



# Les Universités de l'AN2V



22-23 mai 2024 à  
Strasbourg



Inscrivez-vous !  
En flashant ce code

Au Palais de la Musique  
et des Congrès – [Strasbourg](#)

- 2 plénières avec des intervenants prestigieux
- 12 ateliers de perfectionnement
- 65 partenaires industriels
- 1500 professionnels



# Pourquoi cet événement ?

- Forte de son expérience de 20 ans dans l'animation de réunions d'information et d'échange sur les technologies de sûreté, l'AN2V vous propose un **événement** de **deux jours** qui vous permettra d'avoir une **vision stratégique, théorique et pratique** des nouvelles solutions de sûreté.
- Ces Universités combinent deux conférences **plénières**, des **ateliers** pour approfondir des sujets technologiques, juridiques ou stratégiques et un espace **partenaires** permettant de découvrir l'offre technologique. Cet événement se déroule à Strasbourg dans un cadre convivial, avec des **animations** tout au long de la journée et une soirée de **prestige**.



## Les Universités de l'AN2V rassemblent la profession

- Des **institutionnels** : ministères, référents sûreté policiers nationaux et gendarmes, douaniers, policiers municipaux, sécurité privée, ...
- Des utilisateurs publics : collectivités locales, hôpitaux, universités, départements, régions...
- Des utilisateurs privés : PME, grande distribution, logement social, transport, sites sensibles...
- Des **fournisseurs de solutions de sécurité** : outre les fournisseurs présents sur l'espace partenaires, les Universités de l'AN2V attirent également des représentants d'entreprises qui cherchent à enrichir leurs connaissances sur la sécurité publique et privée.



# Une programmation rythmée...

## Mercredi 22 mai 2024

9h00-9h40	Accueil café Ouverture espace partenaires		
9h40-10h00	Ouverture AN2V		
10h00-12h00	Plénière n°1 Enjeux et défis de la résilience		
12h00-13h50	Cocktail déjeunatoire Visite des espaces partenaires		
13h50-15h00	Atelier n°1	Atelier n°2	Atelier n°3
15h00-16h50	Visite des espaces partenaires		
16h50-18h00	Atelier n°4	Atelier n°5	Atelier n°6
18h00-20h00	Visite des espaces partenaires puis pause hôtel		
20h00...	Dîner de prestige – Ancienne Douane		

## Jeudi 23 mai 2024

8h00-9h00	Accueil café Ouverture espace partenaires		
9h00-10h10	Atelier n°7	Atelier n°8	Atelier n°9
10h10-11h00	Visite des espaces partenaires		
11h00-12h50	Plénière n°2 Résilience des Territoires		
12h50-14h50	Cocktail déjeunatoire Visite des espaces partenaires		
14h50-16h00	Atelier n°10	Atelier n°11	Atelier n°12
16h00-16h40	Clôture		



## Un espace représentatif de l'offre technologique

- Les Universités de l'AN2V réunissent une soixante d'exposants afin de vous offrir un large panel de l'offre technologique présente sur le marché.
- Vous disposez tout au long des deux jours du temps nécessaire pour échanger avec chacun de nos partenaires, dans un cadre agréable et convivial.

## Des animations, des démonstrations

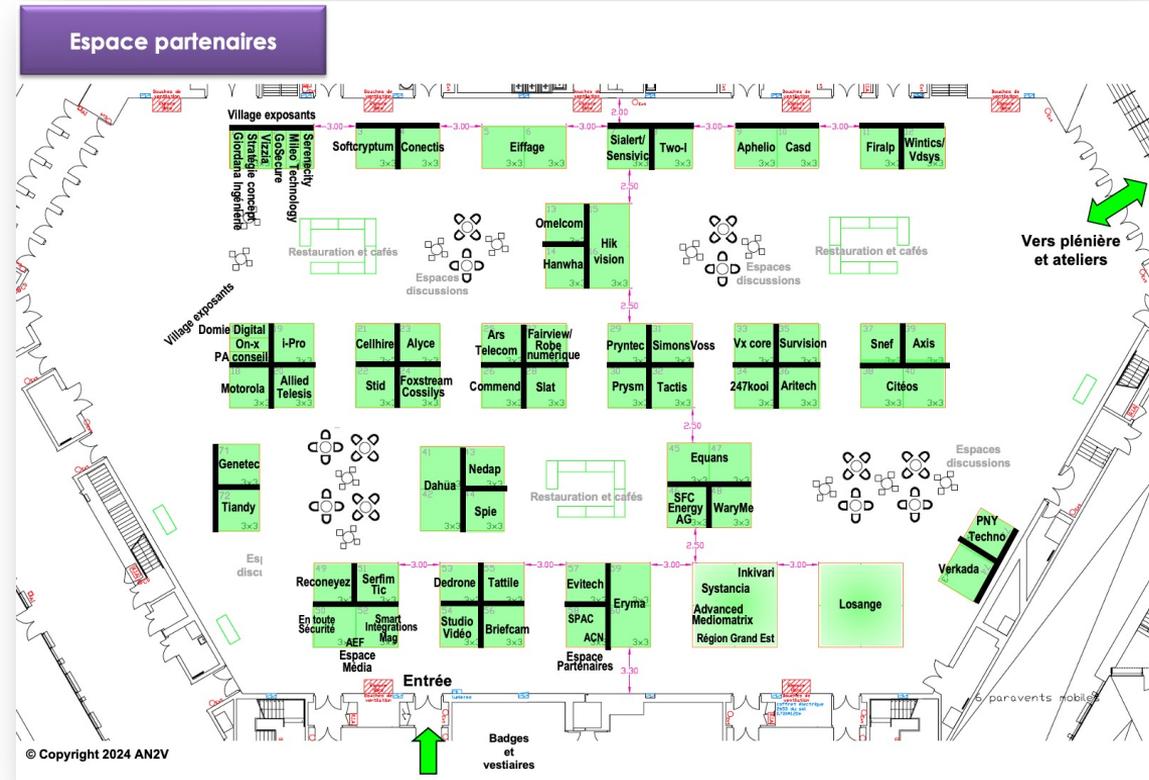
- Nous proposons un parcours de visite des stands, avec un focus sur les innovations technologiques présentées par nos partenaires.
- Des démonstrations concrètes de la mise en œuvre de ces technologies sont proposées tout au long des Universités.



# Les partenaires inscrits



## Espace partenaires



© Copyright 2024 AN2V

© AN2V – 2024 – Toutes reproductions interdites



# Une soirée de prestige

Les universités  
de l'AN2V



L'Ancienne Douane, restaurant classé Monument Historique

Un moment de convivialité pour nous aider à comprendre et synthétiser les moments forts de la journée !



Soirée Universités 2022



L'objectif de cette plénière est de cadrer le thème de la résilience à 360° :

- Les grandes définitions de la résilience, au quotidien ou suite à un choc (de toute nature),
- Les enjeux différenciés pour les sites privés, les sites sensibles, les espaces publics ou ouverts au public ;

Il sera question de continuum de sécurité pour satisfaire toutes les attentes, quelles que soient la taille et la localisation du site atteint par le choc.

- ➔ De quoi avons-nous besoin pour être stratégiquement résilient ?
- ➔ Quels sont les freins ou les blocages en matière organisationnelle, technique, juridique, financière et éthique ?
- ➔ Avons-nous tous les outils de compréhension et de mesure d'efficacité de notre résilience ?

Sont programmés sur cette première plénière :

- Des orateurs avec une vision internationale
- Le SGDSN/PSE (Protection et Sécurité de l'État)
- Le Haut Comité Français pour la Résilience Nationale
- Le CSF-IS (nouveau contrat stratégique de filière 2023-2026)
- Le CSF-Infranum





### Les orateurs de la plénière n°1 :

- ❑ M. Claude STURNI : Vice-Président en charge du développement économique – Région Grand Est
- ❑ M<sup>me</sup> Mauna TRAIKIA : Conseillère territoriale développement numérique – CA Plaine Commune Grand Paris
- ❑ M. Richard LIZUREY : Président du Haut Comité Français pour la Résilience Nationale
- ❑ M<sup>me</sup> Julie MERCIER : La DEPSA - Direction des entreprises, des partenariats de sécurité et des armes
- ❑ M. François MURGADELLA : Le SGDSN/PSE - Conseiller technologies de la directrice de la protection et de la sécurité de l'État
- ❑ M. Daniel LE COGUIC : Président de l'Alliance pour la Confiance Numérique (ACN)
- ❑ M. Hervé RASCLARD : Délégué Général de la fédération des industriels des infrastructures numériques (INFRANUM)





### Au travers de l'outil de la roue d'amélioration de la résilience, l'objectif de cette plénière est de décrire le fonctionnement de la résilience d'un territoire.

- Quelle organisation placer à chaque échelon de son organisation ? Comment la perfectionner ?
- Qu'est-ce qu'une (bonne) analyse de vulnérabilité ?
- Présentation des bonnes pratiques, en temps normal, en temps de crise,
- Quels sont les outils ? Avons-nous des attentes non couvertes ?
- Quels sont les politiques d'exercices et de formations ?

### Sont programmés sur cette deuxième plénière :

- Des retours d'expérience
- Des députés nationaux
- Des régions
- Le SGDSN/SNR (stratégie nationale de résilience)
- Intercommunalité de France





### Les orateurs de la plénière n°2 :

- ❑ M. Christophe NAEGELEN : Député - Élu à la Région Grand Est
- ❑ M. Thibaud PHILIPPS : Vice-Président en charge des transports et des mobilités durables – Région Grand Est
- ❑ M<sup>me</sup> Irène WEISS : Conseillère régionale déléguée Grand Est - Déléguée à la cybersécurité
- ❑ M. Yannick FERRAND : Directeur à la direction des risques majeurs de la mairie de Cannes
- ❑ M<sup>me</sup> Marlène LE DIEU DE VILLE : Co-Présidente commission numérique Intercommunalités de France
- ❑ M. Laurent LEBERON : Directeur de Mission Sécurité au Conseil régional d'Occitanie Pyrénées Méditerranée
- ❑ M. Jean-Christophe ERARD : Délégué pour la stratégie nationale de résilience auprès des collectivités territoriales / Direction de la Protection et de la Sécurité de l'État au SGDSN





## Une occasion d'approfondir vos connaissances

- 70 minutes pour développer un thème technologique, juridique ou stratégique d'actualité. Animés par des spécialistes de l'écosystème choisis pour leur connaissance du sujet abordé, ces ateliers vous permettront d'obtenir toutes les informations actualisées et utiles introduites lors des deux plénières.

## 12 thèmes abordés – 3 ateliers en simultanément

- 12 thèmes seront abordés pour vous rendre compte de la diversité de l'offre technologique de sécurité. Trois ateliers sont organisés simultanément pour que chacun trouve à tout moment un atelier qui l'intéresse.





## Mercredi 22 mai 2024

13h50-15h00

Atelier n°1

1.

Quelle structuration pour une résilience **cyber** ?  
CSF-IS, ANSSI, retours d'expérience

Atelier n°2

2.

Le renforcement de la résilience dans les situations **d'incendie**

Atelier n°3

3.

Quelles **plateformes digitales** pour traiter la résilience ?

16h50-18h00

Atelier n°4

4.

Quelles nouveautés pour les **outils d'IA** concernant les nouveaux usages ?

Atelier n°5

5.

**Infrastructures** physique résiliente : retours d'expérience

Atelier n°6

6.

État de l'art **juridique** Depsa, Cnil, IA Act...

## Jeudi 23 mai 2024

9h00-10h10

Atelier n°7

7.

Pour la résilience, comment générer des **interactions rapides** collectivité/EPCI/département/région/État ?

Atelier n°8

8.

État de l'art technologique **cyber**

Atelier n°9

9.

État, Entreprises, Collectivités : A-t-on encore les moyens de penser **Éthique, Souveraineté** et **Numérique** ?

14h50-16h00

Atelier n°10

10.

Quelles technologies pour la résilience **inondation, tremblement de terre, NRBC**...

Atelier n°11

11.

Quelles **données** pertinentes pour accroître la résilience ?

Atelier n°12

12.

Quelles nouvelles idées pour l'**IA** ?



Pour animer **les 12 ateliers**, **60 orateurs** viendront vous donner leur vision 2024 sur la sécurité/sûreté. Parmi eux, les orateurs experts présents sur la zone des 70 stands exposants, et aussi des structures spécialisées sur la sécurité/sûreté seront représentées, comme :

- La **CNIL** : **Sarah ARTOLA**
- La **DEPSA** : **Élisabeth SELLOS-CARTEL** – Ministère de l'Intérieur
- L'**ANSSI** : **Vincent RHIN** - Délégué à la sécurité du numérique en Région Grand Est  
et **Alexis TASSE** - Sous-direction Expertise - Division Assistance Technique - Bureau sécurisation des systèmes
- L'**ANFSI** : Agence du Numérique des Forces de Sécurité Intérieure – **Alexandre GERLAND**
- L'**ACN** : **François ESNOL-FEUGEAS** - L'Alliance pour la Confiance Numérique,  
et **Yoann KASSIANIDES** – Délégué général ACN
- Le responsable des opérations **CSIRT (Grand Est Cybersécurité)** – **Jean-Luc BELET**
- Le **SDIS72** : avec le Syndicat Mixte de la Sarthe
- La **Région Grand Est** : **Franck SIEGRIST** - Directeur Territoire Numérique chez Région Grand Est
- Le **LORIA** Nancy : **Rémi BADONNEL** Professeur des Universités  
(TELECOM Nancy, Lorraine INP, Université de Lorraine, Loria - Inria Nancy Grand Est)
- Le **SERTIT** : iCUBE, Université de Strasbourg – **Hervé Yésou**, Directeur scientifique
- Le **SAFE CLUSTER** : **Philippe LECLERC** - Directeur des Programmes Sûreté et Sécurité

# Les orateurs des douze ateliers



Et vous aurez également le plaisir d'écouter ces orateurs :



M. Nicolas HECQ  
DGS du Syndicat Mixte  
Sarthe Numérique



M<sup>me</sup> Ysens DE FRANCE  
Chargée de mission IA au service de  
la transformation de la DGGN



M<sup>me</sup> Ilham DJEHAICH  
Présidente de Losange  
La Région Grand Est



M. Mickael WAJNGLAS  
Secrétaire Général SPAC  
Smart Physical Access Control  
Security and Industry 4.0



M. Yannick FERRAND  
Directeur à la direction des risques  
majeurs de la mairie de Cannes



M<sup>me</sup> Béatrice BULOU  
Eurométropole de Strasbourg : Vice-présidente  
et Maire de la commune de Mundolsheim  
Comité d'Éthique Eurométropole de Strasbourg



M. Joël GUERET  
Chef de projet stratégique sécurité  
Région Grand Est

13h50-15h00	Atelier n°1	Atelier n°2	Atelier n°3
	1. Quelle structuration pour une résilience cyber ? CSF-IS, ANSSI, retours d'expérience	2. Le renforcement de la résilience dans les situations d'incendie	3. Quelles plateformes digitales pour traiter la résilience ?



## Atelier 1 : Quelle structuration pour une résilience cyber ? CSF-IS, ANSSI, retours d'expérience

- ACN – François ESNOL-FEUGEAS
- ANSSI – Vincent RHIN - Délégué à la sécurité du numérique en Région Grand Est
- AXIS – Philippe BENARD
- SYSTANCIA – Christophe CORNE
- Responsable des opérations CSIRT (Grand Est Cybersécurité) – Jean-Luc BELET

Cet atelier a pour but de faire un état de lieux de la situation actuelle d'un point de vue général : Au carrefour de la conflictualité entre les états, de la criminalité omniprésente et de la complexité des systèmes en eux-mêmes.

- La cyber : quels risques, quelles conséquences et pour quels types d'acteurs ?
- Quel rôle endossera l'ANSSI ?
- Quid des entreprises françaises ?
- Quid des campus cyber ?
- Où en sont les CSIRT sur les 13 régions ?
- L'atelier aura également pour but de traiter des grands axes de la cyberprotection et de la prospective du nouveau contrat CSF-IS 2023-2026.

13h50-15h00	Atelier n°1	Atelier n°2	Atelier n°3
	1. Quelle structuration pour une résilience cyber ? CSF-IS, ANSSI, retours d'expérience	2. Le renforcement de la résilience dans les situations d'incendie	3. Quelles plateformes digitales pour traiter la résilience ?

Les universités de l'AN2V

## Atelier 2 : Le Renforcement de la résilience dans les situations d'incendie

- DÉPARTEMENT DE LA SARTHE – Mme Martine CRNKOVIC - Vice-présidente du Département de la Sarthe
- Service CTA-CODIS (72) - Adjudant Fabien RENEAUX - Chef de salle opérationnelle adjoint
- AXIS – Henri CARPUAT
- ELLONA – Jean-Christophe MIFSUD
- HIKVISION – Nicolas Hess
- KOOI – Pascal Schneider
- THALES – Richard KALCZUGA

Quelles applications (ou « impacts ») des technologies de pointe et de la vidéosurveillance sur l'évaluation et la gestion des risques d'incendie dans les espaces publics, privés et les sites de recyclage.

Il sera expliqué notamment :

- Sarthe numérique qui expliquera son dispositif original rendu possible grâce aux réseaux à très hauts débits déployés,
- Axis, Hikvision & Kooi : quelles applications de la vidéosurveillance au service de la détection et de la prévention incendie (espaces publics, site de recyclage),
- Ami Panoptès : « détecter en moins de 5 mn avec une précision de 50m sur l'ensemble du territoire ».  
Une initiative de l'entente Valabre, le ministère de l'Écologie et des collectivités territoriales instruit par le pôle Safe,
- Un groupement d'industriels répond avec une solution innovante grâce à un effet zoom (du satellite aux capteurs terrestres intelligents) et un socle technique national, pour orchestrer, suivre et offrir une base de connaissance à l'ensemble des SDIS,
- Quelles technologies de captation ? Caméra longue distance, ou en aérien : drone, satellite...

13h50-15h00	Atelier n°1	Atelier n°2	Atelier n°3
	1. Quelle structuration pour une résilience cyber ? CSF-IS, ANSSI, retours d'expérience	2. Le renforcement de la résilience dans les situations d'incendie	3. Quelles plateformes digitales pour traiter la résilience ?

Les universités de l'AN2V

Mercredi 22 mai – 13h50 à 15h00

## Atelier 3 : Quelles plateformes digitales pour traiter la résilience ?

- ANFSI - Agence du Numérique des Forces de Sécurité Intérieure – Alexandre GERLAND
- CASD – Vivien BACZKIEWICZ
- ERYMA – Bertrand BLAISE
- RÉGION GRAND EST – Franck SIEGRIST - Directeur Territoire Numérique chez Région Grand Est
- LOSANGE – Alain SOMMERLATT

La mutualisation des (grands) dispositifs de vidéoprotection et projets d'IoT est source d'efficacité globale.

La loi de la sécurité globale préservant les libertés adoptées en mai 2021 a par ailleurs créée un cadre juridique prometteur permettant de favoriser les déploiements à grande échelle, notamment grâce à l'article 42.

Les éditeurs (et les nouveaux entrants) enrichissent leurs plateformes, leurs passerelles, les utilisateurs sont demandeurs de nouvelles fonctionnalités.

Il sera effectué dans cet atelier un état des lieux des nouveaux usages et des nouvelles attentes :

- Le parc de caméras et de capteurs IoT à intégrer est exponentiel et vient du monde entier...  
→ comment les plateformes les administrent-ils ? Quid de la souveraineté ?
- Outre la gestion en temps réel, le logiciel doit également permettre une relecture intelligente,  
→ comment s'intègre l'IA pour les CSU – Centre de Supervision Urbaine et les CSM – Centre de Supervision Mutualisé ?
- Comment les VMS deviennent-ils des hyperviseurs ? (facturation des entités clientes, garantie de service pour chaque entité...)
- Les collectivités supervisent des voies publiques et des espaces privés (leurs bâtiments),  
→ les VMS sont-ils adaptés à ces deux usages simultanés ?
- Comment répondre aux attentes des opérateurs pour disposer d'un outil unique ergonomique et performant d'aide à la décision ?
- Quelle intégration de ces nouveaux équipements avec les FSI – Forces de Sécurité Intérieure (CIC et CORG...)

16h50-18h00	Atelier n°4	Atelier n°5	Atelier n°6
	4. Quelles nouveautés pour les outils d'IA concernant les nouveaux usages ?	5. Infrastructures physique résiliente : retours d'expérience	6. État de l'art juridique Depsa, Cnil, IA Act...



## Atelier 4 : Quelles nouveautés pour les outils d'IA concernant les nouveaux usages ?

- **FOXSTREAM** – Ionel POP - Directeur Général
- **HANWHA** – Michael VERNIER - Business Development Manager Vision
- **PRYNTEC** – Marie-Amélia DU COLOMBIER - Business Developer Grands Comptes
- **WINTICS** – Quentin BARENNE - Co-fondateur de Wintics

L'IA se développe rapidement dans notre domaine et les premiers déploiements sont en exploitation.

- Pour quels cas d'usages au final et dans quel contexte ? Quelles attentes réelles ?
- Quel niveau de fiabilité peut-on espérer ? Les faux positifs...
- Quelles ressources faut-il prévoir ?
- En quoi l'IA sera indispensable pour la résilience des Territoires ?
- Est-ce que l'IA frugale reste d'actualité ? (consommation d'énergie, CPU, réseau...)
- Quid des apprentissage biaisés ? Comment garantir un service minimal en la matière ?



16h50-18h00

Atelier n°4

Atelier n°5

Atelier n°6

4.  
Quelles nouveautés pour les outils d'IA concernant les nouveaux usages ?

5.  
Infrastructures physique résiliente : retours d'expérience

6.  
État de l'art juridique Depsa, Cnil, IA Act...

Mercredi 22 mai – 16h50 à 18h00

## Atelier 5 : Infrastructures physique résiliente : retours d'expérience

- **INFRANUM** – Hervé RASCLARD
- **LOSANGE** – M<sup>me</sup> Ilham DJEHAICH
- **SLAT** – Philippe ROUX
- **TACTIS** – Stéphane LELUX - Président Commission Internationale CSF InfraNum

Cet atelier a pour objectif de décrire les grands réseaux départementaux et régionaux, existants et à venir.

- Quels sont les acteurs, quels sont leurs projets et en quoi ils sont acteurs directs de la résilience des territoires ?
- Quid des RIP - Réseau d'Initiative Publique ?
- Quels services pour demain ? Quid de la vidéoprotection ?
- Quid des nouvelles technologies de transmission (comme la transmission en longueur d'onde à très haut débit)
- Quid du déploiement des réseaux 5G ? D'IoT privés ?
- Nouvelle génération de réseaux PMR : Solutions de caméras embarquées, Protection Travailleur isolé et comment cela se combine avec le Réseau Radio du futur du ministère de l'intérieur

Mercredi 22 mai – 16h50 à 18h00

## Atelier 6 : État de l'art juridique : Depsa, Cnil, IA Act...

- Cabinet La robe numérique – Oriana LABRUYERE
- Cabinet Thibault du Manoir – Thibault du MANOIR de JUAYE
- CNIL – Sarah ARTOLA
- DEPSA – Élisabeth SELLOS-CARTEL
- INKIVARI – Cyril MARCH

Compte-tenu d'une accélération sans précédent sur ces deux dernières années de l'approche légale de nos métiers à l'échelle nationale et européenne (IA Act), il est indispensable de faire le point sur les nouvelles pratiques rendues envisageables dans nos dossiers : Lecture de plaques, intelligence artificielle, reconnaissance faciale, caméras augmentées...

Il sera exploré le cadre actuel de la vidéoprotection "classique », puis avec des caméras "augmentées »  
Ensuite, il sera abordé les perspectives d'évolution du cadre juridique à l'échelle nationale et européenne.

Nous ferons appel dans cet atelier aux meilleurs experts pour présenter le cadre juridique en vigueur, les évolutions récentes et celles attendues.

9h00-10h10	Atelier n°7	Atelier n°8	Atelier n°9
	7. Pour la résilience, comment générer des interactions rapides collectivité/EPCI/département/région/État ?	8. État de l'art technologique cyber	9. État, Entreprises, Collectivités : A-t-on encore les moyens de penser Éthique, Souveraineté et Numérique ?



## Atelier 7 : Pour la résilience, comment générer des interactions rapides Citoyens/Communes/EPCI/Département/Région/État ?

- RÉGION GENDARMERIE DU GRAND EST - CEN Guillaume LUNDI
- ATRISC – Ludovic PINGANAUD - Expert en gestion des crises et fiabilité des organisations
- ERYMA – Johann LARA
- GOSECURE – Samuel MACHET
- RÉGION GRAND EST – Joël GUÉRET
- WARYME – Boris BERGER

Cet atelier a pour objectif de décrire les dispositifs d'alertes montantes et/ou descendantes envisageables des services centraux vers les citoyens. L'objectif est le partage d'un même niveau d'information pour éviter toute dispersion et interprétation pour chacun dans son domaine de compétence. Nous décrivons les enjeux, obligations et perspectives de différentes collectivités pour assurer une meilleure sécurité des citoyens tant personnelle que collective

Il existe de nouvelles applications du type « j'ai peur, je signale » permettant de géolocaliser les personnes en insécurité dans l'espace public par envoi d'un sms aux services centraux, l'application pouvant être passerilisée avec les caméras de vidéoprotection permettant de visualiser plus rapidement les faits et -le cas échéant- une intervention ciblée des bons services.

Il sera décrit, avec les technologies associées :

- Les services descendants : alerte pour un incendie de grande ampleur, une fumée type Lubrizol, FR-alert vague submersive...
- Les services montants : comment les citoyens peuvent-ils participer à la résilience sur un événement ?
- La capacité à faire converger/harmoniser/interopérer l'application idoine au niveau des différentes strates des collectivités, acteurs d'une potentielle gestion de crise.

9h00-10h10	Atelier n°7	Atelier n°8	Atelier n°9
	7. Pour la résilience, comment générer des interactions rapides collectivité/EPCI/ département/ région/État ?	8. État de l'art technologique cyber	9. État, Entreprises, Collectivités : A-t-on encore les moyens de penser Éthique, Souveraineté et Numérique ?



Judi 23 mai – 9h00 à 10h10

## Atelier 8 : État de l'art technologique cyber

- ANSSI – Alexis TASSE - Sous-direction Expertise - Division Assistance Technique - Bureau sécurisation des systèmes
- APHELIO – Jérémy GIRAUD
- EQUANS – Lidia MEIRINHO
- LORIA Nancy – Rémi BADONNEL
- SPAC – Mickael WAJINGLAS
- CSO METSYS – Hervé THIBAULT

Avec l'accentuation des interconnexions des dispositifs de sécurité/sûreté, cet atelier a pour objectif de décrire la cyberprotection des produits et des solutions qu'il est indispensable d'utiliser :

- Quels sont les risques ?
  - Exemple sur le contrôle d'accès : Clonage de badge (démon), écoute des trames, interception des données, substitution de lecteurs, rejeu...
- Quelles sont les modes opératoires des attaques récentes ? (quoi de nouveau)
  - Exemple : attaques hybrides (intrusion physique puis attaque cyber), ce qui fait résonance à la NIS 2 et au CER qui lie sécurité physique et cyber
- Comment protéger un dispositif de l'ampleur des JOP ?
- Quelles sont les nouvelles normes françaises et européennes ?
  - Exemple : FR : certification CSPN et qualification et EU : EUCC, NIS 2, CER, CRA, EN17640
- Quels sont les grands axes à emprunter pour la cyberprotection de ces solutions et des sites qu'elles équipent ?
  - ➔ Standard européen, SSCP

Jeudi 23 mai – 9h00 à 10h10

Atelier 9 : État, Entreprises, Collectivités :

➔ A-t-on encore les moyens de penser Éthique, Souveraineté et Numérique ?

- Ministère de l'Intérieur et des Outre-mer - DGGN – Ysens de FRANCE – Docteur en droit – chargée de mission IA
- Eurométropole de Strasbourg – Béatrice BULOU – Comité d'Éthique Eurométropole de Strasbourg
- ACN – Yoann KASSIANIDES
- CASD – Vivien BAGZKIEWICZ

Les dernières avancées technologies puissantes telles que l'IA (ChatGPT, caméras augmentées...), nous obligent à rester très vigilant concernant l'Éthique des dispositifs à mettre en œuvre. Le CSF-IS a œuvré pour la rédaction d'une **charte d'Éthique** dans nos métiers de la sécurité.

Cependant, de nombreuses questions nouvelles se posent, et une fonction de régulation déontologique de l'exploitation des dispositifs de sûreté est indispensable, nous aurons l'occasion d'évoquer la **stratégie nationale IA et européenne** fondée sur l'éthique, et de présenter la première charte éthique IA pour la **Gendarmerie Nationale**.

- Comment saisir l'opportunité & attendus de comités éthiques sur le sujet de l'IA, à quel niveau le placer au sein d'une entreprise et dans le service public, à quelle échelle ?
- Quid de la création d'un comité d'éthique qui doit répondre aux objectifs d'équilibre, d'indépendance et de pluralité (représentants de la collectivité, d'élus, de citoyens, d'associations...).
- Comment intégrer les réflexions pour (non exhaustif) :
  - Garantir le strict respect des règles en vigueur, ou à venir (loi JOP et suite),
  - Garantir le droit à l'information,
  - Garantir le respect des délais de destruction des enregistrements, ainsi que de leur mode d'exploitation,
  - Garantir un mode de fonctionnement consensuel du dispositif (visualisation, relecture) accepté par le plus grand nombre,
  - Garantir la transparence dans la description des objectifs précis que le dispositif doit atteindre,
  - Garantir une traçabilité quant au mode de fonctionnement...

Judi 23 mai – 14h50 à 16h00

## Atelier 10 : Quelles technologies pour la résilience inondation, tremblement de terre, NRBC...

- MAIRIE DE CANNES – M. Yannick FERRAND – Directeur à la direction des risques majeurs
- EQUANS – Anaïs GANDY
- SAFE CLUSTER – Philippe LECLERC
- SERTIT - iCUBE, Université de Strasbourg – Hervé Yésou, Directeur scientifique
- SFC Energy AG – Richard-Enno MEYER

Cet atelier nous renvoie sur des événements graves survenus récemment :

- Inondation du Pas-de-Calais,
- Tempête Alex vallées de la Roya et de la Vésubie,
- Tremblement de terre au Maroc,
- Incendies de grande ampleur sur tout le territoire (Sud-Ouest, Bretagne, Région Grand Est, Occitanie, Grand Sud...),
- Nuage Lubrizol,
- Covid,
- Attentats
- Attaque cyber, ransomware
- ...

Il sera donc traité dans cet atelier les questions suivantes :

- Avons-nous toutes les technologies pour une prévention efficace ?
- Pour le jour J : Les technologies sont-elles encore fonctionnelles ? Quels modes dégradés restent acceptables ?
- Comment se préparer ?
- Les retours d'expériences sont souvent (très) critiques ! Pourquoi, et sur quels sujets ?

14h50-16h00	Atelier n°10	Atelier n°11	Atelier n°12
	10. Quelles technologies pour la résilience inondation, tremblement de terre, NRBC...	11. Quelles données pertinentes pour accroître la résilience ?	12. Quelles nouvelles idées pour l'IA ?



Judi 23 mai – 14h50 à 16h00

## Atelier 11 : Quelles données pertinentes pour accroître la résilience ?

- **ADVANCED Médiométrie** – Sébastien BUANNIC - Directeur Technique et opérationnel
- **PLAINE COMMUNE** – Mauna Traikia
- **THALES projet S3NS** – Jeremy VERNET

Nous avons traité lors des deux plénières et des ateliers précédents, de nombreux dispositifs dont le dénominateur commun reste... **la donnée**.

Cet atelier décrira les modèles économiques de la donnée pour que le Citoyen reste acteur de sa sécurité, et afin également d'augmenter l'acceptabilité des nouvelles technologies, dont IA.

- Qui est propriétaire de la donnée ? Et ensuite, de quelles données parlons-nous ?
- Les données partagées (exemple : nombre de bancs dans la ville et leur localisation)
- Les données confidentielles (exemple : combien de parisiens ont quitté la capitale durant le covid, et quand, et pourquoi...)
- Les données brutes : comment est-il possible de les valoriser ? Puis comment les partager ?
- Les données transformées (exemple : tableaux de bord, analyse croisée de plusieurs flux...)
- Quels sont les modes opératoires (produire, stocker, traiter, diffuser...) ?



10. Quelles technologies pour la résilience inondation, tremblement de terre, NRBC...

11. Quelles données pertinentes pour accroître la résilience ?

12. Quelles nouvelles idées pour l'IA ?

Judi 23 mai – 14h50 à 16h00

## Atelier 12 : Quelles nouvelles idées pour l'IA ?

- EVITECH – Robert COUTIN
- PA CONSEIL – Hervé PETIT
- SENSIVIC – Bruno TATY
- AXIS – Philippe BENARD

Au sein de l'AN2V, nous avons dénombré 180 usages possibles en matière de sûreté !  
Il est aisé d'affirmer que la créativité en IA sur le court, moyen et long terme sera au rendez-vous !

Cet atelier a pour objectif de décrire quelques futurs possibles, au travers des questions suivantes :

- Le futur certain, les invariants,
- Le futur interdit, ce qui ne doit pas être,
- Le futur tendanciel, ce qui a déjà commencé, les différents chemins qui s'offrent à nous,
- Le futur stratégique, quels seront les obstacles à surmonter vers ces futurs ?
- Les options : Quels sont nos degrés de liberté pour surmonter ces obstacles ?

# Testimoniaux des universités

« C'est un salon important pour les intégrateurs et systémiers qui se différencie des autres salons de sécurité plus orientés équipement. C'est un salon majeur pour les donneurs d'ordre pour bien comprendre les enjeux de la mise en œuvre d'un système de sécurité, et des points d'attention associés pour avoir de vrais gains opérationnels. »

« Les universités sont matures et permettent de rencontrer les différents acteurs du secteur en un seul lieu sur une durée précise. »

« Un évènement professionnel à considérer sérieusement dans l'écosystème «sûreté et sécurité». La qualité des intervenants, des prospects et des exposants, permet de réelles découvertes mais aussi un networking très efficace, au niveau régional comme au niveau national. Un évènement où il faut être présent. »

« Un bon moyen de faire le point sur «l'état de l'art», de voir quelles lacunes combler, de rencontrer facilement des acteurs de la sécurité/sûreté (pairs et fournisseurs).

Une organisation bien rodée pour recueillir un maximum d'informations en un minimum de temps : deux jours aux Universités de l'AN2V valent bien deux semaines de recherches et rencontres organisées à titre individuel ! »

« Merci encore pour votre efficacité et votre sympathie, nous avons réellement apprécié la qualité des personnes présentes sur le salon, et les échanges réalisés. »

« Encore félicitations pour l'évènement et l'animation. »

« Juste un rapide message pour vous remercier et vous féliciter pour ce bel évènement. Ce fut une réussite, mais cela n'est pas une surprise connaissant les artisans...

A titre personnel, j'ai passé de bons moments d'échange, de convivialité et de satisfactions. A titre professionnel, je suis très satisfait de l'exposition et des contacts noués, des rencontres et des opportunités. »

« Nous n'aurions pas été excellents si vous-mêmes, vous ne l'aviez pas été également ! Encore un grand coup de chapeau pour toute l'organisation et votre disponibilité sur ces deux jours ! »

« C'est un salon important pour les intégrateurs et systémiers qui se différencie des autres salons de sécurité plus orientés équipement. C'est un salon majeur pour les donneurs d'ordre pour bien comprendre les enjeux de la mise en œuvre d'un système de sécurité, et des points d'attention associés pour avoir de vrais gains opérationnels. »

« Merci à vous, très belle organisation et très bon évènement. »

« Je vous remercie pour la sympathique organisation de cet évènement et la qualité des intervenants. »

« Je m'associe à mes camarades du 04 et 05 pour vous remercier de nous avoir permis d'assister gracieusement aux universités de l'AN2V. C'est pour nous l'occasion de découvrir de nouveaux produits et des nouvelles technologies, d'échanger avec tous les acteurs de la sûreté et d'assister à des plénières et ateliers très instructifs avec des intervenants compétents. Sans parler de la qualité des cocktails déjeunatoires et de la soirée au château de Monchat ; un grand merci. »

« Je participe à de nombreux colloques, et il est rare de trouver une telle qualité chez les exposants et intervenants. J'ai bien compris plusieurs points importants pour moi, les choses sont plus claires, et j'ai noué de bons contacts. »

« Un grand remerciement pour ce salon et les échanges très constructifs obtenus. Un très agréable salon, une belle organisation, félicitations. »

« RDV indispensable pour les utilisateurs de solution. »

Site du PMC à Strasbourg



# Pour les congressistes (inscription en ligne)

Les universités  
de l'AN2V



Cette inscription comprend l'accès aux stands, les deux séances plénières ainsi que les douze ateliers, les repas pour les deux jours, et la soirée de prestige.

Inscription en ligne

[www.an2v.org](http://www.an2v.org) ou ce QR-code

Journalistes, utilisateurs finaux privés et publics,  
forces de sécurité intérieure : **Gratuit**

(une adresse e-mail avec un nom de domaine identifiable est requise :  
@afp.fr, @ratp.fr, @interieur.gouv.fr, @mairie-lyon.fr, ...)



Membres entreprises AN2V

**90€ HT**, soit 108€ TTC

Autres participants au congrès

**290€ HT**, soit 348€ TTC

# Pour les congressistes (inscription papier)

Cette inscription comprend l'accès aux stands, les deux séances plénières ainsi que les douze ateliers, les repas pour les deux jours, et la soirée de prestige.

Veuillez retourner la présente page dûment remplie à l'adresse suivante :

AN2V – 1 quai Colbert – 30240 Le Grau-du-Roi

Accompagnée le cas échéant de votre chèque d'un montant de 108€ TTC ou 348€ TTC.

Mme

M

Nom

Prénom

Fonction

Raison sociale

Adresse postale

E-mail

Tél. portable

# Les universités de l'AN2V

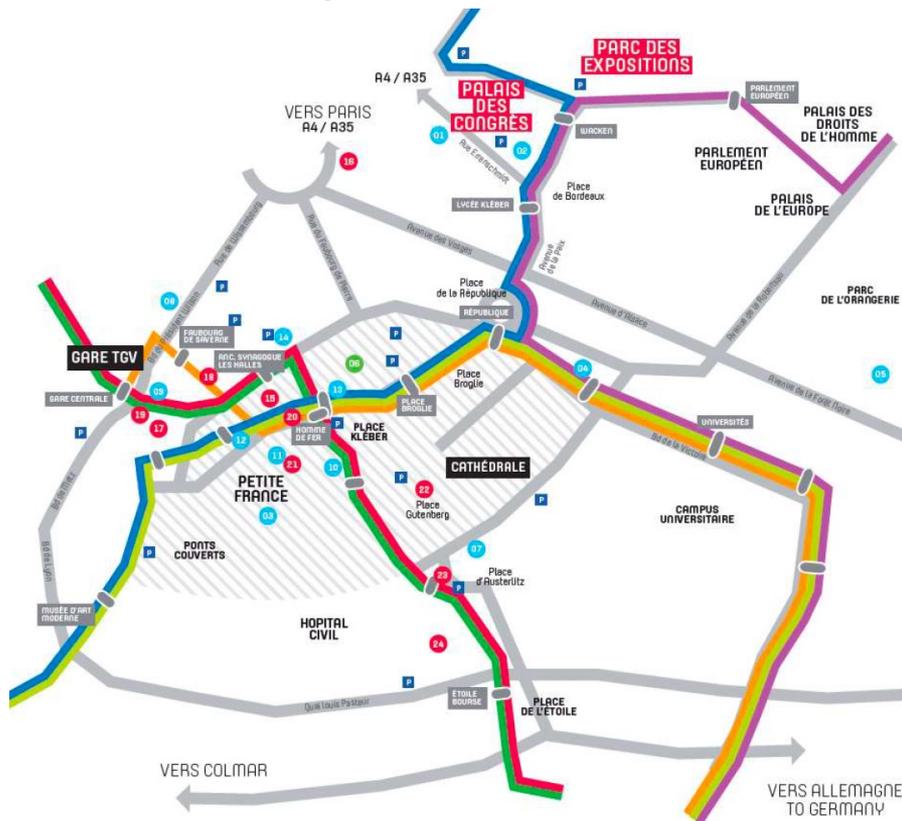


Les universités  
de l'AN2V

AN2V

Accès au salon :

❖ à 15mn de la gare TGV !



## LIAISONS DIRECTES EN TGV NATIONAL

- Paris : 1h45
- Aéroport Charles de Gaulle (CDG) : 1h51
- Metz : 0h51
- Dijon : 1h55
- Marne-la-Vallée : 1h59
- Massy : 2h36
- Lille : 2h51
- Lyon : 3h50

## LIAISONS DIRECTES EN TGV INTERNATIONAL

- Stuttgart : 1h17
- Basel : 1h18 \*
- Luxembourg : 1h40
- Frankfurt : 1h45
- Zurich : 2h20\*\*
- Bruxelles : 3h32
- Munich : 3h42

\* en TER (Train Express Régional)

\*\* liaison avec une correspondance à Bâle



## EN AVION L'Alsace dispose de 2 aéroports :

- L'AÉROPORT DE STRASBOURG : à seulement 9 min du centre-ville, desservi 4 fois par heure par une navette train. Accès moyen et long courrier renforcés par :
  - 2 vols quotidiens Strasbourg - Amsterdam permettant de bénéficier du HUB d'Air France - KLM
  - 4 aéroports internationaux à moins de 2h30 : Francfort, Baden-Baden, Stuttgart et Zurich
- L'EUROAIRPORT BÂLE-MULHOUSE-FRIBOURG situé à 1h30 de Strasbourg



## ACCÈS AUTOROUTES

À 2 minutes du Palais des congrès :

- Axe Paris- Lyon A35
- Axe Grand Est A4 Connexions Bénélux
- Autoroutes allemandes par le Pont de l'Europe à 10 min du Palais des congrès



# Les Universités de l'AN2V

Dominique LEGRAND

Président & Fondateur

06 07 86 07 68

[dl@an2v.org](mailto:dl@an2v.org)



Inscrivez-vous !  
En flashant ce code



AN2V

1, quai Colbert  
30240 Le Grau-du-Roi

