

IN.CRT | INSTITUT NATIONAL CYBERSÉCURITÉ ET RÉSILIENCE DES TERRITOIRES

PARTENAIRES :



CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique



**BANQUE des
TERRITOIRES**
GROUPE CAISSE DES DÉPÔTS

L'Institut National pour la Cybersécurité et la Résilience des Territoires (IN.CRT) a été fondé en juin 2020 .

Il est établi à Vannes (Morbihan).

Il a pour ambition de compléter les efforts fait au niveau national en termes de cybersécurité (ANSSI, Cybermalveillance, PEC...).

Il part des territoires et de leurs problèmes concrets : attractivité, transformation numérique, sécurité (des collectivités, des citoyens, des entreprises, des infrastructures locales), accroissement massif des cyber agressions, révolution technologique, télétravail...

Les fondateurs de l'institut ont des parcours divers qui se complètent : experts en cybersécurité, experts des territoires, officiers et élus locaux.

Conseil d'administration – 2021

- ❖ Général d'Armée (2S) Marc WATIN-AUGOUARD
- ❖ Général de Brigade (2S) Olivier KEMPF
- ❖ Professeur Jean PEETERS
- ❖ Madame Anne LE HENANFF
- ❖ Monsieur Bruno LE JOSSEC
- ❖ Monsieur Eric LAMBERT
- ❖ Monsieur Cyril BRAS
- ❖ Général d'Armée (2S) Richard LIZUREY
- ❖ Monsieur Cédric PRADEL - Délégué permanent aux Départements Français d'Amérique
- ❖ Madame Azmina GOULAMALY

CONTEXTE ET MISSIONS



Contexte :

Les territoires sont divers, ils prennent à bras-le-corps la révolution numérique

La cybersécurité est souvent l'affaire de spécialistes, les cyber-agressions sont de plus en plus massives et inventives

La réglementation est foisonnante et en constante évolution

Au-delà de la dimension numérique, c'est toute la résilience des territoires qui est en jeu. Un territoire seul ne peut répondre à tous les défis

Missions : afin de créer un cyberspace public plus fiable et sécurisé au niveau des territoires

- Fournir une [plate-forme collaborative](#) entre les territoires (communes, EPCI), les agences publiques, le monde universitaire, l'industrie et la société civile
- Être un forum de [partage d'idées et de stratégies concrètes](#)
- Promouvoir [l'innovation technologique](#), organisationnelle et légale
- Assurer la [prospective](#) sur la résilience et la cybersécurité des territoires

L'ICRT aide les territoires à prendre conscience et s'adapter à la nouvelle dimension cyber et numérique

OBJECTIFS



Un territoire comprend :

- Les **collectivités territoriales** proprement dites (régions, départements, communes)
- Les **établissements publics** collectifs (EPCI) associés (agglomérations, communautés de communes...)
- Les **groupements publics** en dépendant (syndicats mixtes, SPL)
- Les **établissements de santé** (hôpitaux, cabinets médicaux publics)
- Les **PME-PMI**, en priorisant les PME-PMI à forte valeur économique et/ou stratégique
- Les **acteurs économiques sensibles** (médecins, pharmaciens, notaires, greffiers) ou non (artisans, commerces, agriculteurs, services divers)
- Les **citoyens** possesseurs de données et acteurs des territoires

L'ICRT a pour objectif de soutenir la constitution, la veille et la diffusion des idées, réflexions et études ayant trait à la cybersécurité et la résilience des territoires. L'institut ambitionne ainsi :

- De favoriser la **prise de conscience** mais aussi la mise en œuvre des bonnes pratiques
- De constituer un **observatoire** des expériences afin de partager celles qui donnent les meilleurs fruits, compte tenu des singularités locales
- Sans normaliser ni standardiser, **d'améliorer** et de concourir au développement d'une culture élargie de la sécurité locale, tenant compte des technologies innovantes mais aussi de l'enracinement durable des mesures adoptées
- D'encourager une mise en place de mesures dynamiques des territoires, de façon à leur permettre de se **développer économiquement** en protégeant mieux leur patrimoine et les acteurs socio-économique locaux

L'ICRT s'adresse d'abord aux EPCI et Communes et au-delà à tous les acteurs des territoires



UN INSTITUT AU SERVICE DES TERRITOIRES... DE TOUS LES TERRITOIRES...

Pour cela :

- Des actions
- Une organisation
- Accompagnement (Projet Cythère)

ACCOMPAGNEMENT



- Mettre en place des outils de **mutualisation** des ressources techniques pour l'ensemble des territoires (communes et EPCI)
- Permettre aux EPCI, aux communes et à leurs élus de répondre à leurs **obligations légales**



- Créer et pérenniser de **l'emploi** qualifié en cyber sur le territoire
- Mettre en place un organisme de **formation** sur les métiers de la cybersécurité pour des publics sans le Bac



- Accroître l'**attractivité** et le développement économique des territoires par les leviers de la **cybersécurité** et de la **résilience**

CYBERTERRITOIRES : SALON DE LA CYBERSÉCURITÉ ET DE LA RÉSILIENCE DES TERRITOIRES



- CYBERTERRITOIRES™ sera le **salon annuel de la Cybersécurité et de la Résilience des territoires**. Il combinera salon ouvert aux candidats, aux employeurs publics et privés (espace du GEIQ-Cyber), aux fournisseurs de solutions et un colloque dédié aux élus (préparé par l'IN.CRT)
- Il constituera un **rendez-vous régulier** associant les décideurs locaux économiques et politiques, aux élus, fonctionnaires, candidats et fournisseurs de solutions afin de préparer les services publics numériques et la résilience de demain et faire de la transformation digitale et de la sécurité numérique des plateformes de développement économique et d'attractivité.
- Il étendra son champ d'intérêt aux questions générales de résilience et de sécurité civile locale.
- Première édition : **Cyber.territoires 2021**, le 7 octobre 2021

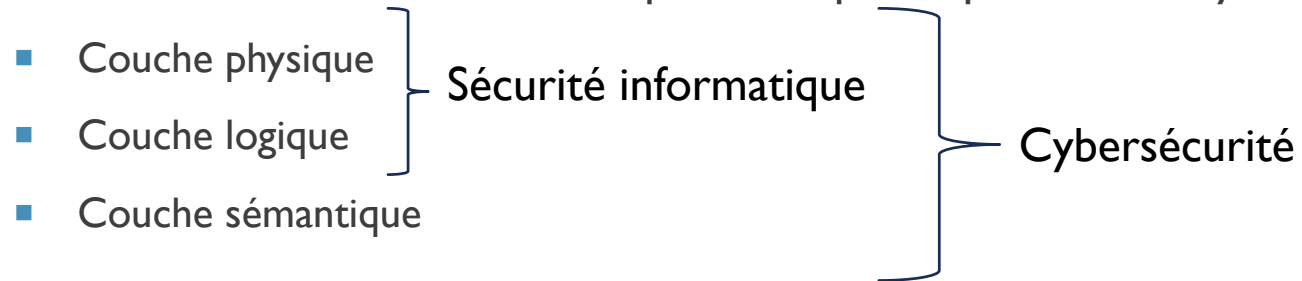
- L'institut dispose d'un collège RSSI qui apporte la vision terrain des enjeux de cybersécurité
- Il en ressort notamment la nécessité de :
 - Faire évoluer la perception du rôle et de la fonction de RSSI au sein des collectivités territoriales
 - Lui permettre d'apporter son expertise auprès des élus et des dirigeants
 - D'être un acteur incontournable de la transformation numérique
- Pourquoi ?

LES DIFFICULTÉS DU RSSI



- La sécurité informatique est perçue comme seulement technique et relevant de fait de la DSI seule

- Mais en fait la sécurité informatique n'est qu'une partie de la cybersécurité



LES DIFFICULTÉS DU RSSI



- Le RSSI est encore perçu comme « *Monsieur NON* »
- Le RSSI doit être un « Monsieur non, MAIS »
 - Trouver la solution adéquate entre le risque et l'usage
 - Faire en sorte que la cybersécurité soit un gage de confiance dans l'usage du numérique

ÉVOLUTION DES RSSI



- En 2021, un RSSI est un manager pas simplement un technicien !
- Ce fait est plus évident sur sa déclinaison anglaise CISO - Chief Information Security Officer
 - Il fait partie de la C-Suite dans laquelle on retrouve les principaux décideurs d'une structure

ÉVOLUTION DES RSSI



- Il doit :
 - Être bon techniquement pour faire des choix pertinents
 - Être un bon communicant pour aider les dirigeants et élus à mieux comprendre les enjeux de cybersécurité
 - Savoir se remettre en question car le domaine de la SSI est en constante mutation
- Panorama des métiers SSI de l'ANSSI
 - Apparition de la fonction de directeur cybersécurité

CONCLUSION



- La cybersécurité ne doit plus être perçue comme un frein au développement du numérique mais plutôt comme une condition nécessaire, un gage de confiance.
- Rendre la cybersécurité accessible y compris aux collectivités de tailles plus modestes.

POUR DES TERRITOIRES NUMÉRIQUES DE CONFIANCE



**MERCI DE VOTRE
ATTENTION**



- GENERAL (2S) MARC WATIN – AUGOUARD – PRÉSIDENT
- M. CYRIL BRAS – VICE- PRÉSIDENT
- M. ERIC LAMBERT – DIRECTEUR GENERAL
- WWW.CYBERTERRITOIRES.FR