

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

Les 24 et 25 janvier 2017 à Lille



## LA PRÉSENCE DU MINISTÈRE DE L'INTÉRIEUR AU FIC

---

- Pour sa 9<sup>e</sup> édition et pour la quatrième année consécutive, le ministère de l'Intérieur est partenaire du FIC. Dans un contexte d'état d'urgence et face aux nouvelles menaces et à 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.
- L'action du ministère s'inscrit dans un changement 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 :
  - les interventions de personnalités spécialisées dans le forum ;
  - l'animation par 35 experts cyber d'un stand organisé en 4 pôles thématiques (voir rubrique dédiée).



La stratégie ministérielle de lutte contre les cybermenaces définit les objectifs spécifiques du ministère de l'Intérieur au regard du cadre fixé par la stratégie nationale de sécurité du numérique présentée par le Premier ministre le 16 octobre 2015.

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.

### **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 sa parole 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.



- **3 300 signalements de contenus illicites reçus par semaine** sur [internet-signalement.gouv.fr](http://internet-signalement.gouv.fr) en 2016;
- **80 appels reçus par jour** par la plateforme téléphonique *Info-Escroqueries* (0805805817, du lundi au vendredi de 9h à 18h30 – appel gratuit);
- Au 1<sup>er</sup> octobre 2016 : **plus de 100 spécialistes cyber, policiers et gendarmes, 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;
- **456 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 2 900 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;
- **36 gendarmes chargés de l'analyse de la cybercriminalité** au sein du centre de lutte contre les criminalités numériques (C3N);
- **750 000 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 2016;
- **24 missions de formation, d'étude ou de dons de matériels relatives à la lutte contre la cybercriminalité** ont été menées à l'étranger en 2016 (ce chiffre ne tient pas compte des visites effectuées par des délégations en France à des fins de formation ou d'études par des partenaires étrangers);
- **60 investigateurs en cybercriminalité (ICC) exercent leurs missions au sein de la Préfecture de Police de Paris** (dont 18 la brigade d'enquêtes sur les fraudes aux technologies et à l'information - BEFTI);
- **La BEFTI traite 300 saisines par an**, répond à **1 500 appels téléphoniques** et à plus de **600 mails** d'internautes.





## 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, il est possible de faire une pré-plainte en ligne ; cela permet de prendre rendez-vous :  
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.

### Sur le salon (sur les deux jours):

Présentations dynamiques par IRCGN : **Investigations numériques autour du véhicule connecté**  
**Chef d'escadron Thomas SOUVIGNET** (IRCGN), **capitaine Hervé DAUDIGNY** (IRCGN), **capitaine Olivier REYNAUD** (IRCGN).

	QUAND	QUI	QUOI	OÙ
MARDI 24 JANVIER 2017	12H - 13H30	<b>Lieutenant-colonel Jean-Dominique Nollet</b> (Europol EC3), animateur <b>Commissaire François Beauvois</b> (SDLC), intervenant	<b>A04 – Atelier :</b> « Quelles nouvelles tendances en matière de cybercriminalité ? »	Salle Vauban
	12H - 13H30	<b>Colonel Franck Marescal</b> (Chef de l'Observatoire central des systèmes de transports intelligents - Gendarmerie nationale), animateur.	<b>A06 – Atelier :</b> « Le véhicule connecté et ses nouveaux usages, en toute sécurité »	Salle Rubens
	12H - 13H30	Ouverture par le <b>Général (2S) Marc Watin-Augouard</b> pour la problématique	<b>A09 – Agora :</b> forum parlementaire « 2022, où en est-on de la transformation numérique ? »	Salle Eurotop
	12H15 - 13H15	<b>Colonel Xavier Guimard</b> (sous-directeur au STSI <sup>2</sup> )	<b>Master class sur la Cryptologie</b> – organisé par la chaire Cyber de l'EOGN	Espace FICLab
	16H45 - 19H	<b>Inspecteur général Thierry Delville</b> (DMIS), intervenant sur table ronde	<b>P02 – Séance plénière :</b> « Quel ordre public pour le cyberspace ? »	Salle Vauban

QUAND	QUI	QUOI	OÙ
11H30 - 12H30	<b>Lieutenant-colonel Jean-Dominique Nollet</b> (Europol EC3), intervenant	<b>A13 – Atelier:</b> « Gestion de crise cyber à l'échelle européenne »	Salle Charles de Gaulle
11H30 - 12H15	<b>Colonel Éric Freyssinet</b> (DMISC)	<b>Master class:</b> « Code pénal et lutte contre la cybercriminalité: propositions pour une meilleure efficacité juridique »	Espace FICLab
11H30 - 13H30	<b>Commissaire François-Xavier Masson</b> (Chef OCLCTIC), intervenant	<b>A16 – Agora:</b> « Comment renforcer la coopération internationale en matière de cybersécurité »	Salle Eurotop
11H30 - 13H	<b>Général (2S) Marc Watin-Augouard,</b> animateur	<b>A18 – Agora:</b> « le droit du robot »	Agora
11H30 - 13H	<b>Myriam Quemener</b> Administrateur général - DMISC - Ministère de l'Intérieur <b>Ronan Doare</b> Directeur du CREC - ECOLES DE SAINT-CYR COETQUIDAN <b>Gérard de Boiboissel</b> Ingénieur de recherche - CREC - SAINT-CYR / CHAIRE CYBERSECURITE ET CYBERDEFENSE <b>Marc Hecker</b> Directeur des publications - IFRI <b>Cécile Doutriaux</b> Avocate - DOUTRIAUX-VILAR & ASSOCIES <b>Michel Vilar</b> Avocat - Barreau de Strasbourg	<b>A20 – Atelier:</b> « Accusé, levez-vous ! Une simulation de procès relatif à l'apologie du terrorisme sur les réseaux sociaux »	Salle Faidherbe
16H - 17H	<b>Myriam Quemener</b> Administrateur général - DMISC - Ministère de l'Intérieur <b>Lieutenant-colonel Fabien Streibel</b> (IRCGN/DCIN), animateur, <b>Chef d'escadron Thomas Souvignet</b> (IRCGN/INL), intervenant	<b>A22 – Atelier:</b> « Investigations numériques: défis et solutions »	Salle Eurotop
16H - 17H	<b>Lieutenant-Colonel Christophe Le Gallo</b> (Adjoint chef Office OCLAESF), intervenant	<b>A23 – Atelier:</b> « La santé peut-elle être connectée en toute sécurité ? »	Salle Van Gogh
16H - 17H	<b>Chef d'escadron Karine Beguin</b> (PJGN/C3N), intervenant <b>Commissaire Sylvie Sanchis</b> (PP/BEFTI), intervenant	<b>A26 – Atelier:</b> « Ransomwares: quelles solutions pour ces nouvelles menaces multiformes ? »	Salle Jeanne de Flandre
16H - 17H	<b>Colonel Nicolas Duvinage</b> (Chef du C3N), animateur	<b>A27 – Atelier:</b> « Blackmarket: la face cachée du web »	Salle Vauban

## 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.

0805 805 811 (Du lundi au vendredi de 9h à 18h30, 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](http://www.internet-signalement.gouv.fr).

### Autres outils

- Spams : [www.signal-spam.fr](http://www.signal-spam.fr)
- Phishing : [www.phishing-initiative.com](http://www.phishing-initiative.com)

## 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](mailto: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](mailto: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](mailto:sicopmedia@interieur.gouv.fr)  
01 40 07 60 70

### Préfecture de Police de Paris :

[www.prefecturedepolice.interieur.gouv.fr/Cybersecurite/Les-actions-PP](http://www.prefecturedepolice.interieur.gouv.fr/Cybersecurite/Les-actions-PP)

Plus d'information : [interieur.gouv.fr/FIC2017](http://interieur.gouv.fr/FIC2017)



[Twitter@Place\\_Beauvau#FIC2017](https://twitter.com/Place_Beauvau#FIC2017)  
[www.facebook.com/ministere.interieur](https://www.facebook.com/ministere.interieur)

