IN CYBER FORUM EUROPE

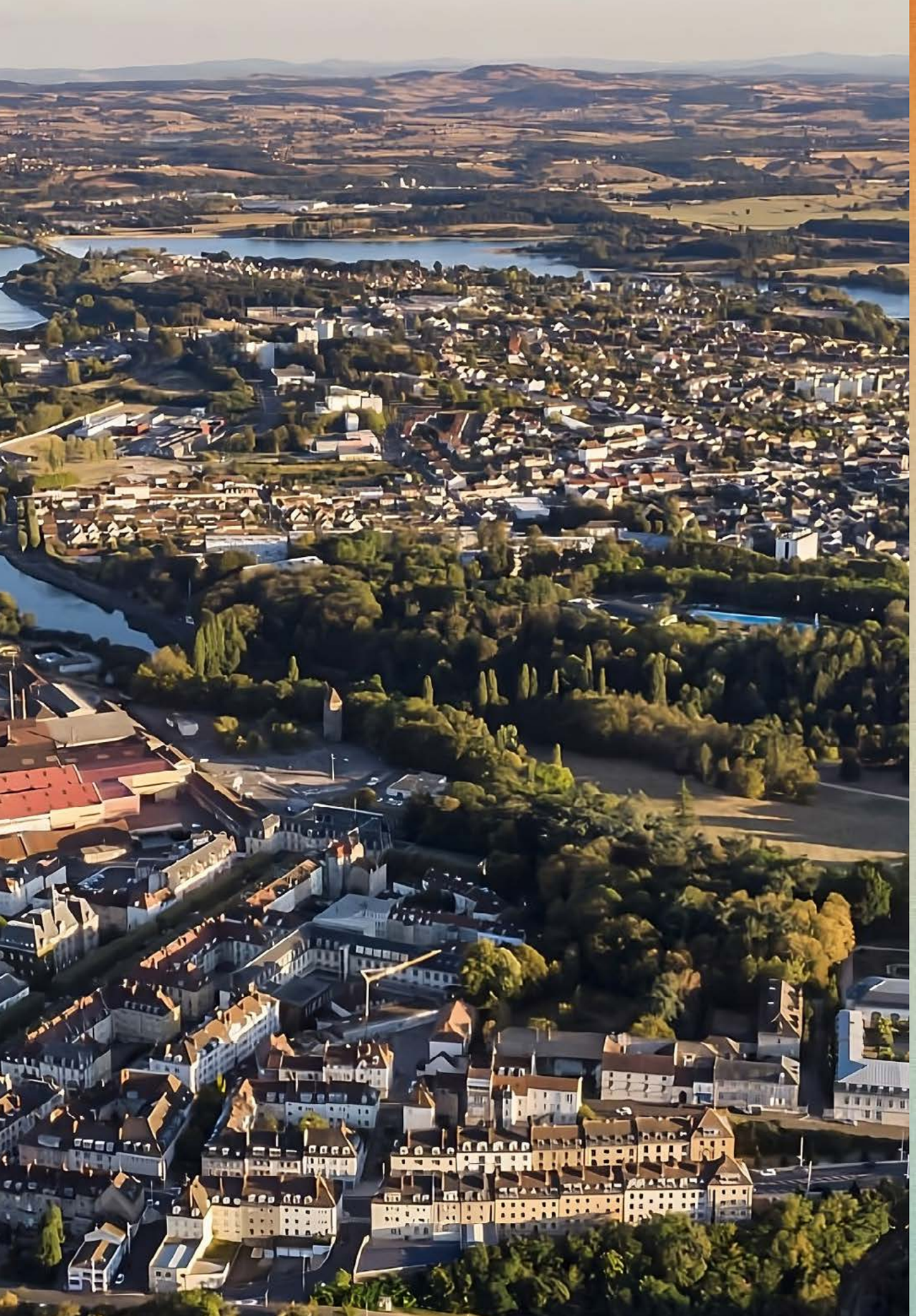
Creusot Montceau Communauté Urbaine

FORUM INCYBER DES TERRITOIRES

TERRITOIRE 4.0 & CYBERSÉCURITÉ INDUSTRIELLE

HUB & GO, LE CREUSOT

22-23 MAI 2025



AVANT PROPOS

Ce document reprend les idées forces qui ont conduit à la création du Forum INCYBER des territoires, dont la première édition a eu lieu, au sein du Hub&Go du Creusot, les 22 et 23 mai 2025.

Les rencontres avec David Marti, président de la Communauté urbaine Creusot Montceau, ses interventions lors des Forums INCYBER Europe à Lille ou lors d'une Agora du Forum, ont fait mûrir une réflexion conjointe, engagée depuis maintenant trois ans, entre la Communauté urbaine du Creusot Montceau et le Forum INCYBER.

Ce Forum INCYBER des territoires s'inscrit dans la durée, puisque sa prochaine édition annuelle aura lieu les 11 et 12 juin 2026 et sera précédée de manifestations intermédiaires — notamment lors du colloque de France Urbaine - destinées à consolider une volonté collective d'aller plus loin ensemble pour faire du territoire un espace cybersécurisé.

Le Forum INCYBER des territoires se veut l'incubateur d'un état d'esprit volontariste qui donne du sens à une transformation numérique reformatant notre société et replace le citoyen, le décideur politique et l'acteur économique au cœur de la cybersécurité en apportant les réponses attendues aux interrogations du terrain.

GÉNÉRAL D'ARMÉE (2S) WATIN-AUGOUARD
Fondateur du Forum INCYBER

Le panel des intervenants

Yves SEGUY, préfet de Saône-et-Loire

David MARTI, maire du Creusot, président de la Communauté urbaine du Creusot Montceau

Murielle LAURENT, députée européenne

Vincent THOMAS, président de l'université Bourgogne Europe

Jean-Marc AUTRET, responsable de la sécurité des systèmes d'information industriels - EDF

Nicolas BERTHAUT, directeur général de l'agence régionale du numérique et de l'intelligence artificielle (ARNIA)

Véronique BRUNET, déléguée à la sécurité du numérique pour la région Bourgogne-Franche-Comté (ANSSI)

Hakim DJELILI, expert en cyberdéfense chez Cyber-expert

Ylan ELKESLASSY, directeur de l'organisme de formation cyber chez Sysdream

David FLOTAT, colonel de gendarmerie, chef de la division proximité numérique

David FOFI, directeur du département robotique (Polytech)

Nicolas HUEZ, co-fondateur d'Interstis

Christophe HUSSON, général de division, commandant du COMCYBER-MI

Sabri KHEMISSA, expert en cybersécurité des installations industrielles Fortress Cybersecurity

Pierre KIRCHNER, directeur général d'Equans Digital Cyber

Arnaud KOPP, consultant cybersécurité

Jean-Yves LAGRANGE, DSI de la Communauté urbaine du Creusot Montceau

Clarisse MAILLET, présidente de la CPME71

Stéphane MENJAUD, directeur des ventes chez Allentis

Sébastien MOREY, responsable du CSIRT Bourgogne-Franche-Comté

Jérôme NOTIN, directeur général de Cybermalveillances

Jérémy PINTO, vice-président de la CUCM, délégué à l'enseignement supérieur, la recherche et l'innovation

Vincent POULBÈRE, directeur exécutif de Sysdream

Emmanuelle SIMON, Trust Valley (Suisse)

Guillaume TISSIER, directeur général du Forum INCYBER Europe

Marc WATIN-AUGOUARD, fondateur du Forum INCYBER

SOMMAIRE

BÂTIR AVEC LES ACTEURS ET PARTENAIRES DES TERRITOIRES, LA CONFIANCE ET LA SOUVERAINETÉ NUMÉRIQUE DE DEMAIN

Le Forum INCYBER des Territoires naît au Creusot, sur le territoire de la Communauté Urbaine Creusot Montceau.

Le 1er Forum INCYBER des Territoires, organisé en mai 2025 au Creusot, a été bien plus qu'un événement fondateur : il a incarné une ambition collective. Co-organisé par la Communauté Urbaine Creusot Montceau et le Forum INCYBER Europe — acteur mondialement reconnu dans le domaine de la cybersécurité et de la confiance numérique — cet événement a permis de rassembler, sur notre territoire, les conditions d'un dialogue stratégique entre décideurs publics, industriels, experts et acteurs du numérique.

Notre territoire connaît aujourd'hui une dynamique sans précédent. Le renforcement de Framatome, l'arrivée de nouveaux projets industriels, l'attractivité grandissante de notre tissu économique et de nos infrastructures témoignent d'un élan qui ne cesse de s'amplifier. La Communauté Urbaine Creusot Montceau se positionne désormais comme un acteur incontournable de l'innovation au sens large notamment industrielle, technologique et numérique.

Cependant cette évolution rapide s'accompagne de nouveaux enjeux. Car derrière chaque avancée technologique : intelligence artificielle, automatisation, interconnexion des systèmes, se posent inévitablement des questions de sécurité et de maîtrise.

Aucun territoire, même le plus avancé, ne peut faire l'impasse sur la cybersécurité. Elle est aujourd'hui la condition indispensable à la continuité des services publics, à la compétitivité des entreprises, et à la sérénité des citoyens dans l'ère numérique.

C'est précisément pour accompagner ces transformations que la Communauté Urbaine Creusot Montceau a choisi de construire une stratégie volontariste : en soutenant l'élévation des compétences, en développant l'offre de formation et en consolidant un écosystème de coopération entre acteurs publics, industriels, académiques et numériques.

Cette vision est aussi celle que nous partageons avec le Forum INCYBER Europe. Depuis trois ans, nous avons su bâtir une relation durable, fondée sur la conviction que les territoires ont un rôle majeur à jouer dans la construction d'une souveraineté numérique solide, partagée et tournée vers l'avenir.

Le Forum INCYBER des Territoires a vocation à s'élargir, à s'ouvrir à d'autres partenaires, à intégrer pleinement la dynamique de Bourgogne Industrie (territoire d'industrie version 2).

Mais son ancrage géographique, lui, ne changera pas. C'est ici, au Creusot, terre d'industrie et d'innovation, qu'il continuera de se tenir.

Parce que ce territoire incarne, l'alliance entre excellence industrielle et innovation dans tous les domaines.

Ce livre témoigne des échanges riches et stimulants de cette première édition. Il capture l'essence d'un moment de convergence, de mobilisation et d'engagement de l'ensemble des acteurs de la cybersécurité et de nos partenaires encrés sur les territoires.

Fort de cette réussite collective, nous donnons rendez-vous à tous les acteurs publics et privés en juin 2026, pour une nouvelle édition du Forum INCYBER des Territoires, toujours au Creusot, pour continuer à bâtir la confiance et la souveraineté numérique de demain.

David Marti
Maire du Creusot
Président de la Communauté Urbaine Creusot Montceau

LES INDUSTRIELS

FRAMATOME

SAFRAN AIRCRAFT ENGINES

INDUSTEEL

ARCELOR MITTAL

BSE ELECTRONIC

INTERSIS

TURBINE CASTING

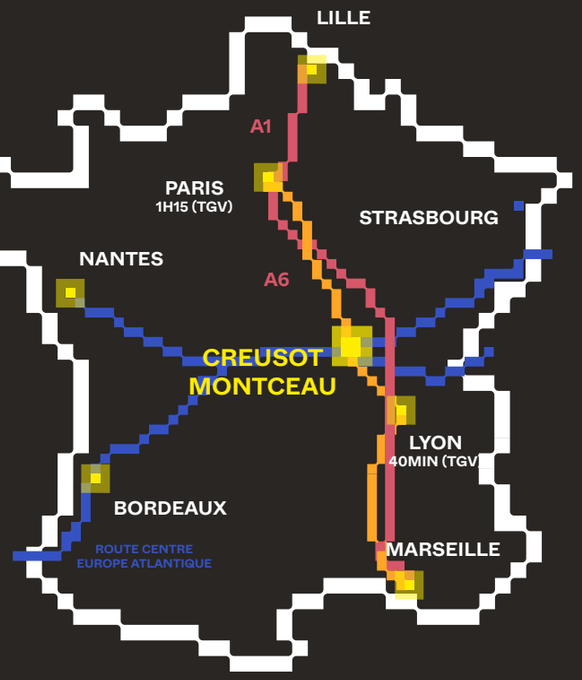
EVAMET

MATIERE

ALSTOM

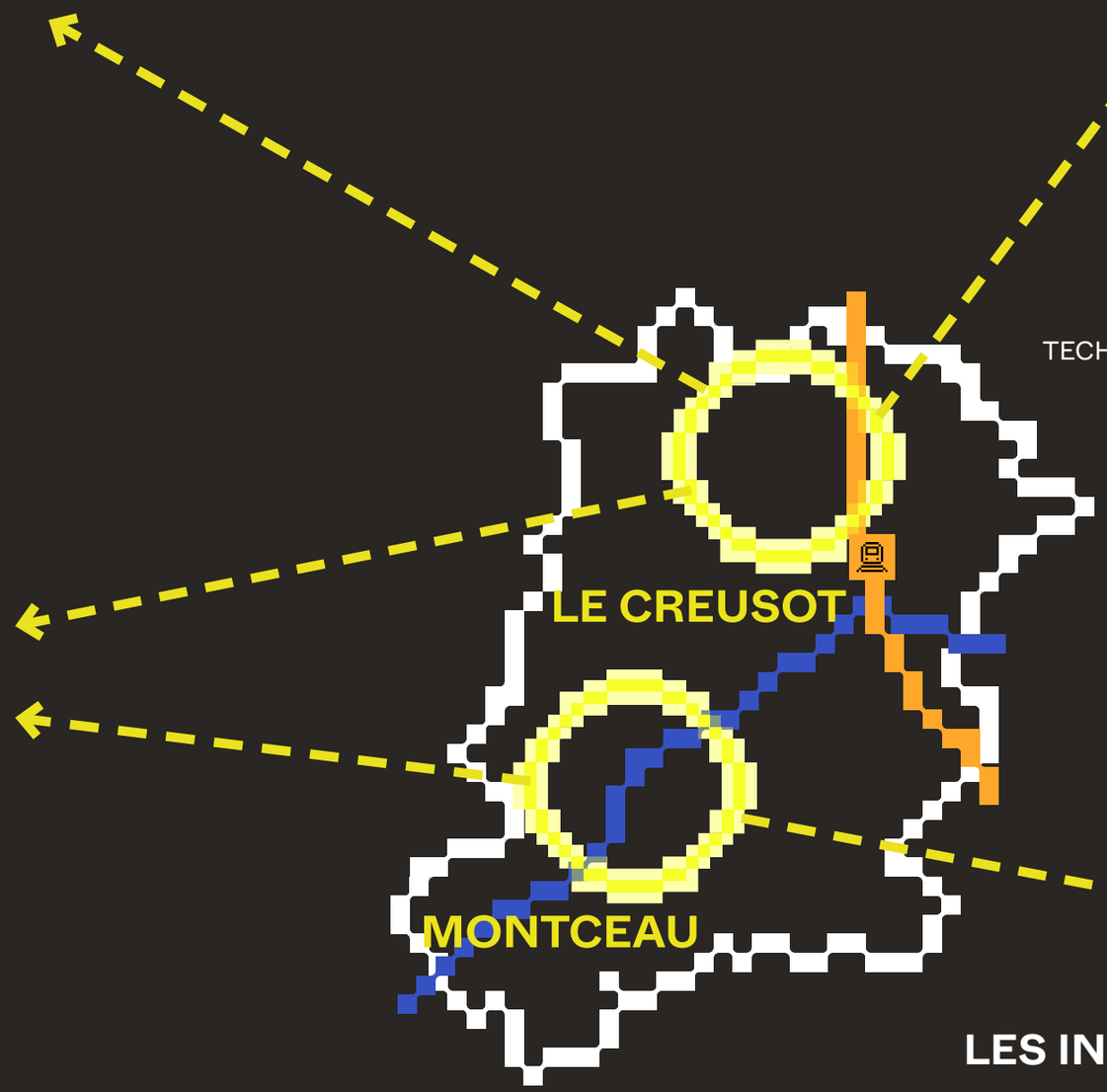
THERMODYN

BAKER HUGHES



CAMPUS SUD BOURGOGNE

8 ÉTABLISSEMENTS
D'ENSEIGNEMENT SUPÉRIEUR



LES INDUSTRIELS

COVAGE

JIMMY

MCGP

ATS INGENIERIE

ROBOT-COUPE

TECHNOLOGIES PERRIN

NOVIUM

ERION FRANCE

BUBENDORFF

BURACCO

POLAKOWSKI

TRONCY

METALLIANCE

SO BAG

MONNET

MICHELIN

LES INDUSTRIELS

Creusot
Montceau
Communauté Urbaine

MAÎTRISONS ENSEMBLE LA TRANSFORMATION NUMÉRIQUE

La cybersécurité est une politique publique qui prend de plus en plus d'importance en raison de l'intensité croissante des cybermenaces.

La France est l'un des pays d'Europe qui est le plus mature, comme en témoigne son influence dans l'élaboration des textes qui s'appliquent désormais au sein des 27 États membres, notamment les directives NIS1 puis NIS2, le règlement européen sur la protection des données à caractère personnel, le règlement européen sur la cybersécurité et celui sur la cyberrésilience. La prise de conscience des enjeux a conduit l'État à se doter d'une architecture et de moyens de cybersécurité qui ont pour ambition de protéger nos infrastructures vitales, nos administrations, nos collectivités territoriales, nos entreprises mais aussi le citoyen. Depuis le Livre Blanc de 2008, la stratégie française de cybersécurité de 2011, le Livre Blanc de 2013, la stratégie nationale de sécurité numérique de 2015, les revues stratégiques de cyberdéfense de 2018 et de 2025, la posture se renforce de manière continue, notamment au sein des ministères régaliens.

La cybersécurité est certes une politique publique, mais elle a aussi la particularité de faire appel à une coopération public/privé sans doute inédite. C'est une des raisons qui a inspiré la création de campus cyber où se côtoient civils et militaires, acteurs régaliens et entreprises pour mieux partager, pour trouver ensemble les voies et moyens d'une cybersécurité plus protectrice. Sans remettre en cause les compétences et les finalités propres, rien ne peut s'accomplir sans un décloisonnement, car chacun possède une parcelle de la solution. La lutte contre les prédateurs passe notamment par le développement de technologies mises à la disposition des défenseurs, des enquêteurs. Cette coopération est clairement évoquée par le ministre de l'intérieur, dans la stratégie de lutte contre la cybercriminalité qu'il a présentée le 30 mai dernier.

Compte tenu des caractéristiques d'internet, du web, des réseaux sociaux, une approche internationale, européenne et nationale est indispensable. Mais est tout aussi indispensable une action s'appuyant sur les territoires. Ce sont des espaces à taille humaine où peuvent se tisser des liens, où peut naître une approche collaborative de la cybersécurité rassemblant tous les acteurs concernés.

Représentant de l'État dans le département, il m'appartient d'assurer une coordination interministérielle de toutes les administrations déconcentrées de l'État. Mais je suis aussi convaincu de la nécessité de contribuer à une entreprise collective qui agrège les initiatives développées par les collectivités territoriales, par les universités, par les entreprises, par les associations, par les citoyens. Je crois aussi que la transformation numérique est une opportunité pour un développement harmonieux des territoires, qu'ils soient urbains ou ruraux, qu'ils relèvent de la Communauté urbaine ou des communautés de communes avoisinantes.

C'est pourquoi le forum, créé par la CUCM, présidée par David Marti, et le Forum INCYBER, répond à une nécessité, alors que le territoire connaît une mutation sans précédent avec le développement ou l'implantation d'entreprises de haute technologie, à forte valeur ajoutée. L'innovation, le développement économique, l'acculturation de tous aux technologies numériques parfois disruptives, nous invitent à mieux comprendre, partager, agir, chacun dans son domaine, pour appréhender des changements qui s'opèrent en s'accélérant. La maîtrise de la transformation numérique, avec ses facettes positives et négatives, est une condition de la construction d'un « territoire de tous les possibles ».

Le Forum INCYBER des territoires au Creusot est appelé à se pérenniser, c'est bien la preuve qu'il n'est pas un événement qui sacrifie à la mode, mais la réponse à une demande. La satisfaction exprimée par tous après sa première édition est un encouragement à poursuivre une aventure, dont les effets devraient dépasser la géographie de la Communauté urbaine pour profiter à l'ensemble de notre département de Saône-et-Loire. C'est un de mes souhaits les plus chers.

Dominique DUFOUR
Préfet de Saône-et-Loire

AGIR AU SEIN DES TERRITOIRES POUR RENFORCER LA CYBERSÉCURITÉ EUROPÉENNE

La cybersécurité est un enjeu majeur pour nos sociétés.

Une cyberattaque peut naître à l'autre bout du monde et avoir des répercussions immédiates sur une commune, un service public, une entreprise.

Face à cette réalité, il était essentiel que les États membres de l'Union européenne renforcent leur coopération pour mieux détecter, préparer et réagir face aux cybermenaces.

Une stratégie européenne, aussi ambitieuse soit-elle, ne peut être efficace qu'à condition de s'ancrer dans les territoires, au plus près des citoyens.

C'est sur le terrain — collectivités, institutions, acteurs économiques — que les politiques européennes trouvent leur pleine légitimité, lorsqu'elles se traduisent en actions concrètes.

C'est à l'échelon local que s'organisent les actions de sensibilisation, de formation et d'accompagnement. Les territoires sont les premiers points de contact lorsqu'il est question de la sécurité des données publiques ou de protection d'infrastructures critiques. Ils transforment les ambitions européennes à travers des initiatives variées : formations, partenariats entre acteurs publics et privés, réseau d'entraide. Cette proximité favorise également l'implication des citoyens, qui deviennent ainsi des acteurs de la sécurité numérique.

Le Forum INCYBER des Territoires a permis de mettre en lumière certaines de ces actions.

La force de l'Europe repose sur sa capacité à conjuguer une vision commune avec la diversité et la richesse de ses territoires. En soutenant les initiatives locales, en encourageant l'innovation, l'Union européenne construit une cybersécurité à la fois solide et proche des citoyens.

Agir au sein des territoires, c'est donc contribuer à l'édifice européen de la cybersécurité.

Cette démarche favorise la réactivité, offre des solutions adaptées et renforce la confiance. La mobilisation de chacun — élus, citoyens, entreprises — est essentielle pour la protection de notre avenir numérique commun.

Murielle LAURENT
Députée européenne

VERS UN SMART TERRITOIRE ÉTHIQUE, INCLUSIF & DURABLE

La Communauté Urbaine Creusot Montceau (CUCM) s'engage dans une transformation numérique ambitieuse pour devenir un territoire intelligent, durable et inclusif.

En intégrant l'Intelligence Artificielle (IA) responsable et éthique, ainsi que des technologies innovantes, la CUCM vise à améliorer la qualité de vie des habitants, optimiser la gestion des ressources et renforcer l'attractivité économique, tout en garantissant une approche respectueuse des enjeux sociaux et environnementaux.

INNOVER AU SERVICE DE TOUS

Le programme « Smart Territoire » de la communauté urbaine repose sur une utilisation éthique et inclusive des technologies numériques, garantissant leur accessibilité et leur contribution au développement durable. Parmi les initiatives mises en place figurent :

- Le déploiement de capteurs intelligents sur les réseaux d'eau et d'électricité permettant d'assurer une surveillance en temps réel pour réduire le gaspillage et améliorer l'efficacité énergétique, dans une logique de sobriété et de préservation des ressources.
- Une mobilité connectée et responsable avec des outils numériques facilitant l'accès aux transports publics et aux mobilités douces, pour une ville plus fluide et moins polluante.
- Un éclairage public intelligent et bas carbone avec des luminaires adaptatifs réduisant la consommation énergétique et limitant la pollution lumineuse.
- Des espaces publics numériques inclusifs : bornes interactives et plateformes accessibles pour informer, impliquer et donner une voix aux citoyens dans l'amélioration des services urbains.

L'INTELLIGENCE ARTIFICIELLE, PILIER D'UN TERRITOIRE RESPONSABLE

L'IA appliquée à la gestion du territoire repose sur des principes d'éthique, de transparence et d'inclusion afin de garantir un développement équilibré et équitable :

- L'IA doit être éthique et transparente, par une utilisation de données ouvertes et sécurisées pour optimiser les décisions sans biais ni discrimination.
- L'optimisation des services publics et des ressources résulte d'une allocation intelligente des budgets ; elle permet une amélioration des services urbains et une réduction de l'empreinte écologique.
- L'accompagnement des citoyens et des entreprises s'opère avec des assistants virtuels et de plateformes interactives favorisant l'accessibilité aux démarches administratives et aux opportunités économiques.

La démarche de la Communauté urbaine s'inscrit pleinement dans l'esprit du rapport sénatorial « IA, Territoires et Proximité » d'Amel Gacquerre et de Jean-Jacques Michau.

« La révolution de l'IA pourrait marquer une troisième étape de la numérisation des territoires, après celle de l'apparition des ordinateurs, puis celle du développement d'Internet et des communications numériques ».

UNE AMBITION FORTE POUR UN TERRITOIRE DURABLE ET INCLUSIF

Le projet « Smart Territoire » de la CUCM est une première étape vers un modèle de développement territorial résilient et évolutif. L'objectif est de généraliser ces innovations tout en garantissant une approche éthique, responsable et durable par le déploiement à grande échelle des capteurs intelligents pour une gestion optimisée des ressources naturelles et une réduction des émissions carbone. S'ajoutent le développement de solutions de mobilité inclusive assurant l'accessibilité pour tous, notamment les personnes à mobilité réduite, et la mise en place d'un réseau de bâtiments intelligents et bas carbone, intégrant des technologies IA respectueuses de l'environnement.

Cette ambition est soutenue par la formation de personnels de la Communauté urbaine et, avant tout, par leur engagement. Le succès ne repose pas seulement sur la technologie ; il ne peut être atteint sans une appropriation humaine et collective d'un projet qui va transformer le territoire.

Avec sa vision « Smart Territoire », la CUCM ambitionne de faire de l'innovation un levier de transformation durable, responsable et inclusive, au service des habitants, des entreprises et des générations futures. D'où l'importance de construire une cybersécurité collective et collaborative.

Evelyne COUILLEROT
2e Vice-présidente de la Communauté urbaine Creusot Montceau
1ère adjointe du Creusot
Conseillère départementale

CONTRIBUER ACTIVEMENT À LA SÉCURITÉ DES TERRITOIRES, DE LEURS INSTALLATIONS ET DE LEURS HABITANTS.

EDF porte des services critiques pour assurer la continuité du système électrique. Pour garantir l'approvisionnement de l'électricité, bien de première nécessité, nous opérons des infrastructures essentielles, nous assurons la résilience de nos installations et la sécurité de nos données.

Nos infrastructures, de plus en plus numériques, gagnent en performance mais s'exposent à des menaces accrues. La cybersécurité n'est pas une option ; elle conditionne la continuité de nos services d'importance vitale, la confiance dans la transition énergétique et la résilience de nos territoires.

Pour assurer ses missions, EDF a mis en place une gouvernance dédiée, appuyée sur une communauté métier et sur un Centre d'Excellence Cyber, qui fédère pratiques, expertises et outils du Groupe. La cybersécurité n'est pas qu'un sujet technique. Elle exige une veille permanente et une coopération étroite et transparente entre industriels, institutions et collectivités.

Les nouvelles réglementations européennes, comme NIS2 et *Cyber Resilience Act,* renforcent cette exigence. Ces textes traduisent une ambition collective : bâtir une souveraineté numérique solide et partagée.

Le Forum INCYBER des Territoires incarne cette volonté. Il offre un espace de dialogue, ancré dans les réalités locales pour renforcer les synergies entre acteurs publics et privés. EDF est fier d'y participer aux côtés de la Communauté Urbaine Creusot Montceau et des différents acteurs publics et privés. Fort de son implantation historique dans ce territoire industriel via Framatome, EDF réaffirme son engagement : fournir une électricité décarbonée et souveraine, soutenir le renouveau de l'industrie nucléaire en France et en Europe et contribuer activement à la sécurité des territoires, de leurs installations et de leurs habitants.

Bernard FONTANA
Président directeur général d'EDF

LA FORMATION ET L'INNOVATION, AVENIR DES TERRITOIRES

L'avenir des territoires se construit et se construira par la formation et l'innovation !

Le succès de cette première édition confirme l'ambition du territoire de la Communauté Urbaine Creusot Montceau (CUCM) comme un acteur incontournable de la cybersécurité. La publication de ce « Livre Blanc » du premier Forum INCYBER des Territoires en est la démonstration.

L'évolution rapide du numérique dans la société transforme profondément les territoires et redéfinit les enjeux de formation et de compétences. En participant au forum organisé par la CUCM, j'ai souhaité partager la vision universitaire d'un accompagnement renforcé de cette mutation, particulièrement sur le territoire bourguignon.

Le Creusot bénéficie d'un écosystème d'enseignement supérieur remarquable avec une présence forte de l'Université Bourgogne Europe, notamment à travers l'IUT - qui célèbre cette année ses 50 ans d'existence - et l'école d'ingénieur Polytech. Cette configuration permet une opportunité d'accompagner les actions territoriales qui dépassent le cadre de la CUCM pour s'étendre à l'ensemble du territoire Bourgogne Industrie, créant ainsi un véritable continuum de compétences entre Le Creusot et Dijon.

Notre responsabilité collective est d'accompagner cette montée en compétences qui répond aux défis contemporains de l'industrie et du numérique. C'est dans cette perspective que nous soutenons les initiatives de formation innovantes, notamment dans le domaine stratégique de la cybersécurité, secteur en pleine expansion qui nécessite des professionnels hautement qualifiés.

Lors des prochaines Journées Nationales de France Urbaine, événement d'envergure nationale qui se tiendront en octobre au Creusot, des ateliers et tables rondes seront dédiées à l'enseignement supérieur. Ces échanges viendront parfaitement illustrer notre capacité collective à innover et à former les talents de demain.

Comme j'ai pu l'exprimer sur le plateau de « B Smart TV » lors du Forum INCYBER, la démarche de l'Université Bourgogne Europe s'inscrit dans une logique de territoire apprenant, où formation, innovation et industrie se nourrissent mutuellement. Cette synergie entre acteurs publics et privés, entre formation initiale et continue, entre recherche et application, constitue le socle d'un développement réussi.

L'Université Bourgogne Europe assume un rôle d'accompagnement de cette dynamique, convaincue que l'excellence de nos formations et la qualité de nos partenariats institutionnels sont les clés de notre rayonnement national et international.

Vincent THOMAS
Président de l'université de Bourgogne Europe

UNE CYBERSÉCURITÉ ENRACINÉE DANS LES TERRITOIRES

Chez Equans Digital Cyber, nous sommes convaincus que la cybersécurité doit s'ancrer dans les territoires, au plus près des infrastructures critiques, des collectivités et des industries locales. C'est pourquoi nous déployons une stratégie d'accompagnement de proximité, sur les trois grands marchés que sont l'Industrie, le Tertiaire et les Villes & Territoires.

Notre force repose sur un réseau national et international, qui nous permet d'être présents là où nos clients ont besoin de nous. En tant qu'expert de la sécurité IT et OT, nous nous appuyons sur l'ADN historique d'intégrateur de terrain du groupe Equans, avec une parfaite maîtrise des environnements techniques : automatisme, supervision, réseaux industriels et télécoms.

Nous mettons un point d'honneur à accompagner les collectivités dans tous les domaines de la cybersécurité : réglementation, audits, solutions techniques, sensibilisation, afin de renforcer la résilience des territoires. C'est notamment le cas dans la région du Creusot, où notre engagement local illustre pleinement cette approche.

Nos équipes certifiées PASSI, nos centres opérationnels de sécurité, et notre capacité à agréger des solutions innovantes — qu'elles soient issues de grands éditeurs ou de start-ups — nous permettent de proposer des dispositifs sur-mesure, robustes et évolutifs. Equans Digital Cyber incarne une cybersécurité de proximité, durable et souveraine.

Pierre KIRCHNER
CEO Equans Digital

CYBER ET TERRITOIRES : LE PARADOXE

Ces deux mots, choisis pour un forum organisé au Creusot, peuvent sembler antinomiques. Le cyberespace est un substrat qui irrigue tous les milieux, terrestre, maritime, aérien, extra-atmosphérique, en s'affranchissant des frontières. C'est une concrétisation du rêve de Paul Otlet, Prix Nobel de la Paix, qui, dès le début du vingtième siècle, voulait relier toutes les bibliothèques du monde par le téléphone. Utopie réalisée quelques décennies plus tard par le web « partout, pour tous, sur tout ». La connexion de quatre universités américaines, en 1969, est le début d'une aventure, au sein de la Silicon Valley, qui va très vite prendre une dimension planétaire. S'inscrivant dans un mouvement New Age de contre-culture américaine, la construction du cyberespace semble vouloir fait fi des frontières, comme en témoignent Marshall McLuhan et son « Village planétaire » ou la Déclaration d'indépendance du cyberespace, prononcée par John Perry Barlow, à Davos, en 1996 : « Gouvernements du monde industriel, vous géants fatigués de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit. Au nom du futur je vous demande à vous du passé de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté là où nous nous rassemblons ». Comme si le cyberespace pouvait être entièrement à part, alors qu'il est de notre monde à part entière.

Au même moment, l'accélération de la construction du cyberespace, encouragée par l'administration Clinton-Gore, ouvre la voie au développement d'un maillage, d'un réseau des réseaux, reliant plus de 120 000 *« autonomous systems »*. Ce réseau a bien une dimension physique : les câbles sous-marins, les réseaux fibrés, les modems, routeurs, serveurs, satellites, qui en permettent le fonctionnement, peuvent faire l'objet d'une cartographie : le matériel est bien le support de l'immatériel. Les frontières demeurent, même si elles sont poreuses face à l'extraterritorialité de certaines lois étrangères, à la domination des *Big Tech,* à l'action des prédateurs agissant généralement depuis des pays tiers. Les États conservent des compétences, notamment juridiques, essaient de sauvegarder leur souveraineté numérique, mettent en œuvre des stratégies pour protéger les personnes physiques ou morales des cyberattaques d'origine souvent étrangère. Mais les solutions exigent souvent d'agir au sein d'entités supranationales, comme en témoigne la stratégie de l'Union européenne en vue de garantir un cyberespace ouvert et sûr. Peuvent être également cités l'OCDE, voire l'ONU.

Dans contexte, les territoires sont-ils pertinents pour accompagner, favoriser, protéger une transformation numérique qui s'accélère ? Tandis que l'élargissement géographique semble une condition pour garantir une meilleure gouvernance du cyberespace, peut-on s'appuyer sur des espaces plus restreints, comme celui de la Communauté urbaine du Creusot Montceau pour conduire une politique ambitieuse ?

C'est sans doute le paradoxe qui motive une approche « micro » quand la tendance pousse à raisonner à une échelle « macro ». Comment expliquer une telle démarche ?

UN TERRITOIRE À DIMENSION HUMAINE POUR UNIR LES FORCES

La dimension humaine est sans doute une des premières réponses. Contrairement à d'autres technologies, le numérique échappe à notre perception,

à nos sens. Il est le domaine de l'infiniment grand, de l'infiniment rapide, de l'infiniment petit. Si Internet est l'âge de la multitude, il est aussi celui de la solitude, celle des personnes physiques et morales confrontées à un incident, à une cyberattaque. La réponse est d'abord locale, fruit d'une proximité qui rapproche les acteurs publics et privés et permet de construire des liens de solidarité. L'union fait la force ! La Communauté urbaine du Creusot Montceau est associée avec la ville de Dijon au sein de Bourgogne Industrie. Ainsi, près de 500 000 habitants partagent une même histoire, une même géographie politique et sociale, tout en associant de manière harmonieuse l'urbain et le rural, l'industrie, l'artisanat et l'agriculture. Cette diversité a pour trait d'union un besoin commun de maîtriser les évolutions des technologies numériques, d'en conjurer les effets négatifs. Sans préjudice des réponses nationales, il est nécessaire de développer des réponses locales. La proximité est sans doute un complément nécessaire à l'universalité. De même que la mer réunit une communauté des « gens de mer », il est aujourd'hui nécessaire de créer une communauté des « gens du cyber ». Si l'amiral peut dialoguer avec le marin pêcheur, l'élu en charge d'une collectivité locale, le gestionnaire d'un service public, le capitaine d'industrie, le créateur de startup partagent les mêmes interrogations, les mêmes attentes, quand bien même les enjeux seraient différents par nature, par intensité. Solidaires et non solitaires, les acteurs peuvent trouver au sein d'un territoire un espace d'échange. La Communauté urbaine du Creusot Montceau et les communautés de communes qui la jouxtent constituent un espace propice à une telle démarche collective qui s'inscrit dans la durée. Le Forum INCYBER des territoires offre cette opportunité.

LA « TRIPLE HÉLICE », MOTEUR DE L'ESSOR D'UN TERRITOIRE

Une telle initiative ne peut se concevoir sans une impulsion politique. Dès lors qu'une équipe porte une « idée force », celle de créer un « territoire de tous les possibles », les initiatives publiques ou privées peuvent trouver un terreau propice au développement, à l'innovation. L'histoire de la Silicon Valley met en évidence la concordance entre une action politique, l'existence de grandes universités (dont Stanford), d'entreprises de haute technologie, des petites entreprises, des startups et la commande publique qui soutient leur dynamisme. Le modèle de la « Triple Hélice » repose sur une coopération étroite entre universités, entreprises et acteurs publics.

Si l'expression « Silicon Valley de la Bourgogne » e st employée à propos du Creusot Montceau, la comparaison pourrait prêter à sourire, compte tenu des différences d'échelle. Cependant, il semble bien que la dynamique, le mécanisme, expliquant le développement du territoire californien soient aujourd'hui le moteur de l'essor de la Communauté urbaine du Creusot Montceau. En témoignent la diversification industrielle, l'implantation d'entreprises nationales, européennes ou internationales, le développement de formations d'avenir (IA, cobotique) au sein de l'université de Bourgogne Europe. Ces créations multiples, complémentaires sont comme un appel d'air qui prouve l'attractivité d'un territoire d'équilibre. Le Forum INCYBER est une des manifestations du spectaculaire renouveau industriel d'un territoire hier en déclin.

TRUST VALLEY, UN MODÈLE À EXPLORER

Sans regarder outre-Atlantique, il est intéressant d'explorer les territoires qui ont déjà entrepris une démarche similaire. Trust Valley en Suisse est un exemple pertinent.

Cet exemple, toutes choses étant égales par ailleurs, montre combien la cristallisation d'une ambition exige du temps, de la constance dans la démarche, bien que les résultats ne soient pas aussi rapides que ce que l'on souhaiterait. « Là où il y a une volonté, il y a un chemin ». Les enjeux sont trop importants pour faire l'impasse sur une coopération qui transcende les différences.

LA TRUST VALLEY : MUTUALISER POUR SE PROTÉGER

La Trust Valley est une alliance visant à promouvoir toute l'expertise de la région lémanique dans le domaine de la confiance numérique et de la cybersécurité. Cet écosystème public-privé, a été créée il y a environ 5 ans sur une initiative de la fondation EPFL Innovation Park. Localisée sur le pourtour de l'Arc Lémanique, elle rassemble et fédère un réseau d'acteurs publics (à l'échelon cantonal ou confédéral), des acteurs académiques, universités et grandes écoles (dont l'École Polytechnique Fédérale de Lausanne) et de nombreuses entreprises, dont Kudeslki Security et SIGPA. Deux grands secteurs structurent Trust Valley autour de Genève et de Lausanne, ce qui n'est pas sans rappeler les deux pôles Le Creusot Montceau et Dijon sur lesquels s'appuie Bourgogne Industrie.

La coopération s'articule autour de trois axes principaux : le rayonnement de cet écosystème unique, l'innovation et la mise en réseau des acteurs régionaux dans le domaine de la confiance numérique et de la cybersécurité. Il s'agit pour ces acteurs de travailler ensemble autour de cet écosystème et de proposer aux PME, aux infrastructures critiques, mais aussi de manière plus large aux citoyens, de vivre dans une société beaucoup plus sûre et beaucoup plus résiliente en matière de cybersécurité.

Trust Valley met à disposition des ressources partagées au sein d'une plateforme. Il s'agit, par exemple, de diagnostics cyber, d'audits, de campagnes de prévention de *phishings.*

S'agissant de la gestion de crise, sont proposées de la sensibilisation, des simulations de gestion de crise. Sont en outre proposées des formations « à 360 », puisque la cybersécurité n'est pas seulement une question technique ou technologique ; elle doit être abordée avec une approche globale et métier.

Lenning Pedron, directrice de Trust Valley souligne l'importance de la proximité qui « permet de se connaître, de se voir, d'échanger. Nous sommes à une heure les uns des autres ». Emmanuelle Simon, Program Manager de Trust Valley, met en avant l'importance d'une communauté engagée : « Les acteurs qui sont dans nos boards vont apporter un savoir-faire, une expertise, une compétence ». Mais créer une telle communauté demande du temps. « Pour monter un programme pour les PME, il nous a fallu plus d'un an et demi pour mettre tous les acteurs autour de la table et aligner les intérêts. Déjà, il y a une première étape, c'est déjà connaître l'existant, quelles sont les ressources qui sont sur mon territoire ? Lors de la deuxième étape, il faut se poser les questions suivantes : quelle direction suivre ? quels sont les besoins aujourd'hui ? quel est le niveau de maturité de l'écosystème ? sur quel secteur d'activité ? Donc, il faut vraiment faire au préalable ce travail d'analyse, puis mobiliser tous ces acteurs qui ont parfois des cultures qui sont différentes, des cultures de sécurité t différentes et à des niveaux différents ».

La Trust Valley, c'est aujourd'hui 400 partenaires (50 pour le programme PME). Les partenaires qui sont engagés dans ce programme participent à des comités de pilotage. Ils ont un mot à dire sur les orientations et apportent les retours du terrain. Emmanuelle Simon poursuit : « Les partenaires vont se mettre ensemble, se mettre à disposition des sociétés. Lors des matinées de formation, on va avoir des concurrents qui vont travailler ensemble pour répondre aux besoins des entreprises. C'est pour ça que ça a pris du temps. Je pense qu'il faut commencer à discuter ensemble au niveau local. Je pense que c'est essentiel pour les PME, pour leur apporter aussi de la lisibilité ».

EN SEM BLE

POUR UNE CYBERSÉCURITÉ COLLECTIVE ET COLLABORATIVE

Le territoire est une zone d'impact pour des prédateurs agissant souvent à distance. La cybersécurité est une des conditions de l'innovation et du développement économique.

Les cyberattaques visent toutes les entités, dès lors qu'elles sont connectées. C'est pourquoi une cybersécurité collective et collaborative, est une exigence. Elle est tributaire d'une coopération public-privé inédite. La volonté d'en faire un marqueur de l'attractivité et de la résilience du territoire est soutenue par le représentant de l'État dans le département et par les principaux organismes qui fédèrent les acteurs économiques : Chambre de commerce et d'industrie (CCI 21-71), Mouvement des entrepreneurs (MEDE71), Confédération des Petites et Moyennes Entreprise (CPME 71) sont autant de relais qui peuvent soutenir la dynamique.

SÉCURITÉ ÉCONOMIQUE : UN DÉFI COLLECTIF, UNE RÉPONSE COLLECTIVE

Dans un contexte de tensions géopolitiques croissantes, de transformations technologiques majeures et de multiplication des risques sur les données et les actifs stratégiques, le MEDEF considère que la sécurité économique s'impose comme un impératif stratégique.

Elle ne concerne plus aujourd'hui uniquement les grandes entreprises mais touche également les TPE, les PME et ETI et même les collectivités. Vol de données, demandes de rançon ou sabotage... sont autant de risques qui pèsent sur nos organisations, avec des conséquences souvent graves, parfois irréversibles.

Cette réalité peut encore sembler lointaine, complexe et coûteuse pour les entreprises, notamment les TPE et les PME. Pourtant la cybermenace et ses conséquences sont très concrètes et ce sont le plus souvent les petites entreprises, moins dotées de dispositifs de protection, qui sont le plus à risque.

La sécurité économique est devenue une clé de la compétitivité. Au-delà de sa dimension défensive, visant à protéger contre les risques émergents, elle permet aussi et surtout aux entreprises de rester compétitive et de développer de nouveaux marchés en intégrant ces nouveaux risques.

Au MEDEF, nous sommes convaincus que la sécurité économique est cruciale au quotidien. Il est important de développer des réflexes, sans paranoïa, et de prendre des actions à court, moyen et long terme pour se former, s'organiser et gérer efficacement les risques. Ainsi, nous nous employons depuis de nombreuses années à accompagner les entreprises face à des cyberattaques de plus en plus sophistiquées et de plus en plus nombreuses, menaçant de fait notre souveraineté économique devenue un enjeu collectif. Les cyberattaques exploitent les vulnérabilités sans distinction, rendant indispensable de se fédérer pour mieux se coordonner et démultiplier l'impact de nos actions en mutualisant les ressources et les expertises entre les différents acteurs. Le décloisonnement à l'échelon territorial et le renforcement des liens publics-privés sont non seulement possibles mais apparaissent aujourd'hui indispensables pour renforcer l'impact de notre réponse à cette menace.

La cybersécurité est un défi collectif qui nécessite une réponse collective. En travaillant ensemble et en partageant les informations, nous pouvons mieux nous préparer à faire face aux cybermenaces et protéger nos organisations. Il est temps de briser les silos et de construire ensemble un avenir cybersécurisé !

Fabien ROSSIGNOL
Président du MEDEF Saône-et-Loire

LA CYBERSÉCURITÉ, UN ENJEU COLLECTIF ET TERRITORIAL POUR NOS TPE PME

La cybersécurité n'est pas seulement une affaire de spécialistes, c'est un sujet de terrain qui concerne les entreprises de toutes tailles, de tous domaines et de tous territoires. Les TPE PME souvent moins armées face aux menaces sont pourtant en première ligne. Elles doivent aujourd'hui répondre aux demandes de leurs clients sur la protection des données, l'intégrité et la disponibilité de leurs systèmes d'information.

Ce que je crois en tant que Présidente de la CPME 71, c'est que l'action d'agir au niveau des territoires présente plusieurs avantages qui sont les suivants : la mutualisation des moyens, le partage d'expérience et la force du collectif ayant un ADN commun.

Notre territoire a déjà démontré sa dynamique économique et humaine a plusieurs égards, c'est pourquoi nous devons rester vigilant et solidaire afin de limiter les risques d'attaque et permettre une réaction rapide en cas d'incident.

Une cyberattaque peut paralyser non seulement une entreprise, mais aussi ralentir tout un écosystème local, fragilisant la confiance et freinant le développement. Les conséquences peuvent être lourdes et porter atteinte à l'innovation, à la réputation, engendrer des pertes de données et ainsi impacter la vie sur le territoire.

Aujourd'hui la cybersécurité est au cœur de notre compétitivité, de l'attractivité de nos TPE PME. Nos entreprises doivent garantir le respect de la confidentialité, de l'intégrité et de la disponibilité de leurs ressources afin de répondre à des obligations légales, économiques et éthiques.

Plus que jamais nous devons sensibiliser et former nos collaborateurs qui ne l'oublions pas, sont nos premiers remparts contre la cybercriminalité ; c'est pour nous, la garantie d'une activité sécurisée, d'emplois sauvegardés et de savoir-faire pérennisés.

À la CPME 71, nous croyons profondément à la force du réseau local. Il nous revient d'agir tous ensemble afin d'informer, de nous fédérer avec les acteurs locaux autour de cet enjeu prégnant pour nos entreprises. En favorisant les échanges et le partage des bonnes pratiques, en soutenant l'innovation, l'entreprenariat et la montée en compétences de nos collaborateurs, nous contribuerons au développement de notre territoire.

La transition numérique est un réel défi pour les TPE PME, mais c'est aussi une formidable opportunité de croissance et de solidarité locale. La cyber sécurité n'est donc pas seulement un bouclier, c'est un atout majeur pour bâtir des PME plus solides, capables de relever les défis numériques d'aujourd'hui et de demain.

Clarisse MAILLET
Présidente de la CPME 71

LA CYBERSÉCURITÉ, UN ENJEU COLLECTIF ET TERRITORIAL POUR L'ÉCONOMIE LOCALE

La cybersécurité n'est pas seulement une affaire d'experts informatiques : c'est une réalité quotidienne qui concerne toutes les entreprises, de la TPE familiale à la grande entreprise industrielle. Dans un contexte où 67 % des entreprises françaises ont été victimes d'une cyberattaque en 2024 (Rapport Hiscox), il est clair qu'aucun acteur n'est épargné. Nos TPE et PME, souvent moins armées, se retrouvent particulièrement exposées : en trois ans, le nombre de petites structures touchées a progressé de 50 %. Pour certaines, les conséquences sont irrémédiables : 60 % des entreprises victimes ferment dans les 18 mois (Infolegale).

Ce que nous croyons à la CCI Côte-d'Or Saône-et-Loire, c'est que la réponse à cette menace ne peut pas être individuelle. Face à des organisations criminelles coordonnées, la seule riposte possible est collective. C'est la force du territoire, la mutualisation des moyens et le partage des savoir-faire qui permettront de protéger efficacement notre tissu économique.

La coopération et la mutualisation, ce n'est pas seulement du matériel ou des logiciels mis en commun. C'est aussi et surtout :

- Échanger des informations sur les menaces et incidents
- Diffuser les bonnes pratiques à l'ensemble des entreprises
- Mettre en commun des ressources de sensibilisation et de formation
- Bâtir des dispositifs d'alerte et d'accompagnement collectifs
- Associer acteurs publics, consulaires, associations professionnelles et entreprises privées dans une même dynamique

Notre territoire a déjà démontré sa capacité à innover et à travailler ensemble. Cette même énergie doit s'exprimer face au risque cyber. Car une attaque ne paralyse pas seulement l'entreprise victime : elle fragilise tout un écosystème, met en danger l'emploi, ralentit les projets et érode la confiance.

À la CCI, nous savons que la cybersécurité est désormais au cœur de la compétitivité et de l'attractivité de nos entreprises. Protéger les données, garantir la continuité de l'activité, répondre aux attentes des clients et donneurs d'ordre, ce n'est pas seulement respecter une obligation : c'est assurer la pérennité de notre économie locale.

En tant qu'acteur public de proximité, la CCI Côte-d'Or Saône-et-Loire se positionne comme un facilitateur et un accélérateur de cette dynamique collective. Ses missions sont multiples : sensibiliser les entreprises à travers ateliers, diagnostics (MyCyber360), conférences et formations ; accompagner les dirigeants dans la mise en place de leurs premières mesures de protection ; animer le réseau territorial en favorisant les synergies entre entreprises, experts et collectivités ; orienter vers les bons interlocuteurs publics, qu'il s'agisse de l'ANSSI, de la gendarmerie ou des plateformes gouvernementales. La CCI agit ainsi comme un point d'entrée de confiance pour les dirigeants locaux, en traduisant un sujet technique en solutions pratiques, adaptées et accessibles à tous.

La transition numérique représente un défi immense pour nos entreprises, mais c'est aussi une opportunité formidable de croissance et de solidarité locale. À condition d'être sécurisée, elle peut devenir un levier de confiance, d'innovation et d'attractivité.

La cybersécurité n'est donc pas seulement un bouclier. C'est un atout stratégique pour nos entreprises et nos territoires, une clé de résilience et de développement durable, et c'est collectivement, grâce à l'action coordonnée des acteurs publics et privés et au rôle moteur de la CCI, que nous pourrons transformer ce défi en levier de confiance, d'innovation et de compétitivité pour l'avenir de notre territoire.

Philippe ROUBALLAY
Déléguée 71
CCI 21-71

ENTITÉ CONNECTÉE, PORTE D'ENTRÉE POUR LES CYBERATTAQUES

Certains pensent qu'ils n'intéressent pas les prédateurs, en raison de leur taille ou de leur raison sociale. Ils ont tort ! Chacun peut être une porte d'entrée pour des attaques en rebond. Chacun s'inscrit dans une chaîne de valeur et peut donc être le point de départ d'une opération altérant la chaîne logistique ou ayant pour objectif une entité particulièrement sensible. La responsabilité est individuelle mais aussi collective.

Bien que les relations numériques ne soient pas circonscrites au territoire de la Communauté urbaine, il est indispensable de créer un état d'esprit partagé par tous.

La cybersécurité doit être une compétence partagée par tous les acteurs des entreprises, des administrations, mais aussi par la population. Si elle dépend de normes nationales ou européennes, elle s'enracine dans le « dernier kilomètre ». C'est donc à l'échelle du territoire qu'il convient aussi d'agir, notamment en raison de l'entrée en vigueur de la directive européenne NIS2 (sécurité des réseaux et systèmes d'information.)

La directive NIS2, un changement d'échelle qui impacte les acteurs publics et privés, même les plus petits. Pierre Kirchner, directeur cybersécurité d'Equans Digital, rappelle que la transformation numérique est source de nouvelles menaces. L'informatique de gestion (IT) converge avec l'informatique de production (OT), ce qui oblige à renforcer les mesures de protection. Avec NIS2 c'est l'ensemble des systèmes d'information qui est concerné. Toute faille sur l'un peut avoir des conséquences sur l'autre. La première des actions à entreprendre est de connaître les risques. C'est nécessaire si l'on veut prévenir par une hygiène informatique, détecter les incidents et y répondre par les plans de continuité de l'activité (PCA) et les plans de reprise d'activité (PRA).

L'ANSSI et le Club de la sécurité de l'information français (Clusif) considèrent, en se référant à la période 2023-2024, qu'une cyberattaque crée un préjudice moyen de 466 000 euros pour une TPE-PME, 13 millions pour un ETI et 135 millions pour une grande entreprise. Arnaud Kopp, consultant en cybersécurité, indique que l'attaquant voit dans les entreprises et les collectivités territoriales un moyen d'obtenir un retour économique par l'exfiltration, l'exploitation des données, souvent confidentielles, par la prise de rançon. L'intelligence artificielle augmente l'efficacité des mails indésirables *(spam),* de l'hameçonnage *(phishing).*

Pour les responsables, la cybersécurité est une obligation qui est accentuée par la directive européenne NIS2. Selon Arnaud Kopp, ce texte est un moyen de « faire peur » aux attaquants qui se détourneront des entités qui sont montées en maturité dans le domaine de la cybersécurité.

LA CYBERSÉCURITÉ N'EST PLUS SEULEMENT UNE QUESTION TECHNIQUE

C'est désormais un enjeu stratégique et réglementaire pour l'ensemble des territoires. Avec l'entrée en vigueur de la directive européenne NIS2, les collectivités, établissements de santé, opérateurs industriels et entreprises locales vont devoir renforcer leurs dispositifs de sécurité et démontrer leur conformité.

Pour un territoire comme le Creusot Monceau, marqué par une forte présence industrielle et un tissu économique diversifié, l'impact est majeur. NIS2 élargit considérablement le champ des organisations concernées et impose de nouvelles obligations : gestion des risques, réponse aux incidents, gouvernance de la sécurité et traçabilité des actions. Les sanctions prévues en cas de non-conformité peuvent atteindre plusieurs millions d'euros, mais au-delà de l'aspect réglementaire, c'est bien la continuité d'activité et la confiance numérique qui sont en jeu.

Développer une stratégie de cybersécurité territoriale, c'est donc anticiper ces nouvelles exigences, mutualiser les efforts et éviter que chaque acteur ne se retrouve isolé face à la complexité des menaces et des obligations.

C'est aussi une opportunité pour le territoire :

- En protégeant l'activité économique et éviter les arrêts de production liés aux cyberattaques.
- En accompagnant les collectivités et entreprises dans la mise en conformité NIS2.
- En valorisant l'attractivité du Creusot Monceau par une résilience numérique exemplaireNotre conviction est claire : la directive NIS2 n'est pas qu'une contrainte, c'est une chance. Elle oblige à élever le niveau de sécurité et incite à bâtir une culture cyber commune sur le territoire. En travaillant collectivement, nous pouvons transformer cette exigence en levier de compétitivité et de confiance au service des citoyens et des acteurs économiques locaux.

Hakim DJELILI
Expert en cyberdéfense
Cyber Expert

La directive NIS2 impacte de très nombreuses entités publiques ou privées dites « régulées ». Les tableaux ci-dessous dressent l'inventaire des 18 secteurs d'activité concernés et présentent les seuils qui permettent de qualifier une entité au regard de la directive.

Secteurs hautement critiques

- Énergie (électricité, gaz, pétrole)
- Transports (aérien, ferroviaire, maritime)
- Secteur bancaire et marchés financiers
- Santé et infrastructures médicales
- Eau potable et eaux usées
- Infrastructure numérique et services TIC
- Administration publique

Secteurs critiques

- Services postaux et logistique
- Gestion des déchets
- Production chimique
- Industrie agroalimentaire
- Fabrication de dispositifs critiques
- Fournisseurs numériques

Seuil de classification des entités essentielles et importantes

NOMBRE D'EMPLOYÉS	CHIFFRE D'AFFAIRES MILLIONS D'EUROS	BILAN ANNUEL MILLIONS D'EUROS	SECTEURS HAUTEMENT CRITIQUES	SECTEUR D'ACTIVITÉ CRITIQUE
250 >	50 >	43 >	Entités essentielles	Entités importantes
50 > 250	10 > 50	10 > 43	Entités importantes	Entités importantes
< 50	< 10	< 10	Non concernées	Non concernées

Les collectivités territoriales ne sont pas exclues, puisque les régions, les départements, les communautés d'agglomération, les communautés de communes et les communes de plus de 30 000 habitants, leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques, sont concernées par NIS2. C'est bien évidemment le cas de la Communauté urbaine du Creusot Montceau, comme le constate Jean-Yves Lagrange, son DSI, en soulignant que l'impact pour une collectivité va dépendre de sa maturité au niveau de la cybersécurité et des ressources dont elle dispose pour se mettre en conformité. Ayant bénéficié, en 2022, du parcours cybersécurité, mis en place par l'ANSI dans le cadre du plan France Relance, la Communauté urbaine, entité essentielle, ne part pas de rien. À partir du diagnostic de son système d'information, elle a établi une série de plans d'action pour monter en maturité. Mais des questions doivent être tranchées, s'agissant de l'eau, par exemple, qui est en délégation de service public ou de l'office de tourisme dont la CUCM assure l'infogérance.

LA CYBERSÉCURITÉ N'EST PLUS UNE OPTION POUR LES TERRITOIRES

Elle conditionne désormais la continuité des services essentiels et la compétitivité des entreprises. Les organisations locales sont aujourd'hui tout aussi exposées que les grands groupes ou les administrations nationales. Les cibles à protéger sont multiples : réseaux d'eau, services sociaux, urgences, vidéosurveillance, mais aussi le tissu de PME et d'ETI qui forment l'ossature économique locale.

La directive NIS 2 marque un tournant majeur. Elle fait passer la cybersécurité d'un sujet périphérique à une obligation prioritaire. Si elle incite à l'action, elle impose aussi un défi considérable : élever le niveau de compétences des équipes IT et accroître les moyens financiers consacrés à la cybersécurité. Pour beaucoup d'acteurs locaux, tout reste à construire !

C'est pourquoi une approche ancrée dans la réalité du territoire est indispensable. Au Creusot Montceau, le secteur industriel est particulièrement exposé. Les ETI et PME doivent non seulement protéger leurs chaînes de production, de plus en plus pilotées par des technologies OT *(Operational Technology),* mais aussi répondre aux exigences croissantes de leurs clients grands groupes qui sécurisent leur *supply chain.*

Construire une stratégie de cybersécurité territoriale prend alors tout son sens, autour de trois objectifs :

— Accélérer la montée en compétences des acteurs critiques du territoire, en lien avec NIS 2

— Mutualiser les moyens pour faciliter le passage à l'action

— Faire de la cybersécurité un levier d'attractivité du territoire, au même titre que les autres atouts numériques

L'erreur serait de s'arrêter à la sensibilisation. La véritable ambition est de bâtir de réelles capacités de résilience face à la menace cyber. Le principal obstacle reste le déficit de compétences dans les organisations locales. Pour y répondre, des grands plans de formation couvrant les volets techniques (administrateurs, développeurs) mais aussi non techniques (RSSI, managers) pourraient s'envisager localement. C'est ce socle humain de professionnels capables d'opérer la cybersécurité au quotidien qui constituera la base d'une stratégie territoriale durable.

Vincent POULBÈRE
Directeur général Sysdream

À l'analyse des critères posés par la directive NIS2, Vincent Poulbère, CEO de Sysdream, estime qu'une grande partie du tissu industriel de la région du Creusot est concernée, directement ou indirectement. NIS2 est un plan de montée en capacité cyber de tout un écosystème, secteur d'activité par secteur d'activité. Clarisse Maillet, présidente de la CPME71 regrette que, selon un sondage effectué auprès des entreprises adhérentes, 83 % disent ne pas connaître la nouvelle réglementation européenne qui sera applicable sitôt la loi la résilience des infrastructures critiques et au renforcement de la cybersécurité sera promulguée. C'est dire si un effort de communication est nécessaire.

La cible de la directive NIS2 semble limitée à certains acteurs qui, par leur secteur d'activité et leur taille, sont directement impactés par les exigences de cybersécurité intégrées dans la loi française. La mise en application du texte montrera que de nombreuses entités, a priori exclues du champ de la directive, seront concernées par « capillarité », par « rebond », dès lors qu'elles entrent dans la chaîne logistique, dans la sous-traitance d'une entité régulée. Comme le souligne Vincent Poulbère, les sous-traitants vont devoir présenter une feuille de route de cyberrésilience et de cybersécurité s'ils veulent continuer à travailler avec des grands groupes. Cela a pour conséquence d'être en capacité d'offrir des garanties de sécurité sur les échanges de services, de données, de respecter les politiques et procédures de cybersécurité, imposées par les clients, et d'être prêt à signaler tout incident pouvant impacter leur activité.

Jean-Marc Autret, responsable cybersécurité en charge de la politique et de l'animation de la sécurité des systèmes d'information industriels du groupe EDF, met en exergue le *Cyberresilience Act,* règlement européen qui impose aux fournisseurs de garantir la cybersécurité des produits qu'ils livrent par l'absence de failles ou de vulnérabilités. La fragilité des objets connectés qui ne répondent pas aux normes est un sujet de préoccupation. La convergence IT-OT doit être maîtrisée. Pour filtrer les flux d'information qui montent de l'OT vers l'IT, il faut contrôler ce qui descend vers les systèmes industriels. La cybersécurité doit être une ligne de défense de la sûreté et, pour cela, il est nécessaire d'acculturer le personnel en incorporant de la cybersécurité dans les formations de sûreté. Il y a des exigences, des règles à respecter, des usages à maîtrise, des infrastructures conçues pour protéger ce qu'il y a de plus critique.

La prise de conscience, on le voit, ne se limite pas au responsable de la sécurité des systèmes d'information (RSSI) ou au directeur des systèmes d'information (DSI) ; elle est désormais partagée par les chefs d'entreprise, le COMEX. C'est dire l'importance d'une réflexion collective à laquelle chacun doit participer, ne serait-ce que parce que nul n'est à l'abri d'une crise liée au cyber.

LA CONFORMITÉ, UN TRAVAIL DE LONGUE HALEINE

La directive européenne NIS2 représente une évolution majeure en matière de cybersécurité pour les collectivités territoriales. Cette directive vise à renforcer la cybersécurité dans 18 secteurs critiques, dont plusieurs relèvent directement des compétences des collectivités : santé, eau, énergie, transports, gestion des déchets, etc.

La communauté urbaine est directement concernée du fait des politiques publiques qu'elle porte soit directement, soit par délégation. Cette directive est une opportunité pour elle de mieux sécuriser ses actifs numériques et ainsi renforcer la confiance des administrés. Elle arrive aussi à point nommé pour sécuriser le développement du futur « Smart Territoire », source d'un volume de données important et indispensable pour favoriser son attractivité.

NIS 2 donne un cadre et des obligations pour tous les acteurs du numériques. Parmi ces obligations, l'une concerne la gestion des risques de la chaine d'approvisionnement. Elle implique de s'assurer que l'ensemble des acteurs en relation avec les actifs numériques délivrés par la communauté disposent eux aussi de mesures de sécurité appropriées en fonction de leur niveau de risque.

Ainsi le travail de mise en conformité engagé par la communauté aura des impacts sur l'ensemble des acteurs en lien avec ses services numériques notamment les prestataires, les éditeurs de logiciels mas aussi les communes, l'office du tourisme, les délégataires et toutes les autres entités utilisatrices.

Du fait de l'interdépendance des différents services numériques, il est primordial que chaque acteur concerné prenne conscience qu'il fait partie d'un ensemble et que s'il n'est pas en conformité alors il fragilise le système global.

Cette mise en conformité sera un travail de longue haleine et elle ne pourra pas se faire sans un travail collaboratif avec l'ensemble des acteurs internes et externes. Enfin, elle ne devra pas se contenter d'initialiser une démarche mais il faudra qu'elle soit aussi efficace durant tout le cycle de vie de chaque service numérique.

Jean-Yves LAGRANGE
DSI de la Communauté urbaine du Creusot Montceau

S'ENTRAIDER EN CAS DE CRISE LIÉE AU CYBER

Il n'y a pas de crise cyber mais des crises liées au cyber, soit en raison d'une erreur humaine, soit à la suite de l'action de prédateurs. Comme le souligne Guillaume Poupard, ancien directeur général de l'ANSSI, « la question n'est pas de savoir si je vais être attaqué, mais quand ? ». Pierre Kirchner énonce les interrogations qui viennent à l'esprit au sein de l'entité attaquée : « qui j'appelle ? quelles sont mes obligations légales (signalement à l'ANSSI, à la CNIL pour les données à caractère personnel), qui prend des décisions, comment communiquer ? ».

Clarisse Maillet le reconnait : quand il y a une cyberattaque, on ne sait pas vers qui se tourner. On ne sait pas qui on doit appeler. Que devons-nous faire ? Cette interrogation est révélatrice d'une insuffisance de communication. Jérôme Notin, directeur général de Cybermalveillance, Véronique Brunet, déléguée à la sécurité numérique pour la région Bourgogne-Franche-Comté (ANSSI), Sébastien Morey, responsable du CSIRT Bourgogne-Franche-Comté, et le colonel David Flotat, chef de la division proximité numérique de la gendarmerie nationale, apportent lors du Forum une clarification.

La difficulté ne se pose pas pour les opérateurs d'importance vitale (OIV), ceux dont les activités sont indispensables au fonctionnement de l'économie ou de la société ainsi qu'à la défense ou à la sécurité de la Nation. Depuis la loi de programmation militaire (LPM 2014-2019), au moins, ils sont soumis à des obligations particulières, renforcées par la directive européenne REC (résilience des entités critiques), transposée dans le droit français.

Ils connaissent ces obligations et sont en contact avec l'ANSSI à laquelle ils doivent rendre compte dans les 24 heures en cas d'incident. Dès la loi de transposition votée, le nombre d'interlocuteurs de l'ANSSI va passer de 500 à 15.000, car, comme le précise Véronique Brunet, les entités essentielles et les entités importantes, définies par la directive NIS2, sont aussi des organismes régulés qui ont pour référent l'Agence nationale pour la sécurité des systèmes. Ils ont également l'obligation de signaler dans les 24h les incidents qui les affectent. Pour tous les organismes précités, le CERT-FR (Computer Emergency Response Team) est un interlocuteur qui est disponible 7j/7, 24h/24. Il répond notamment au numéro 3218.

UN DIAGNOSTIC POUR FAIRE FACE À LA CRISE CYBER

Pour faire de la gestion de crise, il faut savoir faire un diagnostic dans l'objectif d'être en mesure de prendre les bonnes décisions rapidement. Aujourd'hui on constate des combinaisons dans la façon d'attaquer les systèmes d'information. On peut leurrer un exploitant en lui faisant croire que les choses se passent à tel endroit alors qu'en fait l'attaque elle est bien ailleurs. Pour faire un diagnostic, il faut connaître son patrimoine numérique. J'arrive à comptabiliser environ 10 millions de matériels numériques au sein du groupe EDF. Si les entités ne connaissent pas les matériels qu'elles exploitent et ne savent pas comment ils sont configurés, utilisés et par qui, c'est très compliqué de faire un diagnostic quand il y a un problème de cybersécurité qui peut se répandre partout. C'est un sujet de préoccupation majeure que les collectivités vont devoir regarder dans leurs différents cas d'usage ou dans leurs différentes institutions. Mais en tout cas, il y a lieu, je pense, de s'inspirer déjà de ce qui se fait de meilleur dans les environnements critiques comme EDF, notamment autour de la sûreté nucléaire.

Carmen MUNOZ-DORMOY
Directrice EDF action régionale

AGIR AU PROFIT DES ENTITÉS NON RÉGULÉES

Quelle est la situation de toutes les autres entreprises et administrations qui se sentent parfois oubliées des politiques de cybersécurité ? Jérôme Notin, apporte une réponse. Le Groupement d'Intérêt Public Action contre la Cybermalveillance (GIP ACYMA) est issu de la Stratégie numérique du Gouvernement présentée le 18 juin 2015 et dont les objectifs ont été ensuite détaillés dans la Stratégie nationale pour la sécurité du numérique publiée le 16 octobre 2015. Il a été créé spécifiquement pour mettre en place un dispositif en capacité d'accompagner les particuliers, les collectivités et les entreprises non régulées (hors Opérateurs d'Importance Vitale, entités essentielles et entités importantes). Si l'on considère que 0,5 % des entreprises et des collectivités (certes les plus sensibles) seront concernées par NIS 2, le nombre de ressortissants directs de Cybermalveillance est très élevé.

L'ouverture de la plateforme Cybermalveillance.gouv.fr, en octobre 2017, offre un dispositif national de sensibilisation, prévention et d'assistance aux victimes d'actes de cybermalveillance.

Cybermalveillance.gouv.fr propose aux demandeurs une mise en relation avec des prestataires en sécurité informatique situés sur l'ensemble du territoire. Ce sont 1200 prestataires référencés et 200 prestataires labellisés. Les prestataires labellisés constituent un début de réponse à une partie des problèmes sur la partie relative à la sécurisation et l'accompagnement des collectivités, des très petites, petites et moyennes entreprises (TPE-PME) dans les territoires. En 2024, la plateforme cyber-malveillance.gouv.fr a accueilli 5,4 millions d'utilisateurs, contre 3,7 millions en 2023. Pourtant, Jérôme Notin regrette qu'il y ait encore trop de collectivités, d'entreprises, ou de particuliers qui n'aient pas encore compris que l'utilisation d'un outil numérique expose de facto à un risque.

LE 17 CYBER, POINT D'ENTRÉE

Depuis le 17 décembre 2024, le ministère de l'Intérieur et Cybermalveillances ont lancé 17Cyber.gouv.fr, service public d'assistance en ligne destiné aux particuliers, entreprises, associations et collectivités victimes d'infractions numériques. Il permet une mise en relation avec un policier ou un gendarme pour assister les victimes en leur donnant des conseils de première urgence et en leur permettant d'engager les formalités judiciaires nécessaires. Depuis sa mise en service, le nombre de parcours d'assistance a doublé.

La manière qu'on a de rendre le service d'assistance auprès des publics cibles a évolué, puisque, initialement, le site accueillait les victimes, posait différentes questions à travers un questionnaire fermé : êtes-vous en particulier une entreprise, une collectivité ? le problème concerne un poste de travail, un site web, des serveurs ? En quelques questions la menace était qualifiée.

Depuis le 17 décembre dernier, la victime a, en outre, la possibilité d'échanger 24 heures sur 24, 7 jours sur 7, avec un policier et un gendarme, sur l'aide à la judiciarisation. Il est fondamental que les victimes puissent déposer plainte pour permettre d'de identifier les auteurs, faire cesser l'infraction. La puissance publique a ainsi connaissance de l'impact de ces faits de cybermalveillance, puisqu'une cybermalveillance, c'est une cybercriminalité qui n'est pas encore judiciarisée. Le général Husson, chef du commandement du ministère de l'Intérieur dans le cyberespace 'COMCYBER-MI) considère que le 17Cyber doit constituer le point d'entrée, lisible pour tous.

Sébastien Morey est responsable du CSIRT (Computer Security Incident Response Team) de Bourgogne-Franche-Comté. Les CSIRT territoriaux ont été créés depuis 2021 dans le cadre du France Relance. Il y en a 13 aujourd'hui en Métropole qui ont pour mission de renforcer le niveau de résilience cyber au plus proche de leurs territoires et de favoriser la mise en relation entre les prestataires et les utilisateurs de cybersécurité. Ils ont un vrai rôle de relais à la fois auprès du secteur privé mais aussi auprès des partenaires étatiques. Notre cercle de bénéficiaires — dit-il — est plus restreint : ce sont les entreprises, les collectivités et les associations de la région Bourgogne-Franche-Comté. Sébastien Morey précise que son centre régional de réponse aux incidents sera intégré, à l'automne 2025, dans le dispositif 17 Cyber. La plateforme ne mettra plus en relation la victime avec un prestataire, mais elle l'orientera vers le CSIRT qui est proche. Le CSIRT Bourgogne Franche Comté n'est pas qu'un centre de réponse à incidents. Il peut alerter lorsqu'il découvre des vulnérabilités sur des sites Internet de collectivités, d'entreprises. Il contribue à la sensibilisation en participant à l'animation de la filière cyber. Le centre peut être joint directement par téléphone et, lorsqu'on appelle directement vers le CERT-FR (ANSSI), un serveur local interactif renvoie vers le CSIRT régional. Quel que soit le chemin d'accès, personne ne pourra rester sans réponse.

Cet échange met en évidence que le dispositif d'accompagnement est encore en construction. Il ne doit pas seulement être un « placage » venant d'en haut qui est certes nécessaire mais non suffisant. Les acteurs du territoire doivent aussi tisser la trame.

GENDARMES ET POLICIERS AU CONTACT

Sur le terrain, l'action des services de police et des unités de gendarmerie s'intensifie. La stratégie ministérielle de lutte contre la cybercriminalité, présentée en avant-première par le ministre de l'intérieur lors du Forum INCYBER de Lille (avril 2025) : « La réponse opérationnelle du Ministère pour lutter contre la cybercriminalité débute par le développement de contacts avec les acteurs, plateformes du numérique et grand public. Il s'agit d'abord d'informer la population, victime potentielle, des outils existants et mis à sa disposition par l'État pour l'aider dans la connaissance ou le traitement des difficultés ou infractions cyber auxquelles elle peut être confrontée. Il s'agit ensuite de mettre en place des collaborations et des modes d'action innovants, facilitant le contact avec les usagers de plateformes numériques d'intérêt ».

Si, comme le souligne le colonel Flotat, la mission principale est le traitement judiciaire des infractions commises, le travail en amont, avant et pendant la crise, s'opère au profit des entreprises, des collectivités territoriales et des particuliers. La gendarmerie nationale a la responsabilité de la sécurité sur 95 % du territoire, là où vit plus de 50 % de la population et où se concentrent la plupart des TPE et PME. L'action de prévention et menée par un réseau de militaires de la gendarmerie formés, spécialisés, en capacité d'aider, d'accompagner. Cela se matérialise notamment par des diagnostics cyber. Le ministère de l'Intérieur contribue au dispositif MonAideCyber, développé par l'ANSSI et qui crée une communauté de confiance composée d'« aidants cyber » issus de la sphère publique ou sont membres d'associations œuvrant pour un numérique de confiance. Les gendarme, comme les policiers, sont des aidants en capacité de venir dans les entreprises, dans les collectivités pour réaliser gratuitement un petit diagnostic. Il ne s'agit pas d'un audit ; toutefois, la démarche permet en quelques heures d'avoir un état de la menace ou d'en prendre conscience. Ces diagnostics sont révélateurs des carences qui, heureusement diminue avec une prise de conscience collective de la menace. Le citoyen est, bien sûr, au cœur de l'action, car c'est aussi un salarié, un cadre, un chef d'entreprise, un élu.

UN DÉVELOPPEMENT DE LA CYBERCRIMINALITÉ À UN RYTHME INDUSTRIEL

« Les criminels ont désormais pleinement investi le monde numérique. [...] La criminalité s'y développe à un rythme industriel ». Ce constat, dressé dans le Rapport annuel sur la cybercriminalité (2025) du ministère de l'Intérieur, dénote une « métamorphose de la criminalité ».

Réfléchir à sa cybersécurité, au sens de « système d'information qui résiste aux cyberattaques et pannes accidentelles survenant dans le cyberespace », demeure dès lors essentiel. L'infrastructure, en particulier dans sa dimension matérielle, est la première composante dont dépend un système pour revendiquer un niveau satisfaisant de sécurité, et ce à travers des *datacenters*, des terminaux mais aussi des câbles conçus pour résister aux accidents ou attaques volontaires. En parallèle, le recours à des solutions informatiques fiables, et de préférence souveraines, demeure un préalable indispensable à la protection des données (bancaires, de santé, etc.). Enfin, une organisation doit préparer sa résilience par un effort permanent de formation et d'informa-

tion des personnels pour diffuser les bonnes pratiques en matière d'hygiène numérique.

En outre, face à une « industrialisation » de la cybercriminalité, l'État constitue un acteur résolument engagé. Mais une action unilatérale, celle des services de l'État, ne saurait constituer l'unique rempart. Une coopération entre les forces régaliennes, et leurs éléments déconcentrés, les collectivités territoriales, les TPE et PME, les hôpitaux, avec l'implication des particuliers, s'impose en effet, notamment dans les territoires où le besoin de proximité reste fort.

Elle s'exprime par exemple à travers le MOOC Sency-Crise, créé par le COMCYBER-MI et cybermalveillance.gouv.fr, qui vise à accompagner les petites et moyennes entreprises, associations et collectivités à mettre en place ou améliorer leur dispositif de gestion de crise cyber. MonAideCyber, outil de diagnostic permettant à une organisation d'évaluer sa maturité cyber, et le 17 cyber, outil d'assistance en ligne pour toute victime de cybermalveillance, participent également de cette volonté d'accompagnement.

En parallèle, les collectivités locales, notamment les régions et les départements, conduisent des opérations de sensibilisation cyber à destination de leurs administrés. La mise en place de CIRT régionaux densifie le maillage d'aide aux collectivités et TPE / PME dans leur réponse aux attaques cyber. Les campagnes de prévention dans les territoires, à l'image de l'opération interministérielle CACTUS dans les établissements scolaires, illustrent enfin la nécessité de faire converger les forces dans la lutte contre les cybermenaces.

Chaque citoyen, chaque organisation, publique ou privée, de l'échelon national jusque dans les territoires, a donc un rôle à jouer dans le développement d'une culture cyber, où la coopération demeure primordiale.

Général de division
Christophe HUSSON
COMCYBER-MI

L'offre de conseil, on le constate, est à plusieurs « étages » : national, régional, local. Elle s'inscrit dans une verticale qui vient « d'en haut » et prend racine à l'échelon territorial avec la communauté des aidants, à laquelle est associé réseau local des policiers et gendarmes. Cette dorsale doit être complétée par une communauté des gens du cyber, manifestation d'une volonté de renforcer collectivement la cyberrésilience du territoire. Cet engagement, plus « horizontal », pourrait être précisé par une charte de cybersolidarité territoriale.

VERS UNE CHARTE DE CYBERSOLIDARITÉ TERRITORIALE ?

Le Forum INCYBER des territoires n'est pas une fin mais le début d'une démarche collective qui a pour ambition de renforcer la cyberrésilience du territoire. Trust Valley, en Suisse, invitée le 22 mai au Creusot, est un exemple dont on peut s'inspirer, mais il en existe d'autres. Par exemple, la métropole Nantaise a rassemblé, en mars 2025, 24 organisations publiques et privées autour d'une Charte de solidarité territoriale de cybersécurité. Son préambule est ainsi rédigé : « La présente charte a pour objectif de partager des connaissances et de promouvoir la solidarité entre les entreprises, les établissements publics, les organisations et les collectivités du territoire en matière de cybersécurité. Elle vise à établir un cadre d'échanges d'information et de coopération de proximité et de partage de ressources face aux menaces numériques qui pourraient affecter la sécurité des systèmes d'information de chaque entité engagée. Cette démarche collective vise à renforcer la résilience numérique de ce cercle territorial de coopération et de solidarité et ainsi contribuer à la résilience économique du territoire ». Ces quelques lignes résument la démarche qu'il convient d'entreprendre. En Normandie, une Charte a également été instituée : elle vise à « diffuser les bonnes pratiques en cybersécurité auprès de tous les acteurs normands pour élever le niveau global de cybersécurité en Normandie dans l'objectif de réduire les risques numériques des entreprises, des structures de développement ou des collectivités territoriales, tant au niveau des prestataires que des usagers, et à identifier les spécialistes du domaine à même d'accompagner, d'anticiper, de résoudre ou de gérer les crises ». Une charte existe également dans le Morbihan, mais elle est destinée aux collectivités territoriales. Ses objectifs sont les suivants :

- Former les élus et les agents territoriaux aux enjeux cyber
- Proposer un diagnostic cyber pour toutes les collectivités du Morbihan
- Accompagner les collectivités pour assurer leur protection en matière cyber
- Encourager une offre de conservation sécurisée des données
- Permettre la diffusion d'une culture de gestion de crise cyber

Il est bien évidemment exclu de reproduire in extenso des documents existants, car une Charte doit être conçue collectivement par les acteurs locaux. Il convient donc, dans un premier temps, de recueillir l'assentiment des acteurs publics et privés prêts à s'engager dans sa conception, car plus qu'un texte, c'est un engagement collectif pour faire de la Communauté urbaine du Creusot Montceau une terre de résilience numérique. La Charte pourrait avoir pour objectifs de :

- Renforcer la coopération interinstitutionnelle face aux cybermenaces
- Déployer une culture de cybersécurité partagée
- Assurer la protection des systèmes critiques du territoire
- Sensibiliser tous les usagers du numérique, professionnels et particuliers
- Mettre en place des pratiques responsables et sécurisées
- Partager les alertes de cybersécurité avec le réseau territorial
- Participer à des actions de formation et de sensibilisation
- Diffuser une culture de gestion de crise cyber
- Coopérer dans la réponse aux incidents numériques

S'agissant de la méthode, il conviendrait de désigner un référent cybersécurité au sein de chaque entité partenaire, puis de constituer un groupe de travail chargé d'identifier les besoins. Cette Charte devra rappeler le rôle des acteurs nationaux (ANSSI, Cybermalveillance, 17 Cyber) et régionaux (CSIRT-Bourgogne Franche Comté), dont il convient de respecter les missions et prérogatives.

Cette réflexion collective doit être le prélude à une mutualisation de capacités, chaque fois que cela est possible, notamment pour les petites entreprises ou collectivités territoriales qui n'ont pas les moyens d'agir seules. Elle doit aussi aider l'ensemble des acteurs à se préparer à la gestion d'une crise cyber.

MUTUALISER, QUAND L'UNION FAIT LA FORCE

Hakim Djelili, expert cyberdéfense chez Cyber-expert a créé une forme de mutualisation pour accompagner des collectivités territoriales, des PME, des ETI, sur le bassin Rhône-Alpes. Pour mieux défendre ces entités il travaille sur des offres, par exemple sur les coûts des licences des antivirus, ce qui peut être considéré comme marginal mais qui se montre efficace. Mais aujourd'hui, pour une petite PME, investir quelques euros par actif dans sa cybersécurisation, c'est un enjeu. Il faut donc l'accompagner et lui montrer qu'il existe des dispositifs de financement mis en place par l'État, notamment par la BPI avec des offres d'audit cyber. L'État va prendre jusqu'à 70 % à hauteur de 80 000 euros des projets de sécurisation. Pour les petits, créer un SOC (centre de cybersécurité) mutualisé, cela représente entre 10 et 20 euros par actif. Si l'on possède 100 actifs, le coût est de 2 000 euros. Il est intéressant de comparer avec le prix d'une journée d'expert cyber qui se situe entre 500 et 1000 euros. Une solution mutualisée permet de couvrir la plupart des risques avec un bon SOC 24-24 et une solution et des antivirus de nouvelle génération.

La mutualisation peut porter sur d'autres domaines, notamment en ce qui concerne la formation, lorsque la CPME71 crée avec le CNAM une offre pour ses adhérents. Elle peut notamment partager des expériences, aider tous les acteurs, quelle que soit leur taille, à mieux se préparer à la crise cyber, à monter en compétence.

LA CYBERSÉCURITÉ TERRITORIALE PARTAGÉE : UN ENJEU COLLECTIF

La transition numérique des territoires s'accélère, rendant la question de la cybersécurité plus cruciale que jamais. Pour les collectivités, une cyberattaque n'est pas seulement un incident technique : elle peut paralyser des services publics essentiels, compromettre des données sensibles, désorganiser les acteurs économiques locaux voire entamer la confiance des citoyens. Lorsqu'un territoire est attaqué, ce sont ses capacités à fonctionner, coopérer et protéger ses habitants qui vacillent. Face à ces menaces croissantes, la cybersécurité ne peut plus être l'affaire des seuls DSI ou élu(e)s. Elle doit devenir une responsabilité partagée à l'échelle du territoire. Cela implique d'associer les collectivités, les entreprises, les acteurs du numérique, mais aussi les citoyens à une gouvernance collective, capable d'anticiper, de réagir et de reconstruire. La Communauté Urbaine Creusot Monceau dispose d'un écosystème solide : tissu industriel dense, institutions publiques engagées, partenaires privés. C'est cette diversité d'acteurs qu'il faut mobiliser pour construire une véritable résilience numérique. En travaillant main dans la main, le territoire peut se doter d'une stratégie cohérente, fondée sur la confiance, la transparence et l'ancrage local des solutions numériques. Chez Interstis, éditeur de la suite collaborative Hexagone, nous défendons cette approche territoriale. Une cybersécurité efficace repose sur des outils conçus pour les usages publics, hébergés en France, maîtrisés et fiables. Investir dans la cybersécurité, ce n'est pas seulement se protéger : c'est préparer le territoire à relever les défis numériques de demain, ensemble.

Nicolas HUEZ
CEO Interstis

MONTER EN COMPÉTENCE

La population, acculturée, est mieux à même de répondre aux exigences des emplois du futur. Le Forum est certes destiné à un public « cible », les décideurs publics et privés, mais il a aussi pour vocation d'être le fer de lance d'un mouvement plus large, plus englobant. Monter en compétence, c'est informer et, mieux encore, former. Le Forum INCYBER doit entraîner dans son sillage des initiatives locales qui permettent de diffuser une culture de cybersécurité, ciment de la résilience du territoire.

L'industrie 4.0, le déploiement très rapide de l'internet des objets appellent des comportements vertueux, le partage d'une même « hygiène informatique » qui, selon l'ANSSI, permet d'éviter près de 85 % des incidents ou attaques. Le développement de l'intelligence artificielle est un atout pour les défenseurs, mais aussi une opportunité pour les prédateurs qui peuvent, sans réelle compétence, utiliser des outils qui permettent d'automatiser, d'accentuer les cyberattaques.

Dans 80 % des attaques, c'est l'humain qui est en cause, souligne Nicolas Huez, co-fondateur et CTO d'Interstis, entreprise qui est née, il y a 10 ans, au Creusot. Selon lui, la formation des collaborateurs est essentielle. Cela ne concerne pas seulement l'administrateur système et réseau qui gère les réseaux, mais c'est l'ensemble des collaborateurs. Le chef d'entreprise, le responsable de l'administration, si lui-même n'est pas sensibilisé, l'ensemble de ses collaborateurs ne le seront pas.

Clarisse Maillet, présidente de la CPME71, évoque une enquête effectuée auprès des adhérents. Une entreprise sur deux n'a pas de service informatique en son sein. Donc, elle sous-traite. L'informatique, pour elle, c'est loin. Seulement 33 % des entreprises sensibilisent leurs collaborateurs.

La directive NIS2 n'est pas connue par 83 % d'entre elles. La présidente reconnait qu'il y beaucoup d'actions de sensibilisation à accomplir à l'échelon de TPE et des PME.

Le chantier est vaste ! Il dépasse le champ de la cybersécurité pour épouser celui du numérique et de l'intelligence artificielle. La transformation numérique s'accélère et impacte les modes de vie, les rapports aux services, les métiers. Une ressource humaine en phase avec les mutations en cours et à venir est une condition de l'attractivité du territoire et de l'ajustement des compétences aux emplois du futurs.

L'offre de formation existe déjà au Creusot. L'IUT du Creusot (Université de Bourgogne Europe) dispense notamment un Mastère Expert du Design Numérique, une Licence Professionnelle Ingénierie Numérique en Conception et Fabrication, un bachelor Génie électrique et informatique industrielle. Polytech forme des ingénieurs en Robotique et Instrumentation / Cobotique.

Le besoin en formation devrait croître, ne serait-ce qu'en raison du nombre d'entreprises qui s'implantent ou envisagent de le faire sur le territoire de la Communauté urbaine. Parmi les offres à venir figure celle de SysDream, fournisseur de services spécialisé en cybersécurité, filiale du groupe de technologies Hub One qui fait partie du groupe ADP (Aéroport de Paris). Vincent Poulbère, directeur général de cette entreprise, a annoncé lors du Forume INCYBER son intention de créer un Centre de Formation Cyber du Territoire au Creusot s'adressant aux professionnels de l'IT du bassin d'emploi (emplois ciblés : responsables informatiques, DSI, RSSI, administrateurs réseau, développeurs, experts IT, experts sécurité…). Il faut, selon lui, former des personnels qui ne sont pas nécessairement spécialisés en cybersécurité mais qui font du développement logiciel, qui configurent les serveurs, les réseaux et sont donc les premiers bastions de protection des organisations.

IA & TERRITOIRES

Il n'est pas possible d'évoquer la cybersécurité sans porter un regard sur l'intelligence artificielle. Celle-ci connaît un développement accéléré depuis la mise en service de ChatGPT. L'IA générative précède l'IA agentique, capable d'effectuer des actions multiples. ChatGPT5 est sans doute le prélude à une intelligence artificielle générale, égale, voire supérieure, à celle de l'humain.

L'IA renforce les capacités de lutte contre la cybercriminalité en même temps qu'elle permet aux cyberattaquants d'améliorer l'efficacité de leur action sans avoir besoin de connaissances approfondies en programmation. L'IA offre un « kit sur étagère » qui facilite l'hammeçonnage, l'usurpation d'identité, la détection des chemins d'attaque. La cybersécurité d'un territoire ne peut être conçue sans une appropriation de l'IA, sans qu'il soit nécessaire d'être un expert.

LA CYBERSÉCURITÉ RENFORCÉE PAR L'IA

Les équipes en charge de la cybersécurité sont confrontées à plusieurs évolutions : l'augmentation exponentielle des systèmes connectés (notamment du fait de l'internet des objets) au sein d'infrastructures numériques de plus en plus complexes, l'explosion du volume de données, l'industrialisation des cyberattaques.

L'intelligence artificielle facilite le travail des défenseurs, car elle permet de traiter un volume considérable de données, libérant ainsi les équipes d'une surcharge informationnelle. Elle est opérationnelle, sans rupture dans le temps et avec la même intensité, évitant ainsi les effets dus à l'alternat des équipes et à la baisse d'attention inhérente à la nature humaine. Elle ne remplace pas l'humain, mais elle permet d'accomplir des actions habituellement chronophages ou répétitives. Détecter et répondre aux nouvelles menaces, comme les menaces persistantes avancées requiert l'anticipation et l'analyse du comportement des utilisateurs. C'est notamment le rôle de l'*Endpoint Detection & Response* (EDR), outil qui permet de détecter, d'investiguer et de remédier aux attaques plus rapidement dès les premiers signes.

La détection des incidents bénéficie des apports de l'intelligence artificielle qui, grâce à l'apprentissage automatique *(machine learning),* intègre de manière itérative les événements vécus et ajuste ainsi sa capacité de veille au regard de l'évolution des menaces. L'IA contrôle en temps réel les connexions des utilisateurs, leur localisation, les adresses *Internet Protocol* (IP) et s'inscrit dans une démarche de confiance vis-à-vis des applications. Les analystes peuvent prendre le temps de réaliser un Threat Hunting, recherche proactive des cybermenaces qui sont présentes dans un réseau mais n'ont pas encore été détectées. L'IA permet le développement de la « cybersécurité cognitive », c'est à dire l'agrégation et le traitement de données non structurées (texte, images, vidéos, écrits des experts, réseaux sociaux, etc.) et structurées (logs de connexion par exemple) dans le but d'assister les équipes de sécurité dans la prise de décisions en temps réel. Ainsi les situations anormales peuvent être identifiées et déclencher l'alerte. Cela ne remplace pas l'intervention des opérateurs qui ont notamment pour mission de contextualiser, de lever le doute en cas de faux positif.

Le traitement automatique du langage naturel *(Natural Language Processing (NLP)),* lié à l'IA générative, simplifie considérablement la relation avec la machine. L'IA donne aux acteurs de la cybersécurité la liberté de porter leur attention et leurs efforts là où ils sont plus efficaces que la machine. Ses apports sont multiples : elle peut détecter des comptes compromis ou des logiciels malveillants sur un système protégé.

L'IA offre un dispositif efficace dans la lutte anti-spam, les mails douteux étant souvent la première étape d'une cyberattaque. Elle facilite l'analyse comportementale par la connaissance des habitudes des utilisateurs et le repérage par des algorithmes des actions inhabituelles, grâce aux technologies UBA ou UEBA *(User Behavior Analytic et User & Entity Behavior Analytic).* Ainsi peuvent être identifiés les réseaux d'ordinateurs « zombies » en les distinguant des requêtes provenant des humains. L'intelligence artificielle appliquée à la cybersécurité permet d'identifier les vulnérabilités, de déceler une attaque en cours, avant que les objectifs des prédateurs, comme l'exfiltration des données, ne soient atteints. Les centres opérationnels de sécurité (SOC) qui utilisent l'IA voient leurs capacités singulièrement augmentées, notamment en termes d'investigation et de remédiation. L'IA leur permet d'accélérer et de rendre plus efficace la détection et la réponse aux cyberattaques, réduisant ainsi les dommages que les attaquants peuvent causer à l'organisation.

Partenaire, l'IA peut aussi être adversaire de la cybersécurité, dès lors qu'elle offre aussi aux cyberattaquants des possibilités inédites.

LA CYBERSÉCURITÉ À L'ÉPREUVE DE L'IA

Le duel entre le canon et la cuirasse, entre le défenseur et l'attaquant est bien illustré par le développement de l'IA. Nous sommes dans une dialectique entre « voleurs et policiers », où les voleurs, potentiellement, ont peut-être un « risque d'avance ». Parce que les IA sont accessibles, les prédateurs peuvent s'en servir à des fins mal intentionnées et les plus ambitieux d'entre eux peuvent créer leur propre modèle. La démocratisation de l'IA permet à un spectre plus large d'individus de tenter une carrière cybercriminelle. Au final, les délinquants ne sont pas plus intelligents qu'avant mais ils sont beaucoup plus efficaces qu'avant dans le volume et la pertinence de leurs attaques. L'IA introduit dans la cybercriminalité la notion de productivité. Certains ont entraîné leurs équipes à être beaucoup plus performantes, à être beaucoup plus pertinentes, plus rapidement, et surtout à moindre coût. On leur a appris à être productifs. Un exploit, une vulnérabilité coûte très cher à trouver. Il faut donc rentabiliser l'investissement quand les groupes criminels en acquièrent. Grâce à l'IA, les prédateurs ne seront pas plus performants qu'avant en termes de qualité d'attaque ; ils vont être plus efficaces et surtout opérer à une échelle qui est sans commune mesure. Témoin de l'usage de l'IA par les cybercriminels, le code pénal a été récemment modifié par la loi Sécurité et résilience de l'espace numérique (SREN). Son article 15 modifie l'article 226-8 du code pénal en sanctionnant l'hypertrucage *(deepfake),* technique ayant recours à l'intelligence artificielle permettant de réaliser des images, des paroles ou vidéos concernant une personne qui n'a pas donné son consentement, dès lors que l'utilisation d'algorithmes n'est pas expressément mentionnée. Jérôme Clauzade, de Crowdsec, déclarait lors de l'Agora du Forum INCYBER (FIC), en mars 2024 : « Il y a une dernière étape, peut-être inquiétante pour le reste du monde, lorsque les IA vont être capables de concevoir des choses auxquelles on n'avait pas encore pensé. Ce n'est pas le cas en ce moment, car les IA sont des robots. Ce sont des robots stupides qui reproduisent juste plus vite ce qu'on sait faire, en tout cas en termes de cybersécurité. Nous n'apprenons rien d'une IA. Nous allons juste plus vite à moindre coût. Plus précisément, le coût est moindre pour les prédateurs. Plus inquiétant est ce qui va arriver avec la prochaine génération d'IA qui va leur permettre de concevoir de nouvelles techniques d'attaque en utilisant la capacité d'attaque par « force brute » massive des IA et les combiner avec leur propre capacité d'ingénierie sociale, pour créer des faux profits LinkedIn, se faire passer pour des faux collaborateurs, obtenir des informations qui vont rendre les attaques encore plus pertinentes » .

Cette inquiétude est renforcée par une réglementation asymétrique : certains pays n'adoptent pas la même approche que les pays démocratiques ; ils développent intensivement l'intelligence artificielle sans éthique pour une stratégie de déstabilisation et de confrontation. Ainsi, il est crucial de prendre en compte tous les développements en matière d'intelligence artificielle, actuels et futurs. Les meilleures recherches et les développements les plus avancés se trouvent parfois dans le mauvais camp. La cybercriminalité est devenue un secteur très lucratif, générant des revenus bien supérieurs à ceux des organisations criminelles traditionnelles. Les cybercriminels cherchent constamment à accroître leurs gains. Par conséquent, il est impératif de contrer ces comportements malveillants en développant des technologies qui nous permettent de comprendre et d'anticiper les menaces potentielles. Ces acteurs malintentionnés continueront d'investir massivement sans se soucier de notre législation.

Si nous ne prenons pas le dessus, d'autres le feront, et nous ne serons pas prêts à affronter les défis posés par leur maîtrise de ces technologies. Il est donc essentiel d'être extrêmement vigilants et attentifs. Le besoin de cybersécurité est une réalité pressante. Nous devons intensifier nos investissements dans ces technologies car nos adversaires le feront sans considération pour les lois ou les responsabilités. Assurément, il est crucial de réglementer l'utilisation de l'IA et d'insister sur l'importance de l'éthique dans son déploiement. Il est également vital d'accroître la coopération internationale, non seulement pour l'échange d'informations mais aussi pour la recherche, car nous ne disposons pas des mêmes ressources que nos adversaires.

L'IA AU SERVICE DES TERRITOIRES

Le territoire est un espace pertinent pour développer une cybersécurité qui bénéficie des apports de l'IA et contre ses effets négatifs. Mais, comme l'a exprimé Evelyne Couillerot, l'IA est aussi un moteur pour le développement économique au sein d'un « Smart territoire ».

Nicolas Berthaut, directeur général de l'Agence régionale du numérique et de l'intelligence artificielle, estime, en effet, que la révolution de l'IA un caractère exponentiel posant un certain nombre de questions qui ne relèvent pas seulement du domaine de la cybersécurité. Son Agence, opérateur public, opère au profit de 1 850 adhérents dans la région Bourgogne-Franche-Comté. Il y a encore, selon lui un public indifférent, voire réfractaire. Mais il y aussi des personnes qui s'engagent, comme en témoignent les 22 000 inscrits au MOOC que l'agence a conçu pour le CNFPT.

L'IA concerne tout le monde, ne serait-ce qu'en raison de son impact sur l'emploi.

David Fofi, directeur du département robotique (Polytech) au centre Condorcet du Creusot évoque les conséquences de la démocratisation de l'IA : « cela pose la question des nouvelles compétences à introduire dans les formations. On sait que 60 % ou 70 % des métiers seront impactés par l'IA dans les 5 ans à venir. Sur 100 métiers impactés par l'IA, il y en aura 90 pour lesquels une connaissance technique approfondie de l'IA sera inutile. Donc on utilisera l'IA sans connaître la technique. En revanche, il faut avoir une pensée suffisamment analytique, du recul, une culture métier assez grande pour pouvoir juger, amender et contredire l'IA. 10 % environ des métiers demanderont des compétences techniques, Il y aura peut-être 1 % des métiers qui exigeront un niveau de chercheur ou d'expert en IA. Ce 1 %, il est en haut de la « chaîne alimentaire ». Quand on raisonne en compétences nouvelles à introduire dans les formations, il faut aussi penser aux compétences que l'on va perdre, celles qui vont être très rapidement obsolètes. 70 % de nos compétences seront obsolètes dans les 5 ans ».

On ne peut donc faire l'impasse sur une montée des compétences en matière d'IA si l'on veut développer un « territoire de tous les possibles », car de nombreuses actions possibles sont déjà ou seront conditionnées par des usages permis par les IA. L'exemple de Wasoria, startup implantée au sein du Hub&Go en offre une illustration. Thierry Petitjean, ingénieur R&D, présente la solution développée avec l'IA et qui permet de détecter dans les déchets les matériaux dangereux (batteries, bouteilles de gaz ou de protoxyde d'azote).

Cette application intéresse directement les collectivités territoriales, notamment le service public en charge du traitement des déchets. Mais elle n'est pas la seule.

En septembre 2025, la Chine rend obligatoire la formation à l'IA dans toutes les écoles, dès le plus jeune âge. Si l'on veut que les territoires demeurent compétitifs, c'est un modèle à copier sous peine d'être déclassés, suiveurs et non leaders. Jeremy Pinto, vice-président de la CUCM, délégué à l'enseignement supérieur, la recherche et l'innovation, est convaincu de la nécessité d'une connaissance commune qui exige une formation importante, qu'elle soit initiale ou continue. La Communauté urbaine est membre du consortium CAIRE (Citizen-oriented Artificial Intelligence training for a Responsable Education), projet visant à mettre en place une démarche durable et massive de formation des citoyens aux usages de l'intelligence artificielle. CAIRE, impulsé notamment par l'ENSAM, le CNAM et l'université de Bourgogne Europe, rassemble le monde économique et les institutions publiques autour de formations courtes, certifiantes. Le regard de Jeremy Pinto va au-delà de la formation, puisqu'il intègre la réflexion sur l'IA au sein de la CUCM dans une approche plus globale qui prend en compte les effets environnementaux (impacts sur l'énergie, l'eau, la production de CO^2) et sa relation avec la productivité et l'innovation.

Cet élargissement du champ souligne que l'approche cyber par un territoire dépasse le cadre strict de la cybersécurité pour s'ouvrir à un écosystème complexe et interdépendant. Le Forum INCYBER des territoires est certes centré sur la cybersécurité, condition d'une croissance maîtrisée, mais il met aussi en évidence les interactions, les influences qui cristallisent des domaines, apparemment distincts, mais tous contributeurs à une maîtrise de la transformation numérique du territoire.

POURSUIVRE L'AVENTURE

Nous avons été rapidement convaincus, quand nous sommes venus ici, par le terreau très favorable de que constituait la Communauté urbaine du Creusot Montceau et toute la région pour cette 1ère édition du Forum INCYBER des territoires.

Terreau favorable en matière d'innovation sous toutes ses formes, qu'elles soient industrielles ou numériques, et les deux vont de pair aujourd'hui,

Terreau favorable dans le domaine industriel avec la présence de nombreux fleurons.

Terreau favorable sur le plan de la formation, comme le démontre la présence à nos côtés de Vincent Thomas, président de l'université de Bourgogne Europe qui offre des cursus dédiés notamment à l'ingénierie industrielle et aux technologies opérationnelles.

Terreau évidemment favorable, enfin, au niveau politique avec des collectivités qui sont résolument engagées dans la transformation numérique avec la recherche permanente de nouveaux usages au service des territoires.

4 MOTS-CLÉS PEUVENT DÉCRIRE LA TENEUR DE NOS ÉCHANGES

Le premier est la proximité. Le numérique est une réalité relativement désincarnée, parfois même nébuleuse. Il faut donc le rapprocher des utilisateurs, des citoyens. Et pour cela, comme le dit l'adage, penser global, mais agir localement. L'échelon local est essentiel pour toucher les citoyens, les TPE, les PME. Cette proximité doit notamment se traduire par l'assistance aux victimes d'arnaques en ligne ou de cyber attaques. D'où l'intérêt du dispositif 17 cyber, qui vient d'être mis en place par Cyber Malveillance dans le cadre d'une approche collective associant l'ensemble des acteurs publics, que ce soit l'ANSSI, la Gendarmerie nationale, le ministère de l'Intérieur et tous les services régionaux et bien sûr les prestataires privés.

Le deuxième mot-clé, c'est la maturité. Elle est évidemment très variable en fonction des acteurs, avec des TPE et PME qui sont souvent des oubliés de la cybersécurité. Aujourd'hui, la priorité est de traiter les plus fragiles, et pour cela de « passer à l'échelle ». Nous disposons pour cela d'un formidable levier en matière de prévention des risques avec la directive NIS2. Bien sûr, ce sont aussi des contraintes, et donc des coûts. Je rappelle que 73 % des petites et moyennes communes ont des budgets IT inférieurs à 5 000 euros. Attention, donc, à ne pas être en décalage ! Néanmoins, c'est à ce niveau-là qu'il faut développer « l'hygiène numérique ». C'est à ce niveau-là qu'il faut mutualiser des ressources parce que la plupart du temps ces acteurs n'ont pas besoin d'un responsable cybersécurité à temps plein. Et c'est pour cela qu'il faut aussi développer des offres, des solutions de sécurité très intégrées, très packagées. On dit souvent que la sécurité coûte cher. Oui, elle coûte cher pour des organisations complexes. Mais le marché offre aujourd'hui aussi des solutions adaptées à des structures plus légères. Il est possible pour quelques euros par mois de sécuriser un poste de travail, ce qui constitue une garantie forte de pérennité.

Le troisième mot clé, c'est la résilience, qui prend dans le domaine numérique une sens particulier. C'est tout d'abord la capacité à surmonter un certain nombre d'aléas, qu'il s'agisse de pannes, de cyberattaques mais aussi d'erreurs humaines. Dans des systèmes aussi complexes, il faut en effet accepter que les erreurs puissent arriver. C'est enfin la maîtrise de ses dépendances, de ses sources d'approvisionnement, avec un risque qui est de nature beaucoup plus géopolitique que technique. Exemple : votre fournisseur *Cloud* décide de couper les services qu'il vous fournit sur l'injonction d'un gouvernement ou à la suite de sanctions internationales. Bien sûr, il est impossible de revenir sur ces chaînes de valeurs qui sont très globalisées, en particulier dans le domaine numérique, mais il est essentiel de diversifier ses approvisionnement et de recourir — lorsqu'ils existent — à des prestataires souverains pour gérer les données les plus sensibles ou maîtriser certains points critiques comme la gestion des identités ou le chiffrement des données. Et pour cela, ne pas hésiter à choisir des solutions européennes. C'est un choix courageux, difficile, car la facilité commande de choisir des solutions implantées beaucoup plus largement et depuis longtemps sur le marché. Ce qui empêche la montée en puissance de solutions françaises et européennes, qui pourtant existent.

Le quatrième mot-clé, c'est la collaboration. L'espace numérique est une sorte de brouillard qui favorise toujours l'attaquant. La seule façon de répondre à cette asymétrie, c'est donc un surcroit de collaboration et d'intelligence collective des défenseurs. D'autant que les attaquants collaborent évidemment très fortement aussi. Collaboration entre le public et le privé, collaboration également entre les entreprises privées pour partager l'information sur les menaces. Collaboration, enfin, entre les États. Ce sont ces collaborations qui ont permis ces derniers mois de spectaculaires opérations contre des groupes cybercriminels. Il n'y a donc pas de fatalité en matière de lutte anti-cybercriminalité !

Ces quatre mots clés nous engagent à poursuivre avec vous l'aventure du Forum INCYBER des territoires. Le Forum in Cyber s'étend désormais de Lille à Montréal et du Creusot à Tokyo.

Guillaume TISSIER
Associé Forward Global
Directeur général du Forum INCYBER Europe

PAROLE DONNÉE À DES PARTENAIRES DU FORUM

Le Forum INCYBER des territoires a pu être organisé grâce aux soutiens de partenaires engagés, chacun dans son domaine, dans la cybersécurité des territoires. Si leurs propos n'ont pas été intégrés dans le corps du texte, dans la mesure où ils n'ont pas participé à une table ronde, ils trouvent ici une place pour exprimer leur point de vue.

UNE STRATÉGIE DE CYBERSÉCURITÉ TERRITORIALE N'EST PLUS UNE OPTION

C'est une nécessité pour garantir la souveraineté numérique, la résilience des services publics et la confiance des usagers.

Les territoires, qu'ils soient urbains ou ruraux, hébergent des infrastructures critiques (mairies, hôpitaux, écoles, etc.) qui sont de plus en plus exposées aux cybermenaces. Une attaque réussie peut compromettre la continuité des services publics et entraîner des pertes économiques majeures.

Dans un contexte économique dégradé et de pression réglementaire accentuée, comment renforcer la sécurité des territoires tout en soutenant leur transformation numérique ?

S'appuyant sur la convergence de ses expertises *Cloud*, connectivité, cybersécurité, communication et collaboration, adista héberge, sécurise et opère les systèmes d'information des entreprises et collectivités partout en France à travers ses 45 agences commerciales et ses 16 *datacenters* de proximité. Un ancrage territorial unique sur le marché.

adista propose une approche structurée de la cybersécurité fondée sur les piliers : gouverner, identifier, protéger, détecter, répondre et restaurer.

Les besoins en cybersécurité varient selon les territoires (densité de population, infrastructures numériques, niveau de maturité IT des métiers). Audit et Conseil en Sécurité, Protection DDoS & Firewalling, Détection et Réponse aux Incidents (EDR/MDR), etc.,adista adapte ses solutions en fonction des contraintes opérationnelles et budgétaires propres à chaque collectivité.

En complément, adista s'appuie sur devensys cybersecurity. Un centre d'opérations en cybersécurité (SOC) assurant une surveillance 24/7, la détection des menaces et la mise en œuvre de recommandations préventives. Son engagement envers la sécurité est attesté par nos certifications ISO 27001 - HDS (Hébergeur de Données de Santé) - Rapport ISAE 3402 »

Adrien SUEUR
adista

PROXIMITÉ ET INNOVATION AU SERVICE DE LA CYBERSÉCURITÉ DES TERRITOIRES

Le territoire Creusot Montceau, riche de son patrimoine industriel et de ses acteurs publics et privés dynamiques, incarne un concentré d'innovation, de savoir-faire et de résilience. Dans un monde où les cyberattaques se multiplient, protéger nos données, nos outils de production et notre patrimoine économique local est devenu un enjeu stratégique.

Depuis 55 ans, AMG Informatique s'engage aux côtés des entreprises, collectivités et structures industrielles locales pour proposer une cybersécurité humaine, réactive et souveraine. PME indépendante enracinée en Bourgogne-Franche-Comté, nous défendons une approche pragmatique et transversale : audits sur site, sensibilisation, supervision, sauvegarde, gestion des accès, réponse à incident. Nos solutions reposent sur des technologies éprouvées et des choix produits français et européens.

Notre engagement repose sur trois piliers fondamentaux :

— La proximité, avec des équipes locales qui connaissent le territoire et ses enjeux

— L'innovation, avec des outils comme notre solution d'audit Sylink, rapide à déployer et simple à interpréter

— Le respect de nos engagements

Chez AMG Informatique, nous ne sommes pas de simples fournisseurs : nous sommes des partenaires de confiance. Nous privilégions une relation durable fondée sur l'écoute et une parfaite compréhension des enjeux métiers.

Chaque recommandation est issue d'une analyse rigoureuse des besoins, des risques et du contexte opérationnel.

Enfin, nous adoptons une démarche résolument proactive, grâce à une veille continue et des audits réguliers, afin d'aider à anticiper les menaces et garder une longueur d'avance sur les défis numériques.

Développer une stratégie cyber territoriale, c'est garantir la continuité des activités, sécuriser les infrastructures critiques et préserver l'attractivité de notre région.

Forte de son histoire et tournée vers l'avenir, AMG Informatique est plus que jamais prête à protéger et accompagner le territoire du Creusot Montceau, aux côtés de ceux qui le font vivre.

Mickaël LECOUSTRE
Directeur de la division cybersécurité
AMG Informatique

UNE STRATÉGIE TERRITORIALE DE CYBERSÉCURITÉ POUR UNE INDUSTRIE 4.0

Le territoire du Creusot Montceau, fort de son héritage industriel et engagé dans la transition vers l'industrie 4.0, se caractérise par un écosystème dense où interagissent grands groupes, PME, collectivités locales, acteurs de la recherche et infrastructures critiques. Cet environnement, porteur de développement, constitue également une cible privilégiée pour les cybermenaces, rendant indispensable la mise en place d'une stratégie territoriale de cybersécurité.

Dans le secteur industriel, la vulnérabilité s'accroît avec l'interconnexion des systèmes de production et des réseaux numériques. Les cyberattaques, au-delà du vol de données, sont désormais susceptibles d'interrompre des chaînes de production, de compromettre la sécurité des salariés et de provoquer des dommages matériels significatifs. La sécurisation des systèmes de contrôle industriel doit ainsi être considérée comme un enjeu prioritaire et structurant pour la compétitivité du territoire.

Les collectivités locales sont par ailleurs confrontées à des risques accrus du fait de la digitalisation des services publics. Les plateformes d'e-administration, les services liés à l'état civil ou encore la gestion des déchets constituent autant de points d'exposition. Une attaque de type *ransomware* pourrait paralyser l'accès aux services essentiels, fragiliser le versement des aides sociales et mettre en péril la continuité de services vitaux, tels que la distribution d'eau potable.

Les citoyens ne sont pas en reste face aux menaces liées à la généralisation des usages numériques. Hameçonnage, fraudes en ligne et usurpation d'identité soulignent la nécessité d'un volet de sensibilisation, afin de promouvoir des comportements responsables et sécurisés.

Dans ce contexte, la construction d'une stratégie territoriale de cybersécurité ne saurait se limiter à une logique défensive. Elle constitue une opportunité de positionner le Creusot-Monceau comme un pôle d'excellence et un territoire pionnier dans le domaine de la confiance numérique.

Au sein de Fortress Cybersecurity, nous sommes conscients de l'importance d'une stratégie à l'échelle locale. Bien que la France dispose d'une stratégie nationale, il est important que celle-ci se traduise concrètement sur les territoires.

Fortress Cybersecurity en qualité d'opérateur de services dédié à la cybersécurité industrielle contribue à la stratégie du Creusot Monceau en accompagnant les entreprises du secteur. Les savoir-faire de Fortress Cybersecurity concernent les états des lieux, de missions de stratégie, conseil, de transformation et d'intégration de solutions ainsi que de détection, réaction et veille sur la menace cyber. Le secteur industriel nécessite un accompagnement spécifique issue du retour d'expérience des deux fondateurs de Fortress Cybersecurity de plus de 25 ans dans le domaine.

Caroline CHAUMET
Responsable du développement
Fortress Cybersecurity

CHAQUE MAILLON A UN RÔLE À JOUER DANS UNE STRATÉGIE COLLECTIVE

Notre modèle démocratique permet à chaque citoyen de se présenter aux différentes élections, une fois élus ils seront en charge de participer à la vie des territoires. Ces élus peuvent avoir accès à des services ou des données représentant un intérêt pour un acteur malveillant, cependant au niveau local (commune ou communauté de communes) très peu d'entre eux sont formés aux risques cyber. Ce même risque s'applique aux différents services en lignes proposés aux habitants par les collectivités locales (inscription en cantine/garderie, collecte des déchets, etc.). Dans le cas de territoire comme la communauté urbaine du Creusot Montceau regroupant trente-quatre communes, comment s'assurer que chacune d'entre elles à conscience du risque ? Quels sont les moyens que l'on peut mettre à disposition pour avoir un niveau de sécurité minimum ? Ces exemples illustrent le fait que la surface d'attaque d'une communauté de commune est extrêmement vaste, il est par conséquent indispensable de réfléchir à une stratégie cyber à son niveau. Des initiatives au niveau régional existent avec la mise en place des CSIRTs (équipes spécialisées dans la gestion des incidents de sécurité informatique) dans les différentes régions. Cela permet d'ores et déjà aux acteurs publics d'avoir accès à des informations sur cette thématique. L'organisation du premier Forum INCYBER des territoires a également permis aux acteurs locaux de se rencontrer et d'échanger afin de voir comment prendre un compte ce nouveau type de risque pour nos collectivités locales. Le sujet devient de plus en plus important de jour en jour et la mise en place d'une stratégie collective, où chaque maillon à son rôle à jouer, permettra de réduire les impacts voire même d'éviter des attaques.

Sebastien COGNEAU
H4CKRZ

LES CYBERATTAQUES NE SONT PAS UN MYTHE !

Les cybercriminels bénéficient d'un vaste terrain de jeu, au sein duquel nul n'est à l'abri, où la sécurité passe par une prise de conscience commune (acteurs publics comme privés) et la mise en place d'une stratégie de cybersécurité claire et unifiée à destination des territoires pour répondre à plusieurs enjeux cruciaux : sécurité, résilience et souveraineté numérique.

Le secteur public, dans ses fonctions gère des services critiques à destination des citoyens assurant ainsi le bon fonctionnement d'infrastructures telles que : l'eau, l'électricité, les transports, la santé, etc. Par conséquent, une cyberattaque sur ces environnements pourrait créer des situations extrêmement difficiles à gérer avec des impacts forts sur le plan humain et matériel, à court moyen et long terme. En complément le secteur privé, rouage essentiel au développement et à l'attractivité du territoire du Creusot Montceau, est composé d'entreprises industrielles à dimension internationale mais aussi de sociétés à caractère innovant. Celles-ci représentent un capital économique, intellectuel et technologique qu'il faut donc protéger.

C'est pourquoi, l'Humain doit être placé au centre des réflexions et des stratégies à bâtir au milieu de cette menace virtuelle. La sensibilisation doit être pour le futur un axe fort de développement puisqu'elle a une double vertu ; renforcer la résilience des entreprises tout en faisant monter le niveau de perception des risques Cyber à destination des citoyens. A cela, s'ajoute bien entendu la mise en œuvre de solutions techniques robustes et pérennes afin de renforcer les remparts des organisations. Le Forum INCYBER des territoires permet de fédérer les énergies pour faire de la Cybersécurité l'affaire de tous !

Matthieu BOUCHET
Mediane système

RÉPONDRE AUX ENJEUX DES TERRITOIRES INDUSTRIALISÉS

Orange Cyberdefense s'illustre par son expertise sectorielle dans la protection des organisations industrielles, incarnée lors du Forum INCYBER des Territoires organisé au Creusot en mai 2025, événement centré sur la cybersécurité industrielle et la souveraineté numérique locale. Dans ce contexte, son savoir-faire s'articule autour d'une approche globale de la sécurisation des environnements industriels, incluant la prévention, la détection et la réponse aux incidents spécifiques à l'industrie 4.0.

Orange Cyberdefense propose des solutions adaptées aux enjeux des territoires industrialisés : sécurisation des réseaux industriels (OT/IT), analyse des menaces ciblant les chaînes de production, et mise en conformité avec les normes réglementaires telles que NIS 2.

Lors du forum, Orange Cyberdefense a mis en avant sa capacité à accompagner collectivités, PME et grands groupes dans la mise en place de stratégies de cybersécurité sur mesure, grâce à la mobilisation de ses experts, ses services de veille et ses outils avancés de supervision et gestion de crises.

L'intervention au Creusot a illustré une dynamique d'innovation locale : expertise collaborative, partage de retours d'expérience et création de plateformes solidaires face aux risques cyber. Cette approche fait d'Orange Cyberdefense un acteur clé dans la transformation numérique sécurisée des territoires industriels, répondant autant aux défis techniques qu'aux impératifs de résilience et de confiance numérique.

Olivier ROUGET
Directeur innovation territoriale
Bourgogne-Franche-Comté
Orange Cyberdéfense

POUR UN NUMÉRIQUE LOCAL PLUS SOBRE, ÉTHIQUE ET INCLUSIF

Filiale de SPIE France, SPIE ICS est une entreprise de services numériques française. Forte de ses compétences historiques en intégration et en infogérance, SPIE ICS accompagne la transformation numérique de ses clients grâce à ses expertises : environnement de travail numérique, infrastructures, *Cloud*, *Smart Data* et cybersécurité. SPIE ICS s'engage pour un numérique local plus sobre, éthique et inclusif, une démarche reconnue par le label Numérique Responsable niveau 2.

Avec 3 200 collaborateurs et 60 implantations en France, SPIE ICS offre une relation de proximité unique sur le marché, qui lui permet de proposer des solutions sur mesure à ses clients. Acteur global et local des transitions énergétique, numérique et industrielle, SPIE France, filiale du groupe SPIE, propose des solutions qui accompagnent les entreprises, les industries, les villes et les territoires pour l'émergence d'une société bas carbone. Pour mener à bien cette mission, SPIE France s'appuie sur ses 6 filiales, qui comptent 19 000 collaborateurs présents sur 400 sites en France.

Avec plus de 50 000 collaborateurs, le groupe SPIE a réalisé, en 2023, un chiffre d'affaires consolidé de 8,7 milliards d'euros et un EBITA consolidé de 584 millions d'euros. »

Elise BOCCARD
SPIE ICS
Département Bourgogne-Franche-Comté

IN CYBER FORUM EUROPE

Creusot Montceau Communauté Urbaine

FORUM INCYBER DES TERRITOIRES

TERRITOIRE 4.0 & CYBERSÉCURITÉ INDUSTRIELLE

Le Forum INCYBER des Territoires est coorganisé par
la Communauté Urbaine du Creusot et le Forum INCYBER

ÉQUIPE CUCM

Laurent BOUQUIN, Saliha MAKHLOUF,
Marie-Anne GUILLEMIER, Marie-Pierre ANSELME,
Francine LORDEY, Laetitia DURIX,
Marie VENNARI, Fiorina MOREAU

creusot-montceau.org

ÉQUIPE FORUM INCYBER

Guillaume TISSIER, Clémence EPITALON,
Aymeric HUMBERT, Carole SPANG,
Marc WATIN-AUGOUARD

territoires.forum-incyber.com

contact@forum-incyber.com

PARTENAIRES

IN CYBER FORUM EUROPE FORUM INCYBER DES TERRITOIRES 11-13 JUIN 2026