14 H 30	Colonel Bruno Chapuis Chargé de mission à la direction des personnels militaires de la gendarmerie nationale (DPMGN)	Les nouveaux métiers liés aux données	Salle Jeanne de Flandre
	14 H	Myriam Quemener, Magistrate, délégation à la lutte contre les cybermenaces	Procès simulé sur une fuite de données confidentielles	Salle Matisse
	16 H 30	Colonel Eric Freyssinet Conseiller, délégation à la lutte contre les cybermenaces	CeCyF - Signal Spam	Plateau TV

QUAND	QUI	QUOI	OÙ
11 H	Capitaine Catherine Anguille-Blanc Division administration des applications judiciaires du service central de renseignement criminel (SCRC/PJGN)	Data Loss Prevention : enfin quelques solutions matures ?	Salle Matisse
11 H	Colonel Jacques Diacono Chef de l'Office central de lutte contre les atteintes à l'environnement et à la santé publique (OCLAESP)	Santé : la cybersécurité vitale	Salle Faidherbe
14 H 45	Patrick Guyonneau, Délégué adjoint aux industries de sécurité	Le marché européen du numérique : chimère ou réelle opportunité ?	Salle Artois
14 H 45	Lieutenant-colonel Cyril Piat Adjoint au chef du centre de lutte contre les criminalités numérique (C3N) du pôle judiciaire de la gendarmerie nationale (PJGN), animateur Anne Souvira Conseillère cyber du préfet de police de paris (PP) Myriam Quemener, Magistrate, délégation de lutte contre les cybermenaces	Investigations dans le cyberspace : les techniques d'enquête au regard de la protection de la vie privée ?	Salle Vauban
14 H 45	Lieutenant-colonel Patrick Perrot Chef de la division analyse et investigations criminelles du service central de renseignement criminel (SCRC/PJGN)	Big data : l'outil sécuritaire ultime ?	Salle Artois
14 H 45	Colonel Nicolas Duvinage Chef du centre de lutte contre les criminalités numérique (C3N) du pôle judiciaire de la gendarmerie nationale (PJGN)	Cyber threat intelligence : entre mythes et réalité	Salle Artois
14 H 45	CEN Rubens Chef du département Informatique-Electronique de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN/PJGN), animateur Fabrice Mousnier Brigadier-chef, BEFTI (Brigade d'enquêtes sur les fraudes aux technologies de l'information), PP	Analyse forensique : les nouveaux défis	Salle Pasteur
14 H 45	Colonel Franck Marescal Chef de l'observatoire central des systèmes de transport intelligents (OCSTI/PJGN)	De la nécessité de sécurité dans les transports intelligents : challenges et solutions	Salle Eurotop
15 H 10	Commissaire François Beauvois DCPJ / SDLC (Sous direction de lutte contre la cybercriminalité)	«Provadys» les malwares	Plateau TV
16 H 15	Patrick Guyonneau, Délégué adjoint aux industries de sécurité	Présentation du programme européen de recherche et d'innovation en sécurité : Horizon 2020 Sociétés Sûres.	Salle Pasteur

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 ou aux potentielles victimes d'escroqueries, qui peuvent recevoir des conseils en termes d'information et de prévention.

0811 02 02 17 (Du lundi au vendredi de 9h à 18h, prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile).

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.

Autres outils

- Spams : www.signal-spam.fr
- Phishing : www.phishing-initiative.com

POUR EN SAVOIR PLUS

- Le site internet du ministère de l'Intérieur www.interieur.gouv.fr
- Le site internet de la Gendarmerie nationale www.gendarmerie.interieur.gouv.fr
- Le site internet de la Police nationale www.police-nationale.interieur.gouv.fr
- Le site internet du FIC 2016 www.forum-fic.com

contacts :

Ministère de l'Intérieur / Délégation à l'information et à la communication – DICOM-MEDIA

unitemedias-dicom@interieur.gouv.fr
01 40 07 26 78

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

sirpa-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



Twitter@Place_Beauvau#FIC2016
www.facebook.com/ministere.interieur

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

