

## Colloque “Territoire(s) & Sécurité(s)”

6 avril 2023, Aix-en-Provence

Format hybride présentiel et visio (sur inscription)

<https://cts-2023.sciencesconf.org/>

### Appel à communications

« Tout est territoire » a écrit au début des années 1990 la géographe Maryvonne Le Berre (1995). À différentes échelles, celui-ci relève effectivement de l'intime pour chaque individu, du politique pour l'espace public ou de la Nation pour ce qui engage le destin du pays. Plus de 30 ans après, cette formule demeure toujours aussi valable même si les contours de ces territoires n'ont cessé d'évoluer (décentralisation, intégration européenne, émergence des métropoles...). Avec l'entrée dans l'ère de la transformation numérique, de nouveaux territoires sont apparus ou vont apparaître (metaverse).

La représentation des territoires elle-même a changé avec des limites moins marquées entre les villes et les campagnes. Selon l'INSEE, 95 % de la population française vit désormais sous l'influence des villes, si l'on considère les unités urbaines de plus de 1500 emplois et leur aire d'incidence au regard des trajets domicile travail des habitants des communes avoisinantes. Avec le développement des moyens de télécommunications et de transport, l'opposition traditionnelle entre l'urbain et le rural s'est estompée vers des espaces dits « rurbains ». Les espaces atypiques (montagne, littoral, frontière, ...) ont aussi connu leurs propres mutations, de même que l'espace aérien voire spatial. Le questionnement sur le(s) du territoire(s) anime plus que jamais le débat public. L'appellation attribuée en 2020 au ministère de la Cohésion des territoires et des Relations avec les collectivités territoriales traduit à elle seule les préoccupations du moment.

Après un premier colloque organisé en juin 2020, le Centre de recherche de l'École de la gendarmerie nationale (CREOGN) et l'Université Gustave Eiffel ont souhaité poursuivre le développement de ce chantier en organisant un nouveau colloque décentralisé destiné aux chercheurs de toutes les disciplines et aux praticiens en France ou à l'étranger ayant travaillé ou travaillant sur la sécurité des territoires.

Ce colloque vise à encourager la diversité des approches en mêlant les expériences de terrain et les recherches autour de la notion de sécurité. Il s'agit d'ouvrir les communications possibles aux divers sens que peut prendre le terme de « sécurité », dans ses dimensions prospectives et rétrospectives.

Plusieurs axes de réflexions sont déjà proposés dans l'attente éventuelle d'autres pistes nouvelles. Aussi, ces axes ne préfigurent en aucune manière le programme du colloque.

- **La cybersécurité dans le(s) territoire(s).** Le rapport aux territoires (local, national, international ou même numériques) des acteurs privés ou publics ont été profondément transformés au cours de ces dernières années. Dans cette évolution, les questions de

sécurité numérique sont devenues plus prégnantes. La menace touche aussi bien les particuliers, les entreprises que les organismes publics, comme les établissements de santé notamment.

Néanmoins, la prise de compte de ces risques demeure parfois encore insuffisante, comme le souligne le rapport d'information n°283 du Sénat de décembre 2021, intitulé « Les collectivités territoriales face au défi de la cybersécurité ». Ce manque de sensibilisation se trouve aussi parmi les très petites et moyennes entreprises (TPE-PME).

La question relève à la fois de l'ordre de la sécurisation, de la prévention mais aussi de la résilience : comment réagir en cas de cyberattaque et comment s'en relever ?

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), la Direction du renseignement et de la sécurité de la Défense (DRSD) et la gendarmerie nationale sont déjà engagées dans la prévention des risques et la formation aux bonnes attitudes numériques. L'Institut national pour la Cybersécurité et la résilience des territoires (IN.CRT), créé à Vannes, cible plus particulièrement les collectivités locales et les intercommunalités confrontées aux cyberattaques. « *Il est plus que jamais urgent d'agir concrètement et collectivement en matière de sécurité numérique* », explique ainsi Guillaume Poupard, directeur général de l'ANSSI.

- **Acteurs privés et filières industrielles de la sécurité de demain.** On assiste à une diversification des acteurs de la sécurité et à l'affirmation du secteur privé dans ce domaine. « Les agents de l'État ne sont plus les seuls à assurer une mission de sécurité (...) L'État semble se retirer, petit à petit, de son rôle hégémonique de protection. Cette responsabilité, acquise tardivement, pourrait donc sembler quelque peu vacillante » estime Frédéric Diaz en 2003. « Le rôle des États garants de la protection des personnes, des biens et de l'information ne va plus de soi » considère en 2004 Frédéric Ocqueteau. Du côté des bandes criminelles, il existe aussi la tentation de « faire la police ». Chaque jour, près de 250 000 policiers et gendarmes agissent sur le territoire national auxquels s'ajoutent 21500 policiers municipaux et 165 000 agents privés.
- **Les innovations techniques de la sécurité, leurs imaginaires, et leur acceptabilité par les populations et les territoires.** Que proposent les nouvelles technologies dans le domaine de la sécurité et de la gestion d'événements extraordinaires ? Le territoire est devenu plus qu'un « être géographique » grâce aux nouvelles technologies numériques. Les progrès de la digitalisation ont contribué à abolir les distances en offrant une meilleure connexion entre les citoyens et les acteurs de la sécurité. Dans la gendarmerie nationale, l'arrivée de Néogend a bouleversé le rapport du personnel à la brigade territoriale en lui offrant une plus grande mobilité garantissant un accès optimisé aux principaux outils métiers. De son côté, la brigade numérique lancée en 2018 à Rennes permet de répondre 24h/24 et 7j/7 aux interrogations les plus variées des internautes à travers un échange personnalisé avec un gendarme, essentiellement par tchat. Ce poste avancé de l'espace virtuel est également révélateur des nouveaux besoins de sécurité apparus avec le développement d'Internet. Ce nouveau monde numérique a offert de nouvelles opportunités mais il a aussi suscité des craintes en matière de délinquance (escroquerie, pédopornographie, harcèlement, darknet, ...). D'autres innovations comme le Big data ou l'intelligence artificielle (IA) soulèvent des interrogations en matière de sécurité et de gouvernance des Data.
- **La sécurité perçue comme élément d'attractivité des territoires.** Pour les acteurs socio-économiques, un territoire « sûr » est un gage d'attractivité qui favorisera leur ancrage au territoire, la pérennité de l'activité économique et plus généralement, la qualité de vie. Cette sécurité perçue est complexe et mérite d'être analysée du point de vue des territoires, de ses parties-prenantes et aussi du point de vue de la valorisation du patrimoine. A l'ère post-Covid, il s'agit notamment, dans une lecture

large de la sécurité, d'intégrer les prismes suivants : la sécurité comme forme de résilience pour les territoires, la sécurité des déplacements et le lien entre aménagement du territoire et sécurité ...

Le défi de notre temps est bien là : penser tout à la fois les réseaux virtuels, l'identité territoriale et les nouveaux territoires de la sécurité.

### Les mots clés

Appropriation territoriale, crise, Data, drones, frontière(s), formation, flux, innovation, gendarmerie nationale, gouvernance, Intelligence artificielle (IA), mobilité, numérique, patrimoine, police municipale, police nationale, police de sécurité du quotidien (PSQ), proximité, résilience, safe city, smart city, sécurité, simulation, vidéosurveillance, vulnérabilité.

### Références

Ahmadi-Assalemi G., Al-Khateeb H., Epiphaniou G. and Maple C. (2020). Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review. *Smart Cities* 3, 894–927. Doi: 10.3390/smartcities3030046.

Al Dairi A., Tawalbeh L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science* 109C. Pp.1086–1091.

Chen D., Wawrzynski P., Ly Z. (2021). Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*, vol.66.

Diaz F. (2003). Coproduction de la sécurité : une nouvelle forme de l'interventionnisme étatique pour une meilleure sécurité du public ?. *Déviance et Société*, vol. 27, 2003/4. Pp. 429-458.

Laufs, J. H. Borrion, B. Bradford (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society*, 55, 102023.

Le Berre M. (1995). Territoires. In Bailly A., Ferras R. et Pumain D. (dir.). *Encyclopédie de Géographie*. Economica (2<sup>ème</sup> édition). Pp. 617-638.

Ocqueteau F.(2004). *Polices entre État et marché*, Paris, Presses de Sciences Po.

Ocqueteau F., Ventre D. (dir.). (2011). Contrôle et surveillance dans le cyberspace. *Problèmes Politiques et Sociaux*, n° 988. Pp.130.

Soare S. R., Burton J. (2020). "Smart City, Cyber Warfare and social disorder". In Ertan A., Floyd K., Pernik P., Stevens T. (eds) (2020). *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. The NATO Cooperative Cyber Defence Centre of Excellence. Pp. 108-124

### Modalités de participation

Les personnes qui souhaitent soumettre une proposition de communication sont invitées à déposer pour le **15 juin 2022** sur le site du colloque (<https://cts-2023.sciencesconf.org/>) au format Word ou PDF un texte comprenant une courte présentation, un plan détaillé de la communication, l'approche méthodologique envisagée, les résultats obtenus ou visés et une bibliographie (15 références max.). Le texte ne doit pas dépasser 1000 mots.

Une publication des actes est programmée. Les informations seront précisées ultérieurement.

## Le comité scientifique

- BOURRET Christian, PR, Université Gustave Eiffel, laboratoire DICEN-IdF (Dispositifs d'Information et de Communication à l'Ère Numérique)
- CALISTE Jean-Pierre, Université de Technologie de Compiègne / Codata France
- DAVID Amos, PR, Université de Lorraine, laboratoire DICEN-IdF (Dispositifs d'Information et de Communication à l'Ère Numérique)
- FABRY Nathalie, PR, Université Gustave Eiffel, laboratoire DICEN-IdF (Dispositifs d'Information et de Communication à l'Ère Numérique)
- HABERBUSCH Benoît (commandant), docteur en histoire, chef du département Recherche et Stratégie CREOGN
- MOINET Nicolas, PR, IAE Université de Poitiers
- PARRINI-ALEMANNI Sylvie, PR, CNAM Paris, laboratoire DICEN-IdF (Dispositifs d'Information et de Communication à l'Ère Numérique)
- SAINT-GERAND Thierry, PR émérite, Université Caen, CNRS Caen, laboratoire IDEES (Identité et Différenciation de l'Espace, de l'Environnement et des Sociétés)
- SEVERO Marta, PR, Université de Paris-Nanterre, laboratoire DICEN-IdF (Dispositifs d'Information et de Communication à l'Ère Numérique)
- ZACKLAD Manuel, PR, CNAM Paris, laboratoire DICEN-IdF (Dispositifs d'Information et de Communication à l'Ère Numérique)
- ZEGHNI Sylvain, MCF-HDR, Université Gustave Eiffel, laboratoire LVMT (Ville, Mobilité, Territoire)

## Le comité d'organisation

- Claudia DA RE, Université Gustave Eiffel
- Nathalie FABRY, Université Gustave Eiffel
- Commandant Benoît HABERBUSCH, Gendarmerie nationale, CREOGN
- Capitaine Thibaut HECKMANN, Gendarmerie nationale
- Frédérique HERNANDEZ, Université Gustave Eiffel
- Magali JAFFARD, SAFE Cluster
- Marie-Christine LACOUR, CODATA-France

## Partenaires

