FIEEC

FEDERATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

CONFIANCE ET SÉCURITÉ NUMÉRIQUE DANS UN MONDE CONNECTÉ (IoT)

Une filière d'excellence en France

(PME, ETI et grands groupes) force de proposition

Sommaire

Avant-propos - Par Gilles Schnepp
Président de la FIEEC

La complémentarité des technologies de l'électricité, de l'électronique et du numérique est désormais une réalité et chaque secteur fait quotidiennement l'expérience d'une profonde transformation de ses modèles par le numérique. Cette évolution touche l'ensemble des activités et des fonctions des entreprises.

Les électrotechnologies, moteur de la transformation numérique

A la source et au cœur de ce nouveau paradigme se trouvent les électrotechnologies. En effet, la connectivité croissante de tous les objets (IoT), la gestion, le stockage et l'utilisation des données qui en résultent sont les leviers majeurs de la transformation numérique. Ces leviers et leur développement sont permis par les produits, services et solutions des industries électriques, électroniques et numériques qui jouent donc le rôle de catalyseur de cette révolution.

Les bénéfices attendus de la digitalisation sont aussi nombreux que variés. En premier lieu, les innovations générées permettent d'apporter de nouvelles réponses à l'ensemble des grands sujets sociétaux : développement durable, santé, sécurité, urbanisation, production, mobilité, vieillissement de la population, etc. Autant de sujets sur lesquels des solutions nouvelles optimisent les modèles jusque-là en vigueur pour rendre un service plus efficient, plus respectueux de l'environnement ou plus compétitif.

Ainsi, le numérique nous permet désormais d'opérer un grand bond dans la courbe d'amélioration des solutions proposées, à l'Etat, aux administrations et aux citoyens pour satisfaire chacun de leurs besoins. La connectivité et les données rendent chaque application plus intelligente et autorisent une gestion toujours plus fine des réponses apportées par chaque secteur.

Pas de transformation numérique sans sécurité ni confiance

Toutefois, l'ensemble de ces bénéfices ne peut se matérialiser qu'à la condition que chacun ait confiance dans ces solutions. Cette confiance repose sur la certitude que les données, carburant de la transformation numérique, ne seront utilisées que pour ce à quoi on les destine.

Cela suppose que la sécurité numérique soit au cœur de tout développement : la mise en place de dispositifs assurant la disponibilité, la confidentialité et l'intégrité des données est donc aujourd'hui une condition *sine qua non* pour permettre un développement numérique de confiance.

De ce point de vue, la FIEEC constitue un laboratoire idéal et une plateforme d'échanges parfaitement adaptée pour aborder ce domaine de la confiance et de la sécurité numérique. Elle regroupe à la fois les industriels qui sécurisent le numérique (cybersécurité, identité numérique traçabilité,…), ceux qui intègrent ces solutions de sécurité dans leur propres solutions *smart (smart industry, smart city, smart buiding, smart mobility, smart health,* etc.), mais aussi les industriels qui rendent cette sécurisation possible grâce aux outils qu'ils développent (infrastructures électriques et télécoms, capteurs électroniques et physiques, caméras, logiciels, etc.).

Le présent document a ainsi pour vocation d'apporter un éclairage simplifié sur le périmètre, infiniment complexe, de la sécurité et de la confiance numérique, de ses principales applications, ainsi que des enjeux majeurs de nos professions dans ce domaine. Il se veut une cartographie illustrée du rôle de nos industries dans un domaine au cœur de l'actualité et dont les contours restent difficiles à esquisser. Le sujet est stratégique pour le développement économique de notre pays et la FIEEC entend bien y prendre toute sa place.

Nous vous en souhaitons une bonne lecture.

Edito - Par Anne Bouverot
Vice-Présidente de la FIEEC - Sécurité Numérique

La confiance et la sécurité numérique sont sans doute l'un des plus grands défis collectifs de notre société. La démonstration a été faite que nos sociétés ne peuvent se passer de l'ensemble des bénéfices que promet le numérique dans toutes ses applications. Aujourd'hui, de plus en plus d'objets sont connectés, les mobiles bien sûr mais aussi les véhicules, les compteurs intelligents… Les données collectées, transmises, stockées et gérées sont la matrice de nouvelles activités économiques. Le numérique a ouvert un champ immense de progrès pour notre société mais comme toute révolution majeure, elle ne décollera vraiment que lorsque nous aurons chacun et chacune suffisamment confiance dans sa mise en œuvre !

Pour créer la confiance : sécurité du numérique, sécurité par le numérique

Les notions de confiance et de sécurité numérique sont polymorphes et recouvrent de nombreuses réalités concrètes. Il convient notamment de distinguer la sécurité du numérique et la sécurité par le numérique.

En effet, notre vie numérique ou digitale prise au sens large, a un besoin fondamental de sécurisation comme le démontrent les cyberattaques de plus en plus nombreuses et dont les cibles ne cessent de s'élargir. Par exemple, le « ransomware » WannaCry a touché plus de 300 000 utilisateurs dans plus de 150 pays en mai dernier. Il est désormais impératif que chacune des briques numériques soient pensées, *ab initio*, comme devant être sécurisées à la fois en tant qu'unités et dans un ensemble intégré – c'est la sécurité « *by design* ». Les entreprises représentées par la FIEEC offrent un large panel de solutions de sécurité numérique, depuis l'identification et l'authentification, en passant par la cybersécurité et la traçabilité.

Par ailleurs, les produits, services et solutions issues du domaine numérique ont un apport majeur pour assurer la sécurité au sens large. Ces outils permettent par exemple la sécurisation de notre pays, de nos villes, de l'ensemble de nos activités, grâce à des solutions toujours plus performantes. Elles permettent de mieux anticiper et détecter les risques et menaces et de contribuer à mieux coordonner et gérer les actions de sécurisation. Autant de nouvelles réponses applicables tant à l'action régalienne des autorités publiques que par les acteurs privés pour tous leurs besoins de sécurisation. Ainsi, c'est une panoplie très complète de réponses que nos industries apportent tant à l'administration qu'au secteur privé pour faire en sorte que tout ce que le numérique promet de « *smart* » soit également « *safe* ».

L'excellence reconnue des entreprises françaises

La France dispose d'atouts très importants grâce à l'excellence de son enseignement scientifique, de ses ingénieurs, et de son tissu industriel extrêmement dense et dynamique, composé à la fois de grands groupes leaders à l'international dans leurs domaines et de PME-ETI très agiles. Cette excellence est mondialement reconnue et constitue pour notre pays une opportunité forte. Il faut que ce secteur puisse parler d'une même voix pour faire connaître ces atouts et porte ses priorités dans le débat public.

Porter collectivement le secteur en France et travailler à l'échelon européen

Le contexte législatif et réglementaire français et européen est, en effet, particulièrement important. Par exemple, le nouveau Règlement Européen de Protection des Données (RGPD), a pour objectif de protéger les identités digitales des citoyens, et entrera en vigueur en mai 2018. Il est essentiel que notre profession soit force de propositions pour que le cadre réglementaire permette le développement pérenne du secteur. Des positions françaises fortes de notre industrie constituent un socle solide pour, de concert avec nos partenaires européens, définir les règles du jeu de demain. La collaboration étroite franco-allemande entre la FIEEC et le ZVEI est en ce sens un lien à privilégier.

La sécurité et la confiance numérique constituent un enjeu stratégique majeur public-privé, tant pour l'Etat, les administrations que pour les entreprises et les citoyen(ne)s. Nous avons la chance unique de pouvoir nous appuyer sur des entreprises françaises performantes, dans un domaine qui relève du développement économique et social, et souvent de la souveraineté nationale.

Dans ce secteur plus que dans tout autre, la synergie et l'action collective sont la clé du succès. Face aux enjeux majeurs de confiance qui nous font face, il est capital de faire valoir nos atouts et de poursuivre une collaboration soutenue avec les pouvoirs publics en charge des domaines de la confiance et de la sécurité numérique. Allier le développement économique d'un secteur de pointe et l'impératif d'amélioration de notre sécurité numérique est à notre portée. C'est ensemble que nous y parviendrons.

Edito - Par Guillaume Poupard
Directeur Général de l'ANSSI
(Agence Nationale de la Sécurité des Systèmes d'Information)

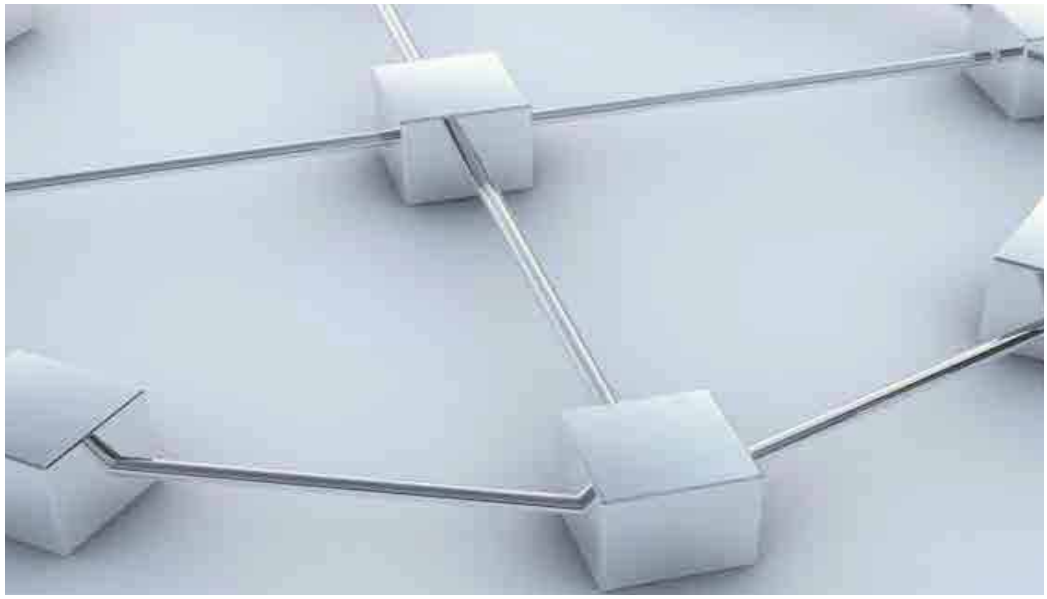
Pour l'administration, les entreprises et les particuliers, le numérique est une source d'opportunités sans commune mesure. Mais les technologies et les usages qui en découlent entraînent irrémédiablement dans leur sillage de nouvelles menaces. De plus en plus inédites, nombreuses et sophistiquées, elles peuvent avoir des conséquences désastreuses sur l'activité de tout un pays, de la prise de contrôle de systèmes industriels à l'atteinte à la stabilité démocratique d'un Etat.

Dès lors, la transition numérique ne saurait se réaliser sans confiance et sans un réel effort de sécurité coordonné. Alors que la prise de conscience du risque numérique se généralise, la France et l'Europe encouragent et encadrent cette transition. Pour élever le niveau de sécurité des opérateurs, le cadre réglementaire national et européen évolue et fait le pari d'imposer un niveau minimal de cybersécurité aux opérateurs les plus sensibles.

Une ambition qui passe par l'animation de tout un écosystème et en particulier par la mobilisation du tissu industriel.

C'est pourquoi j'ai engagé, au niveau national et en collaboration avec les acteurs industriels, de multiples actions visant à favoriser le développement de nouveaux produits de sécurité, notamment dans le cadre des programmes d'investissement d'avenir, à inclure le volet cybersécurité dans les processus des organismes certificateurs privés, ainsi qu'à faire évoluer les méthodes et référentiels de l'ANSSI pour satisfaire les nouveaux besoins en matière de certification et de qualification de produits et services. J'ai également engagé un dialogue avec nos partenaires européens destiné à partager nos principes et méthodes de certification.

Interlocuteur industriel incontournable de l'Etat, j'attends par conséquent de la FIEEC et de ses membres un éclairage permanent sur les nouveaux besoins ou opportunités en matière d'offres, de même qu'un soutien dans la promotion des bonnes pratiques indispensables au renforcement de la confiance dans les offres de produits, services et systèmes.



Edito - Par Isabelle Falque-Pierrotin
Présidente de la CNIL
(Commission Nationale de l'Informatique et des Libertés)

Le numérique irriguant aujourd'hui toutes les activités humaines, les industriels sont confrontés à de grands enjeux. Il s'agit de plus en plus de rendre les systèmes communicants et intelligents. Ces aspects renforcent l'importance de la confiance des utilisateurs dans les systèmes qu'ils utilisent. Plus que jamais cette confiance passe par la sécurisation des dispositifs.

A ce titre, le Règlement européen sur la protection des données est une chance. Il prévoit en particulier la responsabilisation des organismes tout en renforçant les droits des personnes. Il repose sur les principes essentiels que sont le « *privacy by design* », le « *privacy by default* » et la « *security by design* ».

Le conseil et l'accompagnement des professionnels est une des missions cardinales de la CNIL. La CNIL se félicite d'accompagner depuis plusieurs années maintenant la FIEEC dans les chantiers qu'elle met en œuvre. Les industries électro technologiques adhérentes de la FIEEC couvrent un pan essentiel du paysage industriel français. Cet accompagnement fécond permet la promotion des bonnes pratiques dans le domaine de la protection de la vie privée des personnes.

Dans le cadre de cet accompagnement, la CNIL élabore des « packs de conformité ». Elaborés en concertation étroite avec les acteurs d'un secteur d'activité, les packs représentent un nouveau mode de régulation pour la Cnil. On peut parler de co régulation et même de co construction dans la définition des bonnes pratiques qui permettront d'assurer sécurité juridique aux acteurs et accroissement du capital de confiance vis à vis de leurs interlocuteurs. En assurant la diffusion de ces bonnes pratiques parmi leurs adhérents, la FIEEC démontre qu'elle a compris comment tirer parti du droit pour en faire un facteur de succès. Ces packs sont des boîtes à outils de la conformité proposant des lignes directrices pour une utilisation responsable des données, conforme à la loi Informatique et Libertés et au RGPD. L'enjeu est d'intégrer la dimension

« protection des données personnelles » dès la phase de conception des produits et d'assurer la transparence et le contrôle par les personnes de leurs données conditionnant la confiance. Il s'agit aussi de responsabiliser tous les acteurs de la chaine et pas uniquement les exploitants de données. La mise en œuvre de mesures de sécurité adéquate est un prérequis indispensable. Celles-ci doivent être dimensionnées en fonction des risques sur la vie privée que l'utilisation des dispositifs fait peser sur les personnes. La sécurité fait intervenir des dimensions multiples : aspects organisationnels, techniques et humains.

Les travaux menés en partenariat avec la FIEEC s'appliquent à des secteurs de premier plan et porteurs d'enjeux pour les personnes (énergie, transport, aide à la personne, etc.). Un premier pack consacré aux compteurs communicants a ainsi été publié en 2014. Deux autres auxquels la FIEEC est étroitement associée sont actuellement en cours d'élaboration. Le premier consacré aux « véhicules connectés » et le second à la « *Silver* économie ».

Les entreprises françaises ayant intégré ces outils pourront aborder le règlement européen de façon plus sereine car elles auront fait une bonne partie du chemin vers l' « *accountability* », ou principe de responsabilité des acteurs, clé de voûte de la conformité à l'heure du règlement qui s'appliquera à compter du 25 mai 2018.

CNIL
Commission Nationale de l'Informatique et des Libertés

Introduction générale - Par Patrick Bertrand
Vice-Président de la FIEEC - Numérique

Le numérique est au cœur des évolutions de notre société. Cette digitalisation engendre des transformations profondes qui induisent un bouleversement sans précédent des usages, des modes de vie et des modèles économiques, mais emportent aussi des risques nouveaux qu'il convient d'adresser et de mieux anticiper. L'objectif est clair : trouver le bon chemin entre l'enjeu majeur de l'innovation et du progrès économique et social que chacun en attend et l'impérative nécessité que cette formidable dynamique ne remette pas en cause des fondements de la vie citoyenne. Cela est possible, n'en déplaise aux tenants de l'innovation à tout prix qui ne devraient subir aucune contrainte et/ou encadrement visant à protéger le citoyen et le consommateur.

Sans être exhaustif, trois lignes directrices nouvelles semblent aujourd'hui devoir guider nos réflexions.

Tout d'abord, une approche d'anticipation plus forte de la part des acteurs économiques.

La question, centrale, de la protection des données personnelles a conduit les acteurs de la profession à mieux anticiper la bonne gestion du sujet dans la construction de leurs offres économiques. Cette notion de *« privacy by design »* est aujourd'hui bien appréhendée, en parfaite liaison avec la CNIL.

Pour autant, cette démarche doit être aujourd'hui mise en corrélation avec les enjeux de sécurité numérique qu'il est aujourd'hui impératif d'anticiper de la même façon. La notion de « *security by design* » devient dès lors un corollaire indispensable pour les acteurs industriels et économiques. Le présent document brosse de manière pédagogique les enjeux sur ce sujet essentiel afin d'accentuer la prise de conscience sur les risques nouveaux : le partenariat en cours avec l'ANSSI s'inscrit pleinement dans cette approche.

Des interrogations, ensuite, sur l'opportunité d'une nouvelle approche de co-régulation.

Les enjeux de la sécurité numérique interpellent sur les limites de la régulation conventionnelle. Les règles sont posées et ajustées en matière numérique et de sécurité (ie. règlement GDPR, directive NIS, loi sur la république numérique en particulier). Le cadrage général d'application uniforme au sein de l'Union européenne est également important et nécessaire pour l'ensemble des parties prenantes.

Toutefois, force est de constater que l'évolution extrêmement rapide des nouvelles technologies est peu compatible avec l'élaboration de règles juridiques de plus en plus précises et détaillées visant à couvrir l'ensemble des situations.

A celà s'ajoute la complexité croissante de la science des systèmes et la difficulté pour le législateur de répondre, comme par le passé, à des situations très diverses par une réglementation aussi pointilleuse que perfectible. Sans compter que la stabilité juridique est un élément de sécurité essentiel pour les acteurs économiques. Nous touchons là les limites historiques de notre culture juridique romano-germanique.

Cette situation nouvelle implique de compléter utilement notre dispositif législatif et réglementaire par une approche de *soft law,* plus consolidée et partenariale, où l'anticipation et le partage des évolutions semble avoir toute sa place sur fond de responsabilisation plus forte de tous les acteurs.

Le pack de conformité élaboré avec la CNIL sur les *smart grid* illustre bien ce partenariat nouveau.

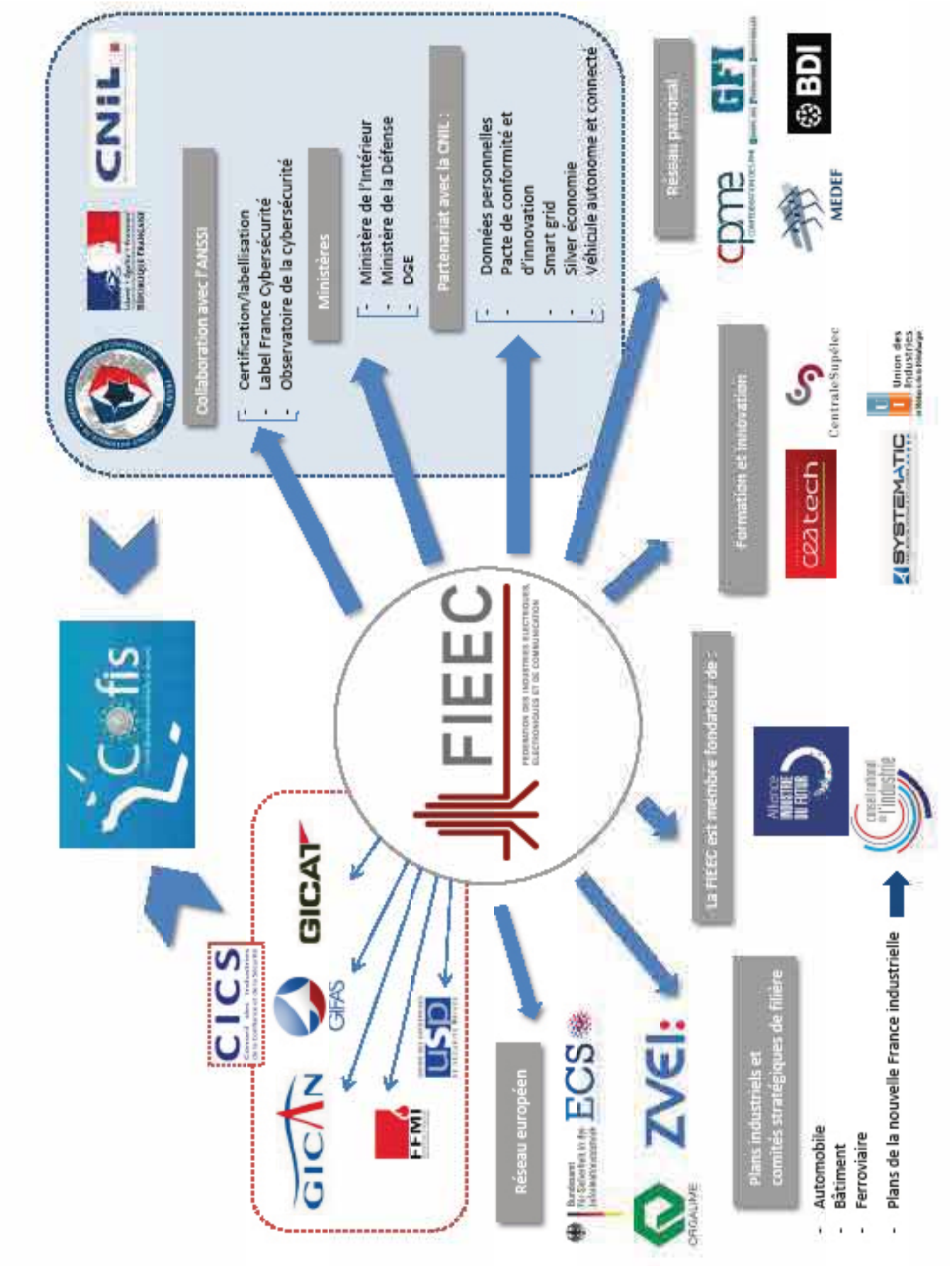
Une action concertée, enfin, de plus grande proximité entre les acteurs pour que l'excellence française des industries numériques puisse se développer dans les meilleurs conditions possibles.

La participation et l'engagement fort des acteurs de notre profession dans les différentes instances administratives et gouvernementales, en lien avec les sujets numériques ou de sécurité, atteste de cette évolution qui soulève de nombreuses questions et/ou enjeux tels que les besoins en formation au numérique, la *blockchain* ou encore le droit à l'expérimentation.

Dans ce cadre, il semble important de ne pas perdre de vue un axe de synergie puissant : l'innovation est une force et un atout stratégique pour notre pays et nos entreprises, leur compétitivité et leur rayonnement international. Nous avons la conviction que celle-ci est compatible, non seulement avec la légitime protection des données personnelles, mais aussi avec les enjeux de sécurité numérique.

A tous les acteurs (entreprises, Organisations professionnelles, Autorités chargées de la réglementation, …) de travailler ensemble pour établir le corpus de règles et comportements cohérent avec ce double enjeu en apparence contradictoire, mais qui, fondamentalement, ne l'est pas. C'est bien cette collaboration active qui nous permettra de relever les défis de la formidable période que nous vivons en s'inscrivant dans la durée.

Cartographie - L'engagement de la FIEEC dans la sécurité numérique



PARTIE 1 :

Les outils à disposition

De quoi parle-t-on ?

Dans notre société, l'identité nous personnifie et nous différencie des autres individus. Propre à chacun, l'identité est une des composantes majeures des droits de l'homme : elle justifie l'exercice de droits et le respect de devoirs. Elle peut se matérialiser par des documents : un passeport, une carte d'identité, un acte de naissance. L'identité recouvre l'identification d'une personne : qui est-elle ? et l'authentification de cette personne : est-elle effectivement la personne qu'elle prétend être ?

L'identité numérique peut quant à elle se définir comme le lien technologique entre l'identité réelle d'une entité (personne, organisme, entreprise ou objet pour définir les relations objets/humain ou objet/objet) et son identité virtuelle (sa représentation numérique). L'enjeu réside dans ce cas dans l'authentification de ce lien et dans le niveau de sécurité lié à cette authentification.

Ainsi, l'authentification fait appel à des facteurs de différents types liés à l'identité de la personne. Il peut s'agir d'éléments connus seulement de la personne (identifiant/mot de passe, code PIN,...), d'éléments possédés par la personne (une carte à puce, un certificat,...) ou encore de caractéristiques intrinsèques à la personne (empreinte digitale, forme du visage,...).

Dans la mesure où les méthodes d'authentification ci-dessus ne s'appliquent pas aux objets, l'identité de ces derniers se développe en se basant sur d'autres systèmes relationnels cryptographiques ou autres.

Plus le nombre de facteurs requis pour l'authentification est important, plus la sécurité de l'identité est renforcée. Ainsi, l'authentification des personnes est dite « forte » lorsqu'elle associe au moins deux de ces types de facteurs et qu'au moins l'un des deux n'est pas rejouable (c'est-à-dire ne peut pas être utilisé s'il est issu d'une interception entre l'utilisateur et le serveur). Pour les objets, une authentification forte est basée sur une identité qui n'est pas falsifiable et une communication cryptée.

Unique, l'identité peut donc être convoitée : vol de données personnelles ou encore usurpation d'identité, les menaces planant sur elle sont nombreuses. Son rôle est d'autant plus important que les transactions numériques et électroniques se multiplient : près de 80% des français sont connectés*(1), 835 millions de transactions en ligne ont été observées en 2015 en France*(2), environ 40% des français sont présents sur les réseaux sociaux*(3). Et les procédures en ligne se multiplient : dématérialisation des procédures administratives, consultation de nos comptes bancaires, paiement de nos factures en ligne, achats électroniques, etc. On constate ainsi une multiplication des données personnelles, plus ou moins sensibles, sur internet. Tous ces éléments constituent autant de traces de notre identité, parfois indélébiles, laissées sur la toile qui peuvent faire l'objet d'attaques numériques. S'assurer de la sécurité de l'identité numérique et adapter le niveau de sécurité et d'authentification en fonction de la sensibilité de l'usage est donc aujourd'hui primordial pour protéger l'identité numérique des personnes.

Il est de même pour les objets. De plus en plus d'objets sont connectés à internet et donc possèdent une identité numérique qui pourrait être détournée afin de réaliser des cyber-attaques. Cette identité numérique des objets est fondamentale pour authentifier les données générées par ces objets.

**(1) et (2) Selon une étude réalisée par la Fédération professionnelle du e-Commerce*
**(3) Selon une étude réalisée par l'institut eMarketer*

L'usurpation d'identité, principale menace à l'identité numérique

La multiplication des transactions numériques étend le champ d'attaque des pirates cyber. Ces attaques sont d'autant plus conséquentes qu'elles ne visent pas uniquement les citoyens mais également les entreprises et les administrations. Ces attaques peuvent être multiples : vol de documents d'identité, détournement de fonds sur internet après avoir récupéré les données confidentielles bancaires, utilisation de l'image physique suite à la publication de photos sur internet etc.

Les entreprises sont elles aussi victimes de telles attaques. On a pu observer le cas de l'usurpation d'identité de dirigeants d'entreprises : piratage des systèmes informatiques puis envoi de courriers contenant de fausses informations aux collaborateurs de l'entreprise, aux organismes financiers avec lesquels elle pouvait interagir ou encore au grand public via les médias.

Les services étatiques ont également été la cible des pirates cyber : le ministère français de la Défense a ainsi déclaré avoir fait l'objet de 24 000 cyberattaques en 2016 dont un certain nombre visaient à nuire à l'image et la réputation du ministère*.

Les conséquences de telles attaques sont considérables, elles peuvent être d'ordre financier, commercial ou moral : la réputation d'un individu peut être ternie, des entreprises peuvent voir leurs actions chuter en bourse, la logistique d'un service étatique peut être troublée etc.

C'est pourquoi il est aujourd'hui essentiel de recourir à des outils de sécurisation de l'identité numérique et d'élever ainsi le niveau de sécurité légitimement attendu par les utilisateurs.

** http://www.opex360.com/2017/01/08/le-ministere-francais-de-la-defense-ete-vise-par-24-000-cyberattaques-en-2016/*

La biométrie, un moyen de protection efficace de l'identité numérique

La biométrie est un outil efficace de protection de l'identité numérique des personnes. A la différence d'autres modes d'identification et d'authentification, elle ne repose pas sur les connaissances de l'usager (nécessité de communiquer un identifiant, un mot de passe ou de répondre à une question de sécurité) ni sur des éléments que l'usager a en sa possession (une carte d'identité, un passeport, un acte de naissance) mais sur le principe de reconnaissance des caractéristiques physiques et/ou comportementales. Ainsi, on peut s'identifier à l'aide d'une empreinte digitale, d'un iris, d'un visage, d'une odeur corporelle ou encore grâce à la voix ou même la démarche ou le comportement. L'objectif de la biométrie

est de permettre l'identification d'une personne. Elle comporte en principe un niveau très élevé de fiabilité puisque les caractéristiques qu'elle utilise sont biologiquement permanentes donc uniques et propres à chacun.

La biométrie est déjà ancrée dans notre quotidien. En France, depuis juin 2009, tous les passe-

ports délivrés sont des passeports biométriques. Ils comportent notamment des données relatives à l'état civil, une photo d'identité et deux empreintes digitales. Depuis quelques années, les fabricants de smartphones se sont également emparés de cet outil : l'usager peut ainsi déverrouiller son appareil à l'aide de capteurs d'empreintes digitales intégrés. Autre exemple, les aéroports ont également recours à ce dispositif pour identifier plus facilement et plus rapidement les passagers. Et les entreprises l'utilisent elles aussi notamment pour restreindre l'accès à certains bâtiments sensibles ou à des fichiers confidentiels. La biométrie est ainsi inscrite dans notre vie de tous les jours et bénéficie à l'ensemble des acteurs : étatiques, industriels, citoyens.

La signature électronique, un mode de preuve sûr de l'identité numérique

La signature électronique est un moyen d'identification numérique dématérialisé. Elle permet à toute personne de signer numériquement un document, de façon officielle, et de réaliser une transaction entièrement en ligne. La signature électronique est un moyen de preuve sûr, elle assure de manière sécurisée, l'identité et l'authentification d'une personne, l'intégrité de la transaction, et la non-répudiation du document signé électroniquement. C'est un tiers de confiance qui délivre un certificat numérique à l'émetteur de la signature électronique. Il peut être logiciel : envoyé sur un ordinateur ou un smartphone par l'organisme de certification ou matériel : dans une carte à puce ou une clef USB. De nombreuses entreprises utilisent aujourd'hui ce mode d'identification numérique : un employé peut ainsi signer électroniquement son contrat de travail. Pour cela, un code à renseigner peut lui être envoyé par SMS ou par mail, pour valider la signature électronique. Ce code est le certificat numérique, il assure qu'aucune donnée n'a été modifiée.

De nombreux systèmes de signature électronique sont ainsi mis en place. C'est pourquoi l'Union Européenne ouvre ainsi la voie vers une harmonisation de l'utilisation de la signature électronique par le règlement « *electronic IDentification And Signature* » dit règlement eIDAS. Entré en vigueur le 1er juillet 2016, son objectif est de mettre en place un environnement réglementaire fiable permettant des interactions sécurisées entre les entreprises, les citoyens et les autorités publiques. Ce cadre juridique autorise la reconnaissance mutuelle des moyens d'identification utilisés par les Etats membres de l'Union Européenne (ce champ s'applique uniquement au secteur public) dans un objectif de sécurité numérique, de simplification et de réduction des coûts.

Cette même infrastructure de signature électronique peut être utilisée comme un moyen d'authentifier l'identité numérique des objets physiques.

Points de vue

Philippe Vallée,
Directeur Général de GEMALTO

« La protection de l'identité numérique est un des enjeux sociétaux et économiques majeurs de la prochaine décennie. Aujourd'hui, l'identité régalienne des citoyens est bien protégée, en particulier grâce à la technologie biométrique. Il n'en est pas de même lorsque les usagers d'un service commercial en ligne s'identifient la première fois et s'authentifient par la suite. Or, la digitalisation de l'économie et des services va s'intensifier dans les années à venir. Les interactions entre les fournisseurs de services et leurs clients se font de plus en plus à travers un PC, un smartphone ou une tablette que par un contact physique. S'assurer que son identité numérique est bien protégée et reste intègre, pouvoir prouver qui l'on est, seront d'un côté la préoccupation des usagers ; Etre sûr que l'usager qui se présente en ligne est bien celui qu'il prétend être sera le souci du fournisseur de services. Notre profession permettra de répondre efficacement à ces enjeux grâce à une combinaison habile et adaptée au contexte de technologies d'authentification et de vérification d'identité, telle que la biométrie qui, dans le futur, s'étendra beaucoup plus à des applications commerciales. De plus, la généralisation de la mise en œuvre de l'identité numérique régalienne dans les services commerciaux permettra à l'Etat de monétiser ses investissements dans la gestion de l'identité. Le modèle dans lequel l'Etat protège et est garant de votre identité numérique, à l'instar de votre identité dans le monde physique, est à mon sens une opportunité unique de fédérer la mise en œuvre de la confiance numérique. L'Estonie est une référence en la matière, cherchons à nous en inspirer ! »

Didier Lamouche,
Président du directoire d'OT-MORPHO

« Notre environnement actuel exige davantage que de simples solutions d'authentification. Alors que nous sommes de plus en plus mobiles et que les transactions gagnent en complexité dans les domaines privé et public, savoir qui est réellement derrière un compte ou un identifiant est devenu une nécessité absolue. Et l'identité digitale ne concerne pas uniquement les personnes. Dans l'internet des objets, il y a un besoin urgent d'identification pour les objets en question, ainsi que pour les utilisateurs y accédant à distance. Lorsque des identités digitales de confiance sont au cœur d'une société connectée, elles forment le socle d'un écosystème dont toutes les parties prenantes - citoyens, entreprises, gouvernements - bénéficient. »

Jean-Pierre Massicot,
PDG d'ADVANCED TRACK&TRACE

« L'identité numérique : un lien nécessaire entre les mondes numérique et physique

La notion d'identité numérique recouvre différentes réalités. Parmi celles-ci un nouveau savoir-faire est apparu : la création de containers de données graphique sécurisés garantissant l'intégrité des données et leur authenticité. Au cœur des évolutions technologiques majeures en cours dans le monde de l'identité numérique, se pose la question des représentations graphiques sécurisées de l'identité. Déjà présent utilisées sur des certificats, permis de conduire ou autorisations diverses, les champs d'application de ces représentations graphiques se multiplient.

S'agissant d'une technologie disruptive, nous sommes forcément aimantés vers les projets de ruptures : identité digitale respectueuse des libertés et de la vie privée, échanges de mobiles à mobiles, d'objet connecté à objet connecté ou au réseau, validations sécurisées hors des infrastructures connectées habituelles et souvent en mode off-line etc… L'arrivée de l'outil sous forme d'un cachet électronique visible est un point marquant dans ce domaine.

L'identité numérique aborde donc les prochaines décennies avec une approche multi support, multi canal… et multi règlements. L'environnement règlementaire normatif, sécuritaire et protecteur des libertés sont de formidables incitation à l'innovation et au renouvellement des outils et des pratiques.

Parmi les grandes innovations déjà à l'œuvre, la première serait naturellement le cachet électronique visible (CEV), équivalent dans le monde physique du cachet serveur du monde numérique, innovation que promeut la toute jeune Association Internationale de Gouvernance du Cachet Electronique Visible - AIGCEV, lancée en France par la Fédération Nationale Des Tiers De Confiance (FNTC) en collaboration et participation de la Mission de Délivrance Sécurisée des Titres (MDST - Ministère de l'Intérieur), l'Agence Nationale des Titres Sécurisés (ANTS) et la Délégation Nationale à la Lutte contre la Fraude (DNLF). Enfin un pont existe entre les 2 mondes qui s'ignoraient quelque peu : le numérique et le physique. Les informations restent garanties et l'émetteur certifié alors même que le contrôle peut être offline sans recours à une infrastructure connectée. Un autre exemple pourrait être l'échange pair à pair de données confidentielles autour de l'identité numérique, échanges maitrisés et traçables via des représentations graphiques à lecture automatisée facilitant la communication. Sécurité, simplicité, vitesse et bas coûts seront les clés du succès d'adoption de ces changements ! Grâce à cette approche, pour la première fois il est aussi possible de manière simple, de vérifier physiquement l'authenticité de l'objet (« est-il vraiment qui il prétend être ? ») auquel on s'adresse numériquement. »

De quoi parle-t-on ?

La cybersécurité peut se définir comme l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles(1). La cybersécurité est un sujet d'autant plus vaste qu'il est lié à trois grands mondes : celui de l'IT (*Information Technology*), de l'OT (*Operational Technology)* et de l'IoT (*Internet of Things*). La numérisation et l'interconnexion croissantes de l'ensemble des activités humaines entraînent corrélativement une exposition accrue au risque de cyberattaques qui peuvent viser aussi bien des entreprises (en France en 2016, on a dénombré près de 11 incidents de cyberattaques par jour soit une perte financière estimée à 1,5 millions d'euros par entreprise(2)) que des Etats (en novembre 2016, une cyberattaque massive a privé le Liberia d'accès internet pendant plusieurs heures). C'est pourquoi, la cybersécurité est désormais un enjeu stratégique pour les utilisateurs et les opérateurs de systèmes d'informations face auquel les chercheurs et les entreprises de la confiance numérique proposent toujours plus d'outils de sécurité innovants.

(1) Source : ANSSI
(2) Source : Etude réalisée par PWC « The Global State of Information Security Survey 2017 »

La cybersécurité : des menaces motivées par divers objectifs

On peut classer les nombreux types d'attaques cyber en trois catégories d'objectifs visés : l'attaque de type crapuleux, idéologique et/ou stratégique.

L'objectif d'un acte crapuleux peut être le vol de données, le chantage ou encore la demande d'une rançon. La « rançongiciel » ou encore « *ransomware* » est une technique de cyber attaque très répandue qui consiste à envoyer à la victime un logiciel malveillant qui chiffre l'ensemble de ses données. En échange du retrait de ce logiciel, le commanditaire de l'attaque cyber demande une rançon ou toute autre information comme un mot de passe ou un identifiant à la victime. Ce logiciel malveillant circule généralement au travers de faux emails par « hameçonnage » ou « *phishing* », technique qui consiste à faire agir l'utilisateur contre son intérêt (en cliquant sur un lien, ouvrant une pièce jointe, fournissant des informations sensibles…) et lui faisant croire que le mail provient d'un destinataire sûr

(comme l'administration, une banque etc.) alors qu'il provient en fait d'un hacker. Selon une étude récente*, près de la moitié des entreprises dans le monde a subi une attaque par *ransomware* au cours des 12 derniers mois. Les conséquences de ce type d'attaques a ainsi conduit 67% des entreprises à augmenter leurs dépenses en cybersécurité. On peut par ailleurs observer la montée en puissance d'une véritable mafia financière : les hackers peuvent avoir une force de frappe relativement large, toucher l'ensemble des acteurs économiques ; et tirer des revenus importants de ces attaques.

L'acte crapuleux peut également prendre la forme de la dénaturation d'un site, d'une attaque par déni de service ou du vol et de la publication de données sensibles. En 2013, 2016 et 2017, Yahoo a ainsi fait l'objet d'un vol massif de données. Ces cyberattaques ont mené à la collecte d'informations confidentielles sur plus d'1 milliard d'utilisateurs. Ces données constituent une denrée précieuse pour les pirates qui leur permettent ainsi d'accroître l'efficience de leurs attaques. Par exemple, un pirate peut récupérer les dates et lieux de naissance des utilisateurs pour les insérer dans un mail et se faire passer pour un tiers de confiance (une banque, un collègue etc.).

Une attaque peut également être de nature idéologique. Dans ce cas, la motivation des pirates n'est pas nécessairement pécuniaire et leurs actions ne sont pas menées dans le but de collecter des informations mais bien dans l'objectif de revendiquer leur désaccord et de punir leurs cibles, par exemple en rendant publiques leurs données confidentielles ou en bloquant leurs systèmes. Le groupe de hackers « Anonymous » mène ainsi des opérations de « désobéissance civile » en ayant notamment attaqué et bloqué plusieurs sites internet dans le cadre d'actions militantes.

Finalement, une cyberattaque peut être stratégique voire géopolitique, en vue d'espionner, de saboter ou encore de perturber des structures, des réseaux, voire des pays. On voit ainsi augmenter le risque de cyberterrorisme notamment à l'égard d'infrastructures liées à l'énergie ou au transport mais également à l'égard des Etats dont les infrastructures critiques deviennent les cibles des hackers. Ces attaques peuvent d'ailleurs être interétatiques : en 2016, l'Ukraine a ainsi soupçonné la Russie d'avoir mené une cyberattaque ciblant l'aéroport de Kiev. En France, ces nouvelles menaces sont prises en compte à travers notamment la mise en place de nouvelles obligations de protection et défense informatique, imposées aux Opérateurs d'Importance Vitale (OIV) prévues par la loi de Programmation Militaire.

**Etude réalisée par le cabinet Vanson Bourne.*

Des outils performants capables de répondre à chaque étape d'une cyberattaque

Les fournisseurs de services, les éditeurs de logiciels ou encore les offreurs de solutions sont des acteurs clefs en matière de cybersécurité. En France, dans le domaine de la confiance numérique et de la cybersécurité, nous disposons d'un tissu de laboratoires reconnus et d'entreprises dotées de compétences larges composé à la fois de grands groupes et de PME agiles et dynamiques. Cet ensemble offre un panel de compétences extrêmement précieux et permet à notre pays de faire partie des leaders mondiaux dans ce domaine stratégique. Les outils sont ainsi disponibles pour les usagers, les entreprises ou les administrations afin de limiter les risques de cyberattaques. Ils sont au cœur de la cybersécurité et permettent d'assurer la prévention, la détection et la réaction face aux menaces.

Une cyberattaque de haut niveau résulte d'un long processus qui peut commencer bien en amont de la détection de l'intrusion d'un logiciel malveillant et de la réalisation de l'objectif poursuivi par le pirate. Celui-ci peut d'abord préparer l'attaque en collectant de nombreux renseignements ouverts sur sa cible, voire en testant la sécurité des réseaux, les faiblesses de ses logiciels, d'un site ou encore la protection d'équipements industriels sans que la cible ne s'en rende compte. Cette étape de reconnaissance intervient avant l'étape de l'intrusion et de l'infection effective recherchée. Le résultat d'une

cyberattaque peut n'être réellement visible que des semaines, des mois voire des années après que l'intrusion malveillante ait eu lieu. Cela a pour conséquence de compliquer la continuité des activités d'une entreprise qui n'a pas su détecter au plus tôt une cyberattaque. Pour améliorer la capacité des entreprises et administrations à résister aux cyberattaques, des actions de cyber-résilience peuvent être mises en place. Cet état de cyber-résilience permet d'anticiper les crises et de résister à ces phénomènes imprévus en maintenant l'organisation et les activités d'une entreprise dans un contexte de crise. Pour anticiper les attaques, des actions de type organisationnel peuvent être mises en place : des mesures d'hygiène informatique peuvent être préconisées à l'égard des collaborateurs de l'entreprise. Des outils de sécurité tels que les antivirus, les pare-feux, les sondes de détection/prévention, le contrôle d'accès, le chiffrement, les outils d'analyse de vulnérabilité etc. peuvent réduire le risque de contamination par un programme malveillant (type vers, virus, chevaux de Troie, etc.), et les évaluations des logiciels installés permettent d'en détecter et d'en corriger les faiblesses. Quand le pirate s'est introduit dans les systèmes et les équipements de l'entreprise mais que l'objectif final ne s'est pas encore réalisé, le but pour l'entreprise est alors de pouvoir connaitre l'intensité de l'attaque grâce à des outils de détection et de procédures d'analyses pour l'aider dans sa décision et de connaitre les moyens à mettre en œuvre pour diminuer l'impact de la cyberattaque. Lorsque l'objectif poursuivi par les pirates est déjà réalisé, d'autres actions peuvent être opérées : ainsi, face à une demande de rançon suite au chiffrement de données, l'entreprise peut par exemple récupérer les sauvegardes (pour autant qu'elles aient été faites) ou s'efforcer de décrypter les informations atteintes, grâce au concours de spécialistes en cybersécurité.

Les technologies et les équipements en sécurité numérique sont toujours plus innovants, ils évoluent et s'adaptent pour être utilisés dans les environnements exposés. Ces nouveaux outils permettent d'accroître la capacité de prévention, de détection et de réaction aux cyberattaques afin d'identifier les acteurs malveillants et réagir au plus vite. Ils ont une capacité d'action pour pouvoir stopper la cyberattaque, la neutraliser et éliminer ses effets et permettent ainsi de pallier les troubles causés à travers des attaques numériques.

Instaurer la confiance numérique en changeant les mentalités

Les cybermenaces sont grandissantes et deviennent de plus en plus structurées, il est essentiel de prendre conscience de ces enjeux de cybersécurité afin d'assurer la confiance numérique, un des attributs majeurs du monde digital.

Il n'y a en effet pas de transformation numérique sans confiance dans les réseaux et les infrastructures. L'arrivée massive des objets connectés dans le quotidien des citoyens et des entreprises a considérablement augmenté les risques d'intrusion et introduit de nouvelles vulnérabilités. L'ensemble des acteurs est concerné, la cybersécurité est multidimensionnelle et nécessite une approche systémique. Les cadres réglementaires et législatifs doivent également être adaptés en conséquence pour intégrer cette dimension cybersécurité dans tous les domaines et dès la conception de chaque produit et projet (*security by design).*

Cette sécurisation ab initio est d'autant plus nécessaire qu'elle conditionne la confiance des utilisateurs, qui est la condition essentielle du développement du numérique. Cette confiance passe notamment par une sensibilisation de tous les utilisateurs sur les risques de cybersécurité et les outils existants. Cette confiance peut également être confortée par des dispositifs tels que des labels et des certifications qui attestent d'un certain niveau de protection des produits, services et solutions. Ainsi, même si la sécurité absolue ne peut jamais être garantie en matière d'informatique, la mise en œuvre de produits, services et solutions ainsi labellisés ou certifiés apporte néanmoins un niveau élevé de robustesse aux attaques. Plus particulièrement, dans le monde professionnel, il est ainsi essentiel de développer la culture cyber au sein des entreprises afin de sensibiliser les salariés à l'utilisation prudente des technologies et de diffuser à tous les publics les règles d'hygiène informatique pour diminuer les risques d'atteinte à la cybersécurité. Car au-delà de l'ensemble des dispositifs technologiques existant et pouvant être déployés, le facteur humain et les habitudes des salariés constituent encore la principale faille dans la plupart des cyberattaques.

Points de vue

Marc Charrière,
Président de la Commission Numérique de la FIEEC

« Un socle numérique de qualité et pérenne constitue une condition essentielle au développement des nouveaux usages. Compte tenu de l'intensification des flux qui transitent sur les infrastructures numériques, leur sécurité devient un enjeu majeur pour les entreprises, les administrations et les citoyens. La tendance à la numérisation des infrastructures, notamment la migration du socle vers le cloud, va accentuer fortement la nécessité de relever ce défi. Pour y faire face, les industries numériques d'excellence de la FIEEC ont un savoir-faire important, au bénéfice de la confiance numérique. »

Jean-Noël de Galzain,
PDG de WALLIX
Président d'HEXATRUST

« Nous vivons actuellement une révolution numérique qui bouleverse nos usages autant que nos organisations ou nos modes de vie. En tant qu'acteurs et/ou utilisateurs nous devons nous adapter rapidement dans un contexte où la technologie a autant d'importance que l'accompagnement au changement.

Dans ce cadre, les entreprises doivent faire face à des défis majeurs tels que la gestion des risques dans la transformation numérique de leur organisation, la prévention des fuites de données, et la mise en conformité avec les réglementations, en particulier NIS et RGPD. La Cybersécurité et la Confiance numérique sont essentiels pour bâtir des espaces numériques de confiance.

Plus largement, des besoins nouveaux émergent autour des systèmes financiers, des systèmes de santé de demain, de l'industrie connectée et la protection des systèmes industriels, la gestion intelligente de l'énergie et les smart cities, l'industrie des télécoms et les opérateurs de cloud public, enfin bien sûr la Cyber Défense et la protection des données utilisateurs collectées en masse. Ils nécessitent des moyens de Cybersécurité modernes aptes à s'adapter aux nouvelles technologies du cloud, de l'Internet des Objets, des big data ou de l'IA dont ils sont partie intégrante. C'est le concept de «privacy by design», un nouveau standard de qualité qui s'impose au monde entier où la cybersécurité devient un facteur clé de succès.

Dans ce contexte, notre mission est d'aider les entreprises à prévenir les fuites de données, reprendre la main sur la gestion des mots de passe de leur système d'information, enfin les aider à se mettre en conformité avec les réglementations NIS, LPM/OIV et RGPD. Développées à partir de technologies de traçabilité des connexions réseaux, les solutions que nous proposons permettent à chacun d'étendre son activité avec le numérique, tout en conservant les clés du royaume ! »

Alexis Caurette,

Vice-Président ESCO (European Cyber Security Organisation)
Global head of Consulting & Integration, Cybersecurity Business Line, ATOS
Vice-président d'ACN, Président du GT2 Cybersécurité

La consolidation de la représentation du secteur : un enjeu clé pour l'avenir

« La cybersécurité est devenue une clé incontournable de la transformation numérique tant il est vrai que celle-ci ne pourra se réaliser sans confiance. La France dispose dans ce domaine d'atouts majeurs et notamment d'un tissu industriel et technologique de premier ordre, composé à la fois de grands groupes mais aussi de PME et d'ETI de pointe. L'enjeu majeur de notre profession est d'agir collectivement pour que notre voix soit entendue dans les travaux législatifs et réglementaires qui foisonnent tant au niveau européen que français. C'est aujourd'hui que notre cadre d'action se décide et il est impératif que nous parvenions à nous structurer pour répondre à cet enjeu. L'initiative menée par l'ACN (Alliance pour la Confiance Numérique) visant à proposer une large consolidation et une représentation institutionnelle unifiée pour toutes les entreprises du secteur, grandes ou petites, est en ce sens une réponse pertinente à cet impératif stratégique. Au-delà du niveau national, il est également primordial que nous unissions nos forces pour porter nos propositions de concert avec nos partenaires européens et peser efficacement auprès des instances officielles (Parlement, Commission) mais aussi dans les initiatives jouant un rôle crucial dans l'avenir de nos professions et de nos marchés, telles que le cPPP cybersécurité porté par ECSO. Il en va de notre avenir : nous avons toutes les cartes en main pour participer à son élaboration et il nous appartient de saisir cette opportunité. »

Philippe Blot

Chef de la division Produits et services de sécurité de l'ANSSI

« Les menaces croissantes liées à l'usage des technologies du numérique et au développement des objets connectés dans tous les secteurs d'activités, imposent aujourd'hui à l'ensemble des acteurs économiques d'intégrer les critères de sécurité et de confiance dans leur mode de consommation et de sélection des produits et services auxquels ils recourent.

Les actions de sensibilisation de ces acteurs à la prise de conscience des enjeux liés à la sécurité du numérique doit aujourd'hui impérativement s'accompagner d'une offre de solutions associée, dont le niveau de robustesse devra être attesté par des labels ou certifications émis par les autorités compétentes et reconnus à l'échelle nationale, européenne, voire internationale.

Or, la France dispose d'un cadre très favorable dans le domaine de la certification de sécurité : concernant les produits, la certification basée les critères d'évaluation internationaux pour la sécurité des technologies de l'information (critères communs), s'est enrichie par une certification plus abordable en terme de coûts et délais (certification de sécurité de premier niveau – CSPN – délivrée par l'ANSSI) ; dans le domaine des services, la qualification de prestataires connait un succès croissant, comme en témoigne la qualification actuelle de près 25 prestataires d'audit de la sécurité des systèmes d'information et l'entrée en phase opérationnelle des schémas de qualification de prestataires de nouveaux services (détection, réponse aux incidents, services d'informatique en nuage).

Les challenges qui se présentent aujourd'hui à nous concernent ainsi, d'une part, le passage à l'échelle de la certification : à l'heure des objets connectés, il est indispensable de pouvoir démultiplier les activités de certification sans sacrifier la confiance devant être apportée à l'utilisateur. D'autre part, la reconnaissance internationale de nos labels, prioritairement à l'échelle européenne. Là encore, les acteurs industriels français jouent un rôle crucial pour relayer l'action de l'Etat sur la scène internationale en assurant la promotion des certificats délivrés par l'ANSSI et en participant activant aux travaux de normalisation destinés à définir le dispositif européen de certification. »

De quoi parle-t-on ?

La sécurité numérique est un des enjeux de la sécurité des bâtiments, de leurs occupants et des biens qui s'y trouvent.

Cet environnement peut en effet être la cible d'attaques motivées par de multiples raisons : symbolique, économique, politique, écologique ou encore en raison du public que les bâtiments peuvent accueillir.

Du contrôle d'accès, en passant par la vidéosurveillance et les systèmes d'éclairage de sécurité qui permettent l'évacuation sûre et rapide de ses occupants, les électrotechnologies offrent un large éventail de dispositifs de sécurité à disposition des entreprises et des individus.

L'enjeu de la sécurité est fondamental et permet de renforcer la confiance des occupants et des visiteurs dans les bâtiments industriels et publics, ou encore dans les logements collectifs et individuels.

Sécurisation de l'accès au bâtiment grâce aux dispositifs de contrôle d'accès

Pour assurer le contrôle de l'accès aux bâtiments, un dispositif électronique doit pouvoir être mis en place à l'entrée de la structure. L'exemple typique du système de contrôle d'accès est le clavier codé (communément appelé digicode). Ce clavier est un système de sécurité permettant de verrouiller et de déverrouiller une porte grâce à la saisie d'une combinaison de symboles. Les dispositifs de contrôle d'accès peuvent permettre également de s'assurer de l'identité d'une personne grâce à différents éléments distinctifs (badge, carte à puce) ou biométriques tels que la voix, la vidéo (reconnaissance visuelle), les empreintes digitales, oculaires, etc. Lorsque le contrôle d'accès est associé à un dispositif d'identification, il permet en outre de donner accès à une zone de manière différenciée selon les personnes et d'assurer une traçabilité des passages.

L'installation de systèmes de contrôle d'accès permet d'assurer la sécurité des individus et des biens situés à l'intérieur du bâtiment en limitant l'entrée aux seules personnes autorisées. Ces solutions sont souvent installées en complément d'autres services pour prévenir d'une intrusion : par exemple, lorsqu'un individu a composé un code erroné à plusieurs reprises, un signal ou une alarme peut prévenir de la tentative d'accès au bâtiment.

La vidéosurveillance et la détection d'intrusion

La sécurité des bâtiments et des logements résidentiels et professionnels, publics ou privés, peut être assurée par des moyens de détection d'intrusion et de surveillance tels que les systèmes de vidéosurveillance. Ce type d'installation est composé d'un ensemble d'équipements et de systèmes permettant de prévenir des attaques physiques et matérielles. L'installation de systèmes de vidéosurveillance a un effet dissuasif pour prévenir les intrusions. En cas d'attaque, elle permet de réagir rapidement et de déclencher les actions appropriées en coordonnant l'intervention des services de sécurité. Si l'attaque a déjà été réalisée, la vidéosurveillance permet de visualiser rapidement les faits et d'apporter des éléments de preuve de l'infraction et d'identification des auteurs grâce notamment aux enregistrements vidéo.

Ce type de système est composé de caméras connectées à des moniteurs ou des ordinateurs localement

ou à distance ; ces systèmes utilisent le plus souvent des réseaux IP pour communiquer. L'utilisateur peut alors consulter les informations délivrées par les caméras depuis n'importe quelle connexion Internet sur un ordinateur ou un smartphone.

Afin de garantir une sécurité maximale, le dispositif de surveillance est sécurisé pour éviter tout risque d'attaque.

Sécurisation interne des bâtiments et de ses occupants via le système d'éclairage de sécurité

L'évacuation des personnes est complexe et s'opère souvent dans un climat anxiogène. Elle survient pour des causes multiples et fréquentes : coupure de l'alimentation électrique, défaillance de l'éclairage, incendie, alerte à la bombe, attaque terroriste, risques naturels (inondation…), risques chimiques…

L'éclairage de sécurité est alors aussi vital qu'indispensable pour la sécurité des personnes.
Il permet de sauver des vies tant son rôle est essentiel pour permettre l'évacuation sûre et rapide d'un bâtiment.

Réalisé à partir de Blocs Autonomes d'Eclairage de Sécurité (BAES) ou de Luminaires alimentés par Source Centrale (LSC), l'éclairage de sécurité assure trois fonctions essentielles à notre sécurité.

Il permet :

- de faciliter l'évacuation efficace des occupants jusqu'aux sorties en balisant les cheminements, les obstacles et les changements de direction et en prévoyant des Dispositifs de Balisage Renforcé pour les Personnes en Situation de Handicap ;
- d'éviter les mouvements de panique grâce à un éclairement minimum des locaux ;
- de réduire les conséquences humaines d'un sinistre en facilitant l'intervention des secours.

Dédiés à assurer la sécurité des personnes et à favoriser leur bonne évacuation si nécessaire, le choix et l'installation des systèmes d'éclairage

de sécurité relèvent de la réglementation liée aux locaux concernés. Leurs caractéristiques répondent à un ensemble de prescriptions normatives et ils doivent être régulièrement testés pour s'assurer de leur bon fonctionnement.

Trois grandes réglementations se distinguent. Pour les immeubles d'habitation, l'arrêté du 31 janvier 1986 modifié dresse les règles à respecter. Les ERT (établissements recevant des travailleurs) sont traités par l'arrêté du 26 février 2003, pris en application de l'article 15 du décret du 14 novembre 1988 relatif à la protection des travailleurs contre les courants électriques. Quant aux ERP (établissements recevant du public), le règlement de sécurité adéquat a été modifié par l'arrêté du 19 novembre 2001. Chaque catégorie de locaux est classée en types et à chacun s'appliquent des règles différentes. Toutefois, les performances demandées des matériels sont globalement identiques.

Points de vue

Pascal Le Roux,
Vice-Président CDVI
Président du Comité de liaison sécurité numérique de la FIEEC

« La sécurité des bâtiments, de ses occupants et de ses biens peut être assurée en amont par des technologies elles-mêmes sécurisées. Celles-ci sont toujours plus innovantes et connectées, notamment en matière de contrôle d'accès électronique. Les systèmes d'accès aux bâtiments constituent en effet de véritables outils de prévention des attaques et des intrusions en permettant de gérer en toute sécurité les flux des personnes et des véhicules dans les différentes zones du bâtiment. Ces systèmes permettent également d'assurer la mise en sécurité ou l'évacuation des occupants au sein des établissements scolaires (action dite PPMS). »

Régis Cousin,
Président de la FFMI (Fédération Française des Métiers de l'Incendie)

« Tous les réseaux sont l'objet de cybermenaces de la part d'Etats, de groupes terroristes ou d'associations criminelles. Le Système de Sécurité Incendie (SSI) ne fait malheureusement pas exception à la règle. Si les risques d'acquisition malveillante de données ou de détournement de certaines fonctionnalités du SSI ne sont pas à négliger, c'est bien la menace de sa mise hors service totale ou partielle qui doit être traitée en priorité. En effet, dans un tel scénario, l'établissement concerné se trouve dépourvu face à un risque exceptionnel, telle une attaque terroriste, comme face au risque premier d'incendie auquel il est exposé. La cybermenace peut donc provoquer une surexposition au risque incendie. Sous l'égide de la Fédération Française des Métiers de l'Incendie, les professionnels travaillent de concert à la prise en compte des risques cyber, avec une seule priorité : la qualité et la fiabilité de la réponse au risque incendie, apportée par le SSI. »

La traçabilité sécurisée

De quoi parle-t-on ?

Dans un contexte de mondialisation, nous assistons à une circulation toujours plus massive des biens et des données. Afin que cette augmentation exponentielle des échanges de toutes natures puisse se dérouler dans les meilleures conditions économiques et de sécurité, des outils de traçabilité de ces flux en temps réel sont désormais nécessaires. La traçabilité permet, via leur identification numérique, de retrouver l'historique, l'utilisation et la localisation de produits, d'activités et de données (personnelles, professionnelles et/ou confidentielles) au moyen d'informations enregistrées. Elle permet notamment de lutter efficacement contre le commerce illicite et la contrebande qui représente près de 10% des échanges mondiaux. Les produits mis sur le marché peuvent en effet faire l'objet de dénaturation ou d'altération à tout moment avant et après leur commercialisation, lors de leur production dans les usines ou encore lors de leur distribution. Les données quant à elles peuvent être indélébiles sur internet et les réseaux. Elles peuvent être utilisées à l'insu de leur propriétaire, être altérées, être vendues ou conservées pour tout autre motif et sans son accord. Associer à des dispositifs d'authentification et de scellé, les différents outils de traçabilité correctement sécurisé assurent un rôle essentiel à travers quatre étapes incontournables : celle d'identifier, d'authentifier, de sceller et de tracer les produits, les activités et les données.

Une traçabilité ainsi sécurisée constitue la clef de voûte pour une confiance accrue des utilisateurs dans les produits et données qui circulent dans le monde.

L'authentification : une étape sine qua non pour déterminer l'authenticité d'un produit ou d'un document

L'authentification consiste pour le consommateur et/ou l'utilisateur à évaluer l'authenticité d'un produit ou d'une donnée, c'est-à-dire sa conformité avec le produit ou la donnée fournie par l'émetteur légitime. A cet effet, le produit ou le document est doté d'un élément authentifiant : objet tangible, caractéristique visuelle et/ou information associée au bien matériel. Pour être efficace, cet élément se doit d'être résistant aux tentatives de falsification ou reproduction et facilement contrôlable, en effet c'est bien le niveau d'usage et la quantité de contrôles réalisés qui déterminent l'efficacité et donc la rentabilité d'une solution d'authentification.

L'authentification peut être assurée via des dispositifs spécifiques dont les caractéristiques varient selon la fonction et l'utilisation du produit ou du document mais aussi selon le public visé (consommateur, distributeur, services douaniers, etc.). Ils sont généralement classés suivant 3 niveaux :

- Les dispositifs de niveau 1 conçus pour être contrôlés par le grand public peuvent ainsi inclure des hologrammes ou des encres spéciales « *Optical Variable Ink* » visibles à l'œil nu.
- Des dispositifs optiques ou digitaux cachés tels que les micro-impressions, les codes résistant à la copie, les marquages invisibles à l'œil sont dits de niveaux 2 : ils nécessitent l'emploi d'outils simples (loupe, éclairage spécifique, mais aussi smartphone).
- Le troisième niveau de sécurité lié à l'authentification d'un produit ou d'un document peut appeler au recours de nano images, d'inclusions dans un produit ou de marqueurs chimiques par exemple.

Sceller un produit : une technique de traçabilité attestant de son origine

Un produit peut être manipulé et/ou altéré entre le moment de sa fabrication et celui de sa distribution à des fins malveillantes : extraction et remplacement ou modification du contenu, re-packaging ou encore dénaturation du produit. Pour pallier ces risques de falsification et de contrefaçon, il convient de vérifier que le produit a bien été scellé.

Cette procédure est rendue possible grâce à des dispositifs spécifiques tels que des étiquettes holographiques codées ou autres dispositifs anti falsification. Le contrôle d'intégrité de ce type d'étiquette collée directement sur le produit peut être réalisé visuellement et/ou automatiquement via des applications par le consommateur ou l'utilisateur puisque toute tentative d'ouverture du produit endommagerait nécessairement l'étiquette. Apposée en fin de chaîne de fabrication par le producteur légitime, elle a pour rôle d'une part, de garantir la fabrication d'origine et son intégrité et constitue, d'autre part, un frein efficace à la copie des produits. Avantageusement, c'est le scellé qui porte les informations d'identification du produit utilisées dans la chaîne de traçabilité.

La contrefaçon d'un produit ou d'un document utilisant un système de traçabilité élaboré est d'autant plus complexe à reproduire qu'il met en oeuvre plusieurs barrières technologiques.

Une collecte efficace d'informations permise grâce au traçage des produits et des données

La traçabilité d'un produit, d'une activité ou d'une donnée court tout au long de sa vie : de sa production jusqu'au consommateur final en passant par toutes les étapes de sa distribution en renseignant à chaque étape de sa localisation des informations importantes telles que le nouveau « détenteur », le reconditionnement…. La nature des outils de traçabilité à utiliser pour accéder à ces informations varie selon plusieurs critères : le destinataire du produit, la nature du produit lui-même et la quantité de produit ou de document conçue et fabriquée. Ces paramètres aident à définir le support adéquat afin de différencier les produits entre eux et de pouvoir collecter des informations. L'outil de référence utilisé dans ce contexte est le code, inscrit en clair ou sous forme de code bidimensionnel comme le *flash code.*

La lecture du code permet d'enrichir puis de vérifier la cohérence du parcours du contenant entre la source (sortie usine) et le point de contrôle dans la chaîne de distribution (sous réserve d'autorisation appropriée). Un code imprimé risque d'être reproduit à l'identique: il doit donc être protégé contre cet acte malveillant par un dispositif d'authentification adéquat (consultation d'une base des données de confiance où en locale, par le biais d'un dispositif du type CEV-Cachet Electronique Visible).

Le code peut également être vecteur d'informations marketing à destination du consommateur final par exemple la fiche d'identité du produit, permettant ainsi la digitalisation d'une partie de l'information à destination du public.

Ainsi le code peut être utile à plusieurs types d'interlocuteurs, du consommateur jusqu'aux services douaniers en vérifiant par exemple l'association du numéro de série de l'étiquette avec le type de produit, sa date de fabrication, etc.

Points de vue

Hugues Souparis,

Fondateur et Président de SURYS

« Le commerce illicite mondial c'est 600 Milliards d'euros, 2ème source de financement du terrorisme. Il est urgent que les Etats, les entreprises et les citoyens prennent les mesures nécessaires pour lutter contre ce fléau, cela relève de notre responsabilité éthique et sociétale. Pour cela 4 composantes indissociables :

1. *Tracer les produits sur la chaine de fabrication, de l'approvisionnement matière au stockage final ;*
2. *Authentifier les produits en circulation, engager les réseaux de distribution et les consommateurs avec des moyens simples et efficaces pour s'assurer de l'authenticité du produit ;*
3. *Tracer le produit dans la chaine de distribution pour éliminer le commerce illicite ;*
4. *Relier le produit et les informations qui le définissent à une base de données indépendante et inaltérable pour remonter les informations aux Etats et Industriels à des fins d'analyse et d'actions préventives et correctives.*

Ces 4 fondements clés de la traçabilité sécurisée ne sont efficaces que si les Etats et les Industriels ne compromettent pas sur la qualité scientifique des éléments d'authentification et d'identification de la solution choisie ; SURYS investit chaque année 10% de son revenu en R&D pour proposer des systèmes de lutte contre la fraude résistants aux contrefacteurs et fraudeurs ; nos étiquettes, scellés holographiques, portent un identifiant sécurisé par des éléments optiques et des algorithmes ; elles donnent aux consommateurs et forces de police la possibilité de vérifier l'authenticité sans outil, ou avec assistance d'un téléphone portable, et d'obtenir ainsi des informations afférentes au produit et à la marque.

Les technologies émergentes de Blockchain viennent renforcer la confidentialité et la sécurité de l'information, faciliter la communication entre les systèmes transnationaux, indispensable à une lutte qui se veut transfrontalière.

Mais seuls les Etats et les Industriels qui acceptent de payer un premium scientifique mettront en place des solutions efficaces ; nous assisterons à ce choix prochainement en Europe et en particulier en France quand viendra le moment en 2018 de décider de la solution de traçabilité sécurisée des paquets de cigarettes dont environ 30% sont estimés contrefaits ou illicites ; seule une solution indépendante des fabricants de tabac, combinant des technologies optiques et numériques, et capable de communiquer entre Etats, permettra de répondre aux enjeux. »

Gilles Barré,

Président de l'AIGCEV (Association Internationale de Gouvernance du Cachet Electronique Visible)

« Le Cachet Électronique Visible (CEV), un nouvel outil au service des industriels.

Authentification, scellement, code, trois mots clés -repris ci-dessus- caractérisent la traçabilité sécurisée. Ces trois mots caractérisent également le CEV.

L'objet initial de ce nouvel outil, qui se présente sous la forme d'un code 2D, est d'authentifier l'émetteur d'un document et de sécuriser les données clés véhiculées par ce document. On voit donc tout de suite que ce nouvel outil, créé pour lutter contre la fraude documentaire, est aussi pertinent dans le champ de la lutte anti contrefaçon. Cet outil, dont la force résulte de l'utilisation d'une signature électronique (cachet serveur), pourrait également être aussi d'une grande pertinence dans la sécurisation de l'internet des objets (IoT). J'invite tous ceux qui ont des cas d'usages qui ressortent de ces problématiques à se rapprocher de l'Association Internationales de Gouvernance du Cachet Électronique Visible (AIGCEV). »

Confiance numérique : des outils aux usages, une filière qui répond aux besoins sociétaux

Par Jean-Pierre Quémard, Vice-Président de la FIEEC, Président de l'Alliance pour la Confiance Numérique (ACN)

La sécurité et la confiance numérique sont des sujets dont l'appréhension est particulièrement délicate tant ils sont étroitement imbriqués avec l'ensemble des développements induits par la transformation numérique. Nous avons choisi de structurer ce document en présentant d'une part les outils qui concourent à la confiance numérique (Partie 1) et d'autre part des exemples concrets de déploiement de cette sécurité numérique (Partie 2), dans lesquels les outils précédemment évoqués sont mis en œuvre en tout ou partie au service d'une application ou d'un domaine qu'il s'agisse du bâtiment connecté, de l'industrie du futur, de la ville intelligente, des transactions ou encore de la santé.

Dans chacun de ces domaines, les outils de la confiance numérique doivent impérativement être intégrés dès la conception c'est la notion de « *security by design* ». La sécurité de l'ensemble repose en premier lieu sur l'assurance de pouvoir compter sur des identités numériques fiables. En se sens, le sujet de l'identité numérique constitue le cœur de la confiance car c'est le point de départ indispensable de toute démarche de sécurisation. Nos industries apportent sur chacun de ces sujets des réponses adaptées à travers les produits, services et solutions développées par un écosystème performant d'entreprises de toutes tailles. La France dispose d'une excellence reconnue dans ce domaine et cela constitue un atout majeur pour l'économie de notre pays mais également pour sa souveraineté en constituant également le socle pour une politique Européenne ambitieuse.

Au-delà de cette réponse opérationnelle, les défis auxquels sont confrontées collectivement nos entreprises sont également législatifs et réglementaires. Les initiatives dans ce domaine sont foisonnantes, en France et en Europe, et il est capital que le secteur structure sa représentation institutionnelle pour que nos messages soient entendus. De même, la prise en compte des libertés individuelles est le complément indispensable à l'acceptation par le citoyen des nouvelles technologies numériques, c'est la notion de « *privacy by design* ».

C'est pourquoi l'ACN (Alliance pour la Confiance Numérique) a entrepris de fédérer largement autour de son action l'ensemble des acteurs du domaine de la confiance et de la sécurité numérique (grands groupes, ETI, PME, laboratoires, ...).

En effet, au-delà des questions de structures, il s'agit désormais de définir ensemble une ambition commune pour notre industrie. Dans le domaine de la cybersécurité par exemple, notre ambition est de parvenir à hisser notre pays parmi les trois ou quatre leaders mondiaux du secteur, en créant les conditions propices à l'épanouissement et au développement de nos entreprises.

Cette ambition passe également par un échange renforcé entre les offreurs de solutions de confiance numérique et les intégrateurs de ces solutions dans leurs propres solutions *smart (smart industrie, smart building, smart health, smart mobility, smart city, …*). En effet, les technologies de sécurité et de confiance de pointe développées par les uns doivent se nourrir des exigences métier des autres pour être parfaitement adaptées aux besoins sociétaux forts, qui sont autant de marchés mondiaux en très forte croissance à deux chiffres. La FIEEC (Fédération des Industries Electriques, Electroniques et de Communication) réunit ces différentes catégories d'acteurs et est donc le creuset pertinent et incontournable pour développer ces actions.

Nous avons désormais toutes les cartes en main pour mettre nos atouts nombreux au service d'une ambition forte. Nos entreprises et notre pays ont un rôle de premier plan à jouer dans le domaine de la confiance et de la sécurité numérique. L'action collective et une structuration forte du secteur seront la clé de nos succès futurs.

ACN
Alliance pour la Confiance Numérique

PARTIE 2 :

Les *use cases*

La safe City

De quoi parle-t-on ?

Aujourd'hui, la ville intelligente prend peu à peu le pas sur la ville traditionnelle. La ville se métamorphose en un véritable espace connecté et interconnecté. Avec près de 7,8 milliards de citoyens urbains d'ici 2020 (prévisions de l'ONU), la sécurisation numérique de cet ensemble devient un enjeu majeur qui réside dans l'accompagnement de la « *smart city* » par la « *safe city* » en assurant l'interconnexion des technologies et la sécurité de tous.

La « *safe city* » s'assimile à une ville connectée et sécurisée, elle se caractérise par plusieurs facteurs clefs tels que la mise en place de systèmes intégrés via des réseaux intelligents, à l'interconnexion des services qui partagent des renseignements, assurer l'ensemble des procédures opérationnelles et de planification. L'objectif de la « *safe city* » pour les électrotechnologies est donc d'instaurer un socle de confiance numérique entre les différents acteurs (les administrations, les industries, les utilisateurs etc.) et secteurs concernés (mobilité, santé, énergie, bâtiments, réseaux etc.). La finalité de ce socle est de permettre une collaboration privilégiée et des actions collectives pertinentes pour échanger des informations, mettre en commun des services et fonctionnalités tout en assurant l'étanchéité nécessaire à assurer la confidentialité des activités et des opérations de chacun. Le raisonnement collectif garantit ainsi une sécurité numérique réfléchie et adaptée aux besoins de la ville intelligente.

Sécurité sociétale : une prise de conscience collective

La « *safe city* » se traduit par un échange des informations en temps réel à l'aide de toutes sortes de données émises par un nombre croissant de capteurs implantés dans la ville et recueillant par exemple des données de trafic, des images de vidéosurveillance, de cartographies interactives, de position des capteurs….

L'interconnectivité des équipements et des logiciels permet le développement de solutions et de services pour accroître la sécurité sociétale.

Ainsi, une personne souhaitant entrer dans un stade, interdite d'accès par les autorités publiques, pourrait être identifiée automatiquement par les équipements de surveillance et se voir refuser l'accès au stade. D'autres infrastructures recevant du public peuvent être sécurisées via des caméras de surveillance intelligentes, pour surveiller par exemple les zones de stationnement réglementées ou les pistes cyclables à proximité d'une sortie d'école et prévenir ainsi des accidents de la route.

La « *safe city* » induit également une meilleure gestion et une sécurité accrue des flux de population dans les villes. Ainsi, à l'occasion d'une manifestation, les solutions et systèmes proposés par les industriels, synchronisés avec les organismes de la ville permettent la prédiction et l'anticipation de perturbations. La ville de Marseille souhaite ainsi recourir à de tels moyens afin de compiler des données numériques et pouvoir gérer au mieux son organisation : l'accès à ces données interconnectées et synchronisées constituent ainsi pour la ville une aide à la décision : anticiper l'effectif du personnel à déployer lors d'une manifestation, faire le choix de déplacer le lieu ou la date d'un événement, savoir quel matériel apporter, etc.

Le succès et l'efficacité des innovations des industriels a déjà été démontré dans certaines métropoles (notamment Mexico) où la combinaison et la gestion centralisée de données issues de divers équipements (caméras, drones ou encore boutons d'alerte installés dans les rues) ont permis d'observer une amélioration sensible sur plusieurs indicateurs de sécurité urbaine : 48,9% de baisse de la criminalité, temps d'intervention suite à un incident passé de 12 à 9 minutes et réduction de moitié des vols de voitures constatés. Cet aménagement est devenu un exemple en matière de « *safe city* ».

Sécurité environnementale : une ville sûre au service du développement durable

Face à une population croissante, les enjeux de sécurité se déclinent également en un volet environnemental. De nouveaux dispositifs electrotechnologiques existent pour permettre de conjuguer au mieux l'urbanisation croissante et la lutte contre les émissions de CO_2.

Là aussi, de nombreux capteurs peuvent être déployés pour mesurer, contrôler et gérer les différents flux urbains en vue d'optimiser leur impact environnemental. Ainsi, des capteurs atmosphériques peuvent être installés, permettant ainsi de délivrer des données et des cartographies en temps réel et faciliter la prise de décision des autorités publiques. Les données délivrées par ces capteurs permettent d'anticiper et de gérer par exemple la circulation des véhicules dans la ville.

L'intégration de nouvelles technologies connectées et sécurisées induit également de pouvoir mettre à disposition de nouveaux modes de

transport sûrs et écologiques, d'installer des éclairages urbains intelligents à basse consommation ou encore de construire et aménager de nouveaux bâtiments en gérant les interactions entre les différents capteurs installés et de mettre en place une approche systémique.

L'éclairage intelligent au service de la ville et de sa population

L'éclairage dans les villes est un enjeu majeur et prioritaire. En effet, les systèmes d'éclairage dans les espaces publics sont nécessaires pour assurer notamment la sécurité de la circulation des habitants ou encore accroître le sentiment de sécurité urbaine. Aujourd'hui, l'éclairage évolue grâce au numérique et devient intelligent. Il permet d'aller au-delà des fonctionnalités qu'il offrait initialement et répond aux enjeux sociaux, environnementaux et budgétaires des villes en développant des solutions toujours plus innovantes et sécurisées au service des citoyens. De nouveaux outils souvent interconnectés peuvent ainsi être mis en place dans les villes. La télégestion et la télémaintenance, par exemple, permettent de gérer l'éclairage public à partir d'un système de gestion centralisée. Grâce aux lampes et lampadaires équipés de « contrôleurs », une carte interactive est ainsi transmise et consultable par ce système de gestion centralisée qui lui permet de commander à distance leur allumage ou leur extinction de manière individuelle ou groupée ou encore de connaitre automatiquement les dysfonctionnements des sources lumineuses et pallier à ces problèmes plus rapidement. Les capteurs de mouvement constituent également une source d'informations considérables pour la ville mise à disposition grâce à l'éclairage intelligent : ils permettent de connaître par exemple la fréquence de passage d'un piéton ou d'un véhicule et d'ajuster les paramètres d'éclairage en conséquence (l'ampoule ne s'allumerait ainsi qu'au passage de l'individu ou de l'objet ou son intensité s'adapterait selon l'heure de passage). Ces nouvelles technologies connectées et interconnectées assurent ainsi de nouvelles fonctionnalités permettant de répondre aux préoccupations de la ville intelligente notamment en termes de sécurité et d'améliorer le quotidien des populations à travers des solutions adaptées et sécurisées. Il est important de signaler que la sécurité de ces nouveaux réseaux est un élément clé car des scénarios catastrophes tel qu'une cyberattaque terroriste pour prendre le contrôle du réseau d'éclairage afin de provoquer un « *black out de la city* » n'est pas que science-fiction.

Points de vue

Laurent Denizot,
CEO d'EGIDIUM

« La digitalisation croissante des espaces urbains rend le développement de solutions de safe city primordial afin notamment d'assurer efficacement la protection de l'ensemble des citoyens et de faciliter l'action des autorités en charge de la sécurité. De nouvelles technologies spécifiques permettent de contribuer à relever ce défi et à rendre la ville intelligente plus sûre face à une densité de population plus élevée et des villes toujours plus mondialisées. Ces technologies aident également les acteurs concernés à appréhender les nouveaux risques urbains, à agir plus efficacement et plus rapidement pour assurer la sécurité de tous. C'est pourquoi il est nécessaire que les autorités publiques intègrent au plus vite cette dimension safe city au cœur de leurs réflexions prospectives et leurs actions de structuration urbaine. »

Marc Darmon,

Directeur Général Adjoint, Systèmes d'Information et de Communications Sécurisés de THALES
Président du CICS (Conseil des Industries de Confiance et de Sécurité)

« Le projet de Système de Sécurité de la ville de Mexico que nous avons déployé est emblématique à plus d'un titre.

Tout d'abord par son effet sociétal et social : depuis le démarrage du projet, la criminalité à été divisée par deux, le temps d'intervention divisé par trois, l'impression de sécurité largement augmentée. La qualité de vie est radicalement transformée, les entreprises reviennent en ville, etc...

Par son côté opérationnel également, toutes les agences de la municipalités (police, samu, pompier, ...) travaillent avec le même système, pour une meilleure performance opérationnelle.

Par son ambition technique, plus de vingt mille caméras, des capteurs et détecteurs de toutes sortes (drones, détecteurs de coups de feu, ...), intégrés autour d'un système de commandement « intelligent » et d'un système de gestion d'appel d'urgence (5 000 par heure !), permettant d'accélérer considérablement la compréhension de l'événement et le choix de la bonne décision.

Par sa capacité d'intégration technologique enfin, les fonctionnalités issues de l'intelligence artificielle et de l'analyse Big Data étant intégrés progressivement (détection d'événement anormaux, traitement vidéo intelligent, ...), grâce à l'ouverture du système. »

Stéphane Mayer,

Président du GICAT (Groupement des Industries de Défense et de Sécurité terrestres et aéroterrestres)

« La safe city n'est pas une ville où policiers et pompiers ont les yeux rivés à des écrans mais une cité dans laquelle des professionnels « augmentés » mettent à profit ces technologies pour simplifier leur activité quotidienne, réduire leurs délais d'intervention, répondre de manière plus ciblée et, au final, pouvoir consacrer plus de temps au dialogue avec les populations qu'ils protègent.

On l'oublie facilement mais la Sécurité est un besoin primaire. Les citoyens ont besoin de se sentir en sécurité et sont moins demandeurs de sécurité réelle que de sécurité perçue. Aucune activité économique pérenne ne peut se développer si la sécurité n'est pas assurée. La réponse des autorités à cette demande se concentre encore souvent sur la mise en place d'effectifs supplémentaires ou des redéploiements de personnels mais cela a un coût qui rend les décisions parfois difficiles.

Heureusement, depuis quelques années, les développements technologiques permettent d'augmenter significativement l'efficacité des agents de sécurité pour une dépense finalement modérée. On peut désormais accomplir une même mission pour une dépense moindre avec un effectif réduit d'hommes équipés de technologie moderne. »

De quoi parle-t-on ?

Aujourd'hui, les bâtiments intelligents sont équipés de nombreux objets électriques, électroniques numériques et/ou connectés. Du détecteur de fumée pouvant prévenir directement les pompiers en cas d'incendie au détecteur de présence permettant d'actionner l'éclairage ou la ventilation grâce aux différents capteurs installés. Ces services innovants répondent aux nouveaux besoins de confort, de sécurité et d'économie d'énergie des usagers. Ces outils, du fait de leur connectivité, doivent apporter un haut niveau de sécurisation pour éviter cyberattaques. Le *safe building* est donc la composante « sécurité » du *smart building* et vise à permettre que les outils numériques déployés dans le bâtiment puissent apporter de nouveaux services notamment de sécurité.

Cybersécurité des objets connectés dans le bâtiment et le logement

La transformation numérique a fortement impacté l'organisation et l'aménagement des bâtiments et des logements. L'utilisation croissante d'objets connectés et interconnectés facilite le quotidien des occupants et permet d'optimiser la gestion de l'ensemble des fonctions des bâtiments.

Dans les grands bâtiments et les installations industrielles, ces objets connectés permettent essentiellement de piloter les systèmes et de visualiser globalement l'état des systèmes installés : température, nombre et localisation des éventuelles pannes, fonctionnement de la ventilation et du chauffage, des contrôles d'accès, de l'éclairage, du fonctionnement d'un équipement, etc.

Dans les habitations, la domotique se développe également à grande vitesse : contrôle d'accès à distance des installations situées à l'intérieur du logement (configuration de la ventilation, pilotage des éclairages, des ouvrants, etc). Depuis son smartphone, tout individu peut, via un réseau local ou internet, consulter et paramétrer les services connectés situés dans sa maison.

Toutefois, les objets connectés représentent un nouveau canal de cyberattaques pour les pirates informatiques.

L'alarme anti-intrusion : un outil de sécurité dissuasif

Pour prévenir toute intrusion ou de vol, les entreprises et les citoyens peuvent équiper leur bâtiment ou leur logement d'une alarme anti-intrusion. Ce système de sécurité permet d'alerter l'occupant ou la personne en charge de la sécurité de la structure de toute entrée non autorisée.

Innovantes, l'efficacité de ces alarmes anti-intrusion peut être renforcée à l'aide de services complémentaires tels que l'ajout de sirène (intérieure ou extérieure), de lumière aveuglante et/ou de fumigène. Plusieurs types d'alarmes anti-intrusion existent. Les alarmes sans fil sont interconnectées avec d'autres objets électroniques du bâtiment ou du logement, leur principal avantage est de pouvoir continuer à fonctionner même en cas de coupure de courant dans le reste de la structure. Elles sont composées d'un boitier central réservé au paramétrage de l'alarme et de détecteurs disséminés dans la zone sécurisée. Ces éléments communiquent par liaison radio hertzienne.

L'éclairage intelligent : une solution novatrice et sécurisée de transmission de données

A l'ère du tout numérique, les solutions d'éclairage s'adaptent aux nouveaux besoins des entreprises au sein des bâtiments. Pour y répondre, l'éclairage devient intelligent : il permet d'accéder à de nouveaux services grâce à des technologies toujours plus innovantes et sécurisées. Aujourd'hui, l'éclairage intelligent est connecté et est devenu un nouveau moyen de transmission de données sécurisé. Il peut transmettre à distance un contenu multimédia (vidéo, son, géolocalisation) vers une tablette ou un smartphone équipé d'un récepteur adapté. En effet, des lampes LED permettent aujourd'hui de transmettre des données en clignotant en modulation très haute fréquence. Les données transmises ne sont que celles captées en dessous du halo lumineux issu de la lampe. Ce nouveau type de solution permet une communication sans fil à très haut débit, sécurisée via l'absence d'interférence avec les ondes radio et de brouillage électromagnétique. La transmission des données via cette solution est donc en principe plus sécurisée que l'envoi de données par un réseau wifi connecté et plus difficilement accessible par les pirates informatiques. Dans les bâtiments, l'éclairage intelligent et connecté constitue donc, d'une part, une véritable solution alternative lorsque le débit de connexion est faible et d'autre part, une solution novatrice et sécurisée lorsque des données strictement confidentielles ou sensibles doivent être transférées.

Points de vue

Sophie Breton,
Vice-Présidente de la FIEEC
Présidente d'IGNES
Directeur Général HAGER France

« Les innovations attachées au bâtiment intelligent et connecté répondent aux enjeux environnementaux et sociétaux d'aujourd'hui et de demain. Elles permettent d'accroître l'efficacité des dispositifs mis en place et améliorent la communication entre les différentes solutions, services et installations existantes au sein même du bâtiment. Elles permettent également une interaction avec son environnement extérieur, par exemple avec les réseaux énergétiques et numériques.

La multiplication du recours à ces innovations et objets connectés peut toutefois décupler les risques de cybermenaces ciblant le bâtiment. C'est pourquoi la sécurité doit être l'un des piliers des bâtiments connectés et doit mobiliser les compétences de chacun pour s'en assurer : des architectes, des concepteurs, des informaticiens mais aussi des usagers. C'est un sujet majeur à considérer de manière collective dès aujourd'hui. Les industriels sont bien conscients de ces enjeux et s'assurent du développement des solutions numériques et de sécurité des biens et des occupants du bâtiment, notamment à travers le security et le privacy by design. »

Emmanuel Gravier,
Président de la FFIE (Fédération Française des Entreprises de Génie Electrique et Energétique)

« Les objets connectés connaissent un développement considérable et multiplient les possibilités de services rendus à nos clients. Avec eux, nos systèmes prennent un nouvel essor et nous devons nous adapter à ces nouvelles demandes.

Mais pour les intégrer dans nos bâtiments, il est indispensable de sécuriser l'ensemble par le travail de l'installateur intégrateur.

En premier lieu, les installateurs intégrateurs ont un rôle déterminant à jouer dans l'information transmise aux clients afin qu'ils utilisent ces objets et données en toute sécurité.

Ensuite, le security by design, soit l'intégration de la sécurité dès la phase de conception, par l'arrivée de la nouvelle réglementation européenne en 2018 oblige à évaluer en amont les failles potentielles des systèmes grâce à une étude analytique très précise.

C'est ainsi que lors de l'installation, le professionnel prendra toute sa dimension de sachant en assurant une mise en œuvre sécurisée des réseaux et de leurs objets. »

L'industrie du futur sécurisée

De quoi parle-t-on ?

L'industrie du futur est en marche. L'interconnexion des machines, des automates et des produits est déjà une réalité et les récentes innovations industrielles constituent de réelles avancées pour les utilisateurs. Cette connectivité engendre de nouveaux risques et de nouvelles menaces numériques. Cela conduit à accroître en conséquence la sécurité des équipements, des produits et des systèmes d'information. Au-delà de la sécurité des sites industriels, la sécurité numérique industrielle concerne d'une part la sécurité des machines et des automates communicants et d'autre part les systèmes d'information industriels. Elle est essentielle pour préserver les quatre critères de sensibilité de tout système numérique : la disponibilité des informations accessibles et utilisables dans des conditions spécifiées de temps, la confidentialité des informations et des services, la garantie de leur intégrité afin d'assurer qu'ils ne soient pas modifiés, et leur traçabilité.

Des sites industriels sécurisés

En France et dans le monde, des sites industriels et des équipements industriels tels que des machines et des automates ont déjà fait l'objet de cyberattaques. Afin de réduire l'impact de ces menaces, l'enjeu aujourd'hui pour toute entreprise industrielle consiste à analyser son niveau de sécurité grâce à une approche fondée sur les risques : comment identifier, évaluer, prendre en compte les vulnérabilités et mettre en place des procédures en cas de survenance d'un incident ? Pour limiter ces risques, les électrotechnologies offrent une palette complète d'outils pour sécuriser physiquement, grâce au numérique, les sites industriels. Il s'agit notamment des caméras de vidéosurveillance, des systèmes de détection d'intrusion, des dispositifs de verrouillage et d'interverrouillage, des systèmes de contrôles d'accès aux bâtiments avec la reconnaissance de plaques minéralogiques ou des badges longue distance etc. L'ensemble de ces outils peut être par ailleurs piloté à distance et de manière centralisée.

Toutefois, tous les sites industriels n'exigent pas le même niveau de sécurité, qui varie fortement en fonction de la criticité du site industriel. Une centrale nucléaire, un aéroport ou une usine de construction automobile ne font pas face aux mêmes risques et n'ont en conséquence pas les mêmes besoins en termes de sécurité. C'est pourquoi, en France, le législateur a consacré un statut particulier à l'égard de certaines structures pour faire face à l'évolution de ce nouveau type de menace. Des dispositions spécifiques sont ainsi insérées dans la Loi de Programmation Mi-

litaire relativement aux Opérateurs d'Importance Vitale (OIV). Une entreprise est qualifiée d'OIV lorsque ses activités sont indispensables ou dangereuses pour la population, elles relèvent ainsi d'une pluralité de secteurs : énergie, transport, banque etc. Ces opérateurs doivent obligatoirement mettre en place des mesures renforcées de sécurité eu égard à la criticité de leurs activités : ils doivent par exemple assurer la sécurité de leur système d'information d'importance vitale ou encore respecter l'obligation de notification lorsqu'un incident se produit dans leur structure.

La cybersécurité industrielle

La sécurité numérique industrielle concerne principalement les systèmes d'informations de l'entreprise, qu'il s'agisse des systèmes d'information généraux ou ceux spécifiques liés à la production. L'objectif d'un système d'information est de fournir une valeur pertinente pour des décisions. Dans une industrie, plusieurs types de systèmes d'informations existent (données produites par les mails, intranet, extranet, objets connectés, capteurs etc.) et sont souvent interconnectés. L'ensemble de ces usages doit être sécurisé mais le risque augmente avec le niveau de criticité de l'élément attaqué. Les automates industriels, eux aussi de plus en plus souvent communicants et connectés peuvent également devenir des cibles. La cybersécurité de ces automates doit donc être assurée et des référentiels ont récemment été élaborés pour encadrer les principes de cette sécurisation.

Les SCADA *(Supervisory Control And Data Acquisition)* sont un exemple de système d'information à sécuriser. Ces SCADA fournissent des données en temps réel recueillies grâce à des capteurs qui sont stockées pour pouvoir être mémorisées en vue de leur analyse. Cette utilisation des données permet ainsi à l'industriel de pouvoir anticiper et prévoir ses activités pour ajuster au mieux ses prestations. Toutefois, ces SCADA ont une durée de vie relativement longue (entre 20 et 30 ans), les technologies utilisées dans les systèmes d'information industriels n'adoptent pas toujours les versions les plus récentes et perfectionnées. Cela peut accroître leur vulnérabilité, d'autant que les SCADA sont aujourd'hui connectés et interconnectés via les réseaux d'entreprise voire même à internet. Ce qui permet aux ingénieurs d'avoir accès à distance à ces données afin de pouvoir les traiter. Toutefois, si les ingénieurs peuvent entrer dans ces réseaux sans être physiquement dans l'infrastructure concernée, alors ces systèmes d'informations peuvent également être accessibles par d'autres et faire l'objet de cyberattaques. Ainsi, la multiplication des données produites constitue une véritable cible de vol et/ou de destruction par les pirates informatiques à l'égard des systèmes industriels. Une faille dans le contrôle des systèmes SCADA a déjà permis à des pirates de pénétrer dans les systèmes d'une entreprise de traitement des eaux. Ces derniers ont ainsi pu modifier les adjuvants chimiques apportés à l'eau potable d'un réseau régional d'approvisionnement en eau de 2,5 millions d'habitants et modifier les débits d'eau, perturbant sa distribution.

Vers un niveau de protection adapté selon les usages

La multiplication des recours au numérique engendre de nouveaux risques et pousse les industriels et les pouvoirs publics à rechercher un niveau de sécurité numérique optimal dans le domaine industriel. L'enjeu essentiel est de permettre d'établir une chaîne de confiance numérique entre les différents intervenants industriels et notamment entre les fabricants d'équipements industriels connectés et les utilisateurs de ces équipements.

La mise en place d'une telle confiance numérique requiert ainsi le développement d'un marché national et européen des produits et des services de cybersécurité compétitif et d'un niveau de sécurité adapté. En outre, la confiance numérique découle de la possibilité pour un fournisseur d'équipements d'attester de la prise en compte, dans son processus de fabrication, des problématiques de sécurité, à travers divers mécanismes tels que l'autodéclaration ou la certification par tierce partie sur la base de référentiels partagés et reconnus au niveau européen. Ces labels ou certifications ne doivent pas être conçus comme une garantie de sécurité, qui est un concept inopérant en matière de cybersécurité, mais plutôt comme la preuve de la prise en compte d'un nombre défini de règles de sécurité. Par ailleurs, le niveau de sécurité requis doit impérativement être adapté à l'usage considéré et à la criticité du dispositif à sécuriser. S'il est en effet impératif d'imposer des critères de standardisation, il convient néanmoins de ne pas créer un seul et unique procédé dans lequel l'ensemble des produits et solutions devrait se plier. Il est essentiel de pouvoir moduler ces exigences de sécurité selon les usages des produits et des solutions proposées par l'industriel. En effet, les niveaux de certification les plus élevés (Critères Communs) entraînent des coûts plus ou moins importants pour l'entreprise les mettant en œuvre. Il est donc impératif de trouver le bon équilibre entre le niveau de sécurité minimal à assurer et l'exigence de compétitivité propre à toute entreprise industrielle.

Des travaux sont actuellement en cours, entre les industries électrotechnologiques française et allemande (FIEEC, ZVEI) mais aussi entre les autorités nationales en charge de ces sujets (ANSSI, BSI). Ils visent à définir les types de labellisation/certification pertinents pour les différents usages industriels et à porter une proposition commune, au niveau européen dans ce domaine. . La certification CSPN pour l'internet des objets lancée récemment par l'ANSSI pourrait être une réponse à ce besoin à la fois de certification et de flexibilité.

Points de vue

Christel Heydemann,
Vice-Présidente de la FIEEC
Président de SCHNEIDER ELECTRIC FRANCE

« Comme le démontre encore l'actualité récente, la sécurité numérique de l'industrie est un sujet d'importance stratégique et tous les secteurs sont concernés. La convergence des systèmes informatiques (IT) et productifs (OT) au sein des entreprises industrielles est source de bénéfice opérationnel précieux mais l'entrée de l'industrie dans le monde connecté doit se faire avec un bon niveau de protection. Les produits de l'industrie électrotechnique assurent le contrôle et la sureté des procédés industriels les plus critiques et, pour cela, nous investissons massivement pour qu'ils répondent aux exigences de cybersécurité. Par ailleurs, chez Schneider Electric nos consultants en cybersécurité accompagnent les clients pour sécuriser et maintenir en conditions de sécurité leurs installations industrielles. Nous disposons en France de nombreuses solutions : il s'agit désormais de les mettre en œuvre. »

Thierry Rouquet,
Président de SENTRYO

« La transformation numérique est enfin à l'œuvre dans le monde industriel. Elle va permettre aux opérateurs industriels de réduire les indisponibilités des installations grâce à la maintenance prédictive, d'augmenter la rentabilité de leurs investissements par une gestion dynamique des actifs industriels, de produire mieux par une meilleure connaissance du client et enfin de produire propre en limitant l'impact sur l'environnement.

Concrètement elle se caractérise par une interconnexion de plus en plus importante des réseaux de contrôle industriel, par la multiplication de capteurs intelligents (IIOT) sur ces réseaux et par le déploiement de cloud spécialisés au travers desquels seront délivrés les services applicatifs basés sur des technologies de data analyse.

Cette transformation intervient brutalement dans un environnement des réseaux industriels où, contrairement à celui des réseaux informatiques, il n'y a pas de culture de la cyber sécurité et où les bonnes pratiques les plus élémentaires ne sont pas en place. Si cette situation était déjà préoccupante, c'est la raison pour laquelle les pouvoirs publics ont légiféré au travers de la LPM obligeant les opérateurs d'infrastructure critique à se doter de moyens de protection à la hauteur des enjeux, elle est clairement un obstacle à la transformation numérique.

Celle-ci augmente en effet considérablement la surface d'exposition des systèmes de contrôle industriel au risque cyber. Les industriels doivent se donner les moyens de maîtriser l'intégrité de leurs systèmes et de détecter les signes de compromission pour pouvoir tirer parti de la transformation numérique tout en contrôlant les risques. »

Klaus Mittelbach,
CEO du ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
(homologue allemand de la FIEEC)
Président du Groupe de travail Politique industrielle et Numérisation d'ORGALIME

« Les industries électriques et électroniques françaises et allemandes sont engagées pour encourager la numérisation au sein de leurs secteurs industriels. Depuis plusieurs années, la FIEEC et le ZVEI travaillent étroitement ensemble sur plusieurs aspects de la numérisation. Nos deux Fédérations sont conscientes des potentiels majeurs provenant des technologies numériques dans les chaînes de valeur, les produits, les process et les systèmes. Au niveau politique, la France et l'Allemagne ont exprimé leur volonté d'aligner leur stratégie industrielle à travers des plateformes nationales telles que l'Industrie du futur et l'Industrie 4.0. Cette fois encore, le fameux couple franco-allemand peut donner une orientation et des impulsions pour le Marché unique du numérique et la numérisation des industries. C'est la raison pour laquelle la FIEEC et le ZVEI ont décidé d'un agenda numérique commun lors de la conférence numérique franco-allemande le 6 juillet 2016 à Paris. En 2017, les deux Fédérations vont publier une feuille de route commune sur la cybersécurité, soulignant la nécessité d'une approche européenne pour la confiance et la transparence. »

La sécurisation de la santé

De quoi parle-t-on ?

Le domaine de la santé est un des secteurs dans lequel les apports des électrotechnologies et notamment du numérique sont les plus forts. Compte-tenu de la pluralité d'acteurs concernés (patients, professionnels de santé, industriels, autorités de santé, institutionnels etc.), de la criticité des fonctions considérées et de la sensibilité des données échangées, la sécurité numérique est un enjeu majeur dans ce domaine. La sécurisation dans le secteur de la santé se traduit principalement par deux leviers : la protection des données des patients d'une part et la cybersécurité des équipements de santé d'autre part. Les données personnelles constituent des cibles potentielles pour les hackers car elles deviennent de véritables sources monnayables. En France, un laboratoire d'analyses médicales en mars 2015 a été victime d'un chantage informatique : les hackers ont menacé le laboratoire de dévoiler des bilans médicaux en publiant un nombre considérable de données personnelles en ligne si la somme de 20 000 euros ne leur était pas versée.

Ces données sensibles et critiques peuvent notamment faire l'objet de vol ou de perte. Les équipements de santé doivent donc également être sécurisées pour assurer la sécurité des données et la sécurité du patient lui-même.

La sécurité numérique des données de santé : gage de protection de la confidentialité

Les nouvelles technologies numériques en matière de santé ne cessent de croître et des millions de données numériques de santé circulent ainsi tous les jours dans le monde. Ce phénomène s'amplifie par le recours croissant aux solutions de télésanté qui permettent au patient d'être plus autonome dans la gestion de son parcours de soin ou encore par le recours au dossier médical partagé (DMP). Le DMP est un carnet de santé numérique, il constitue une véritable source d'informations relatives à l'état de santé du patient. On peut y trouver les résultats d'examen réalisés par le patient suite à des radios ou des analyses biologiques, ses antécédents médicaux, ses allergies éventuelles etc. Pour sécuriser l'accès à ces données confidentielles, l'accès au DMP (à des professionnels de santé tels qu'un médecin, un pharmacien etc.) ne peut être autorisé que par le patient lui-même.

En effet, l'accès aux données et la sécurisation de ces données sont aujourd'hui au cœur du débat public. L'objectif est ainsi d'empêcher que des personnes malveillantes puissent accéder aux données pour les altérer ou les récupérer. Assurer la sécurité des données de santé est une responsabilité partagée : toute personne ayant accès à ces données, y compris le patient, se doit de les manipuler avec une précaution particulière ; par exemple le partage de ces données doit se faire via des messageries sécurisées.

Assurer la confiance numérique dans les nouvelles technologies en santé

Les industriels développent toujours plus d'objets connectés et d'applications mobiles dans le domaine de la santé. Ces innovations de rupture font évoluer les comportements des patients/usagers ainsi que les rapports entre le patient ou l'usager avec les professionnels de santé et avec son entourage (aidants).

Seulement, ces nouveaux produits et services connectés doivent être sécurisés au regard des risques de piratage tel que la prise de contrôle d'un objet connecté. Par exemple, une pompe à insuline (dispositif médical électronique utilisé notamment par les patients diabétiques) doit garantir à l'utilisateur que la juste dose d'insuline va lui être injectée. Le fabricant de ce dispositif médical doit mettre en place toute les mesures permettant d'éviter qu'un tiers puisse à distance modifier les doses d'insuline créant ainsi un risque important pour le patient. Ce risque peut être réduit par la sécurisation de ces outils et la protection des données personnelles. Toutes deux sont indispensables à l'établissement de la confiance numérique dans ces nouvelles technologies.

Il convient également de discerner le degré d'utilité et de fiabilité correspondant à l'outil connecté selon qu'il s'agisse d'un « dispositif médical » répondant à la définition de la directive 93/42 ou d'un objet connecté type « bien-être». Les nombreux équipements connectés disponibles sur le marché peuvent être utiles aux utilisateurs afin de lui fournir par exemple des informations sur son activité physique (distance parcourue, nombre de calories éliminées, etc). De tels équipements doivent être sécurisés notamment pour protéger la confidentialité des données. Dans le cas d'un dispositif médical, il faut également considérer le risque potentiel pour le patient en cas d'accès non autorisé qui pourrait conduire à l'indisponibilité de l'équipement ou un fonctionnement altéré. Ces différents risques font l'objet d'une analyse de risque accompagnée des mesures de maîtrises du risque mises en place par le fabricant ; ces éléments font partie intégrante du dossier technique du dispositif médical qui est soumis à évaluation dans le cadre de la procédure de marquage CE.

En France, la HAS s'est également saisie de ces enjeux en publiant récemment (octobre 2016) un guide de 101 règles de bonnes pratiques visant à promouvoir la confiance dans les applications et les objets connectés en santé.

Les outils de santé numérique au service de la silver économie

En France, l'espérance de vie a progressé. Ainsi, au 1er janvier 2017, les personnes de 65 ans ou plus représentent 19,2% de la population française. L'objectif principal réside donc dans le fait de pouvoir assurer la sécurité de ces personnes âgées en tentant de faire reculer leur perte d'autonomie, notamment à leur domicile à l'heure du virage ambulatoire. Ce dernier consiste à réduire le temps de prise en charge du patient à l'hôpital pour assurer un retour plus rapide à son domicile et un parcours de soin à distance. Il engendre ainsi le recours à de nouvelles technologies pour permettre au patient d'être plus autonome et de continuer à assurer ses soins lui-même sans être ni à l'hôpital ni dans un établissement spécialisé.

L'utilisation de ces nouveaux outils peut ainsi répondre aux nouveaux besoins des seniors via des services permettant par exemple de piloter des équipements dans leur logement lorsqu'ils sont en situation de fragilité ou de dépendance, ou d'accompagner l'intervention des aidants à leur domicile. Grâce au développement de la télésanté qui permet le suivi de l'état du patient par

un ou plusieurs professionnels de santé à distance grâce à des technologies connectées, l'utilisateur peut s'équiper d'outils de téléassistance comme d'un bouton d'alerte en cas de chute ou de malaise qui contacterait automatiquement, à son enclenchement, des services d'urgence et permettrait une intervention rapide à son domicile.

A nouveau, la priorité reste de s'assurer que ces dispositifs soient utilisés conformément à leur usage de destination. Et que les données émises par ces dispositifs soient sécurisées de manière à n'être conservées que dans un temps limité et accessibles uniquement aux personnes concernées.

Le marché de la santé numérique constitue donc un véritable enjeu stratégique et social : les objets connectés, la domotique, la télésurveillance,

la téléassistance et bien d'autres sont des outils clefs pour la silver économie, pour les personnes âgées elles-mêmes, mais également pour leur entourage : personnel soignant, les proches, les structures de secours.

Points de vue

Alexandre Caron,
RSSI d'APICEM (Association pour la Promotion de l'Informatique et de la Communication en Médecine)

« Historiquement, les médecins ont toujours veillé à la confidentialité des données de santé de leurs patients, car ils en étaient clairement désignés les gardiens. La très grande majorité des médecins imprégnés de cette culture du secret médical ont respecté cette règle absolue, dans l'intérêt des patients, en s'équipant, majoritairement, d'outils sécurisés conçus par des professionnels de santé pour des professionnels de santé, par exemple avec la messagerie APICRYPT.
La loi de 2004 confère au patient la propriété et la responsabilité des données personnelles qui le concernent sans qu'un accompagnement adapté ait été mis en place pour éduquer les patients sur l'importance des conséquences d'une divulgation inappropriée.
Le souhait des pouvoirs publics consistant à vouloir agréger les données de santé dans un unique dépôt de données appelé DMP constitue un véritable appel d'air pour les pirates informatiques et un point de fragilité comme l'a démontré l'attaque du NHS britannique par le virus « WannaCry ».

C'est donc une responsabilité collective de l'état et des professionnels de santé que d'accompagner l'ensemble des acteurs dans cette nouvelle appropriation de leurs données et de l'indispensable sécurisation des systèmes d'information qui les concernent. »

Stéphane Regnault,
Président de VYGON
Président du SNITEM

« La sécurité numérique est en enjeu majeur dans le domaine de la santé. La sécurisation dans le secteur de la santé se traduit principalement par deux leviers : la protection des données des patients d'une part et la cybersécurité des équipements de santé d'autre part.

Ce sujet est souvent perçu au stade de l'utilisation de la solution technologique. Ainsi l'augmentation de la connectivité des dispositifs médicaux à des réseaux informatiques et la convergence des technologies nécessite une vigilance de tous les acteurs face aux vulnérabilités potentielles et aux menaces émergentes. Il s'agit bien d'une responsabilité partagée. Mais dès le stade amont, au début de toute innovation, la protection de la vie privée et la sécurité des patients doivent être prises en compte. Les entreprises du secteur que je représente travaillent proactivement sur des solutions de sécurisation de leurs dispositifs médicaux communicants. Il n'est pas très difficile de comprendre la confidentialité extrême qui entoure et doit entourer ces actions, afin de pouvoir continuer à faire bénéficier les patients, le plus sereinement possible, des opportunités innombrables offertes par les nouvelles technologies. »

Jacques Lucas,
Vice-Président et Délégué Général au Numérique du CNOM (Conseil National de l'Ordre des Médecins)

« La sécurité numérique dans le domaine de la santé est une exigence d'ordre éthique. Il en va de la liberté et de la sécurité du citoyen. La protection de ses données personnelles doit lui être garantie, non seulement par des règles juridiques pour les personnes qui sont habilitées à y accéder, mais tout autant par les moyens technologiques d'identification de ces personnes, qui doivent être tracées lorsqu'elles se connectent au système d'information. Cela concerne tous les dossiers informatisés, mais aussi les moyens technologiques pour la pratique de la télémédecine, le domaine des dispositifs médicaux connectés et celui des applications et objets connectés en santé. Plus le champ d'usage des outils de santé connectée se rapprochent du soin proprement dit, plus la cybersécurité du système doit être forte. L'Ordre des médecins ne cesse d'apporter son concours aux différents acteurs dans ce domaine, ainsi qu'à la puissance publique. Je pense aussi que le marché, utile au plus grand nombre, ne se développera durablement que sur des bases éthiques consolidées. Cependant, le citoyen lui-même peut être fasciné par les prouesses des technologies sans se prémunir vis-à-vis des risques de mésusage. Le CNOM demande qu'un débat public sur ce thème soit organisé. Ce débat, bien structuré, aurait au minimum le mérite de donner au citoyen des informations de sources diverses, mais concordantes, afin de l'engager à son profit, sans appréhension mais avec lucidité, dans ce « nouveau monde » du numérique en santé. »

De quoi parle-t-on ?

Les institutions bancaires et financières sont des structures particulièrement sensibles au regard des flux d'informations et de transactions qu'elles gèrent continuellement. Elles traitent et stockent un nombre conséquent de données personnelles et confidentielles et ont la responsabilité des fonds confiés par leurs clients. En conséquence, le secteur bancaire et financier est une cible de choix pour les pirates informatiques : il a concentré plus de 22 % du total des attaques l'an passé, contre seulement 11,92% en 2012*. Ces attaques peuvent cibler des outils matériels tels que les terminaux de paiement ou les distributeurs automatiques de billets. Le succès du développement des services bancaires en ligne (consultation des comptes bancaires, virement ou achat en ligne) attire les hackers. Enfin les réseaux des professionnels constituent également une source de cyberattaques considérable notamment au cours de transactions financières.

La sécurisation numérique de ce secteur apparaît toutefois complexe au regard de sa sensibilité, du nombre d'actions et d'intervenants considérés, ainsi que de la nécessité d'assurer un fonctionnement continu et ininterrompu des services fournis qui constituent la colonne vertébrale de l'activité économique du niveau local au niveau mondial. Par ailleurs, il apparaît délicat pour les

institutions financières de communiquer sur les incidents dont elles sont victimes afin de préserver la confiance des utilisateurs et des partenaires qui constitue le fondement même du fonctionnement du système financier. En France, les établissements ne sont tenus de signaler que les incidents dits « significatifs » auprès de l'autorité de Contrôle Prudentiel et de Résolution (ACPR) (soit toute fraude entrainant une perte ou un gain d'un montant brut dépassant 0,5% des fonds propres de base de la banque). Cela ne devrait toutefois pas empêcher les banques d'informer sur les moyens de lutte mis en place pour assurer la sécurité de leurs systèmes et d'éviter, de manière plus générale, de perturber la stabilité financière.

** Selon les chiffres collectés par Kaspersky Lab auprès de 60 millions d'utilisateurs dans le monde.*

Les systèmes clients, cibles des pirates informatiques : focus sur la sécurité numérique des terminaux de paiement électronique (TPE) et des distributeurs automatiques de billets (DAB)

Les appareils permettant la réalisation de transactions financières et le retrait/dépôt de sommes d'argent font partie de notre quotidien.

C'est le cas du terminal de paiement électronique (TPE). Cet appareil électronique et connecté permet de réaliser des transactions de paiements par carte bancaire de façon sécurisée, électronique ou magnétique.

Du fait de son utilisation quotidienne par des millions d'usagers et du caractère sensible des

données qu'il traite, sa sécurisation numérique est un enjeu stratégique afin de prévenir les cyberattaques.

En effet, des logiciels malveillants peuvent être introduits directement dans le terminal lui-même ou dans les ordinateurs connectés au terminal. Ce type d'attaques peut permettre aux hackers de consulter des données enregistrées par l'appareil et de récupérer les numéros de cartes bancaires.

Les distributeurs automatiques de billets (DAB) constituent un autre canal pour les pirates informatiques de parvenir à détourner des informations/ou des fonds.

Le premier cas de *malware* visant les DAB a été découvert en 2009, il s'agissait du *malware* « *Skimmer* ». En introduisant un logiciel malveillant via le piratage matériel de la machine ou en passant par les réseaux auxquels elles sont connectées, les hackers peuvent en prendre le contrôle, récupérer des données bancaires et retirer de l'argent.

La sécurisation de ces terminaux est donc un enjeu stratégique. Elle repose sur une combinaison de l'ensemble des domaines d'action des industriels de confiance numérique et notamment sur la cryptographie, l'identité numérique, les technologies d'authentification, etc. C'est une tâche qui nécessite l'engagement de l'ensemble des acteurs de la chaîne des paiements et de nombreux investissements afin de garantir une sécurité dans ces infrastructures.

Sécurisation des données collectées via les services d'accès au compte bancaire du client et des achats effectués en ligne

La transformation numérique touche les institutions bancaires notamment à travers les services en ligne accessibles aux clients et aux utilisateurs.

La quasi-totalité des banques propose désormais à leurs clients d'accéder à leurs informations et comptes bancaires en ligne via leur ordinateur, tablette ou smartphone. En quelques clics, l'utilisateur peut ainsi avoir accès à l'ensemble de ses données confidentielles n'importe où, n'importe quand dans un cadre sécurisé. Ces services se développent concomitamment avec l'essor de l'e-commerce qui permet à l'utilisateur d'effectuer des transactions financières à distance. En 2015, 835 millions de transactions en ligne ont ainsi été observées*.

Ces services connectés améliorent le quotidien des usagers mais peuvent représenter autant de cibles potentielles pour les pirates informatiques.

Ces données peuvent être collectées à la suite de cyberattaques. Les pirates peuvent avoir recours à plusieurs méthodes pour pirater un compte bancaire en ligne. Ils peuvent s'introduire dans l'ordinateur de l'utilisateur pour récupérer des informations confidentielles (ses mots de passe et identifiants bancaires), ils peuvent rediriger l'utilisateur vers un site malveillant ou via l'envoi de courriels frauduleux ou « *phishing* » à des clients pour obtenir leurs données bancaires. En 2013, ce nombre d'attaques visant spécifiquement les établissements financiers, banques, sites d'e-commerce ou solutions de paiements en ligne, a grimpé de près de 50 % en un an, pour atteindre près de 104 millions*.

Face à ces diverses menaces, les établissements bancaires et financiers investissent afin de sé-

curiser la relation avec leurs clients : vérification de l'identité de l'utilisateur, renforcement de la validation des ordres de paiement et sécurisation des systèmes d'information.

Des systèmes d'authentification renforcés sont ainsi mis en place. L'enregistrement d'un nouveau RIB ou une opération de virement peuvent requérir la validation d'un mot de passe reçu par SMS pour confirmer l'identité de la personne qui effectue l'opération, en complément des données bancaires. Ces structures peuvent également avoir recours à des cartes de paiement à cryptogramme dynamique. Le code à 3 chiffres situé au dos de la carte de paiement change toutes les heures sur un écran *e-paper* intégré dans l'épaisseur de la carte. Cette nouvelle technologie permet de rendre rapidement inutilisable les coordonnées bancaires volées.

Dans le cadre plus général de la révision de la Directive sur les services de paiement, l'Autorité bancaire européenne consciente de préserver un haut niveau de sécurité demande à juste titre l'interdiction du partage des identifiants des clients à une tierce partie (utilisée notamment pour le *screen scraping*) et l'authentification forte du client par la banque teneur de compte pour les services d'agrégation de compte et d'initiation de paiement.

**(1) Selon les chiffres collectés par Kaspersky Lab auprès de 60 millions d'utilisateurs dans le monde.*
**(2) Chiffre tiré de l'étude réalisée par Fevad sur l'évolution économique des marchés e-commerce.*

La sécurisation des réseaux des établissements bancaires et financiers

Un des objectifs des pirates informatiques relativement au secteur bancaire et financier est le détournement de fonds. Il est donc essentiel que les systèmes d'informations des établissements bancaires soient protégés et sécurisés pour éviter que des hackers ne s'en prennent à leur contenu.

Des cas de cyberattaques visant des établissements bancaires privés ou publics ont déjà été observés ces dernières années. L'exemple le plus frappant est certainement celui du piratage dont a été victime la banque centrale du Bangladesh en février 2016. En exploitant notamment une faiblesse interne de la banque les hackers ont su récupérer des codes via l'insertion d'un logiciel malveillant et d'un système de transfert de fonds leur permettant d'envoyer des messages aux clients au nom de la banque piratée et effectuer des virements sans laisser de trace des transactions frauduleuses. 81 millions de dollars déposés sur un compte de la Réserve fédérale américaine appartenant à la Banque centrale du Bengladesh ont ainsi été détournés. La détection de cette fraude n'est intervenue qu'un an après l'initiation de la cyberattaque, toutefois certains agissements des hackers ont pu être interceptés puisqu'initialement 35 transactions avaient été effectuées pour un montant équivalent à 951 millions de dollars.

Les pirates informatiques usent de nombreuses pratiques afin de détourner des fonds, de procéder au vol de données ou de perturber les systèmes d'une structure bancaire ou financière.

En janvier 2017, en Grande-Bretagne, la banque Lloyds a été victime d'une cyberattaque. Cette fois-ci les pirates ont eu recours à la pratique du déni de service distribué (DDoS) qui a perturbé ses services en ligne pendant trois jours. Un DDoS consiste à rendre indisponible un ou plusieurs services en y empêchant l'accès (par exemple en saturant de données la bande passante du réseau) grâce à l'intervention d'un réseau de machines. Ces attaques ont des impacts conséquents sur ces établissements puisqu'elles engendrent souvent des pertes financières et ternissent leur réputation.

Pour se prémunir de ces attaques malveillantes, s'assurer de la sécurité des systèmes d'information de ces structures constitue une priorité.

Marie-Anne Barbat-Layani,

Directrice Générale de la FBF (Fédération Bancaire Française)

« On ne transige pas avec la sécurité !

La cyberattaque massive et internationale qui a eu lieu le 12 mai 2017 avec un «ran-çonlogiciel » répondant au nom de WannaCry a mis en lumière pour le grand public la puissance de la cybercriminalité.

Les banques connaissent depuis longtemps cette menace qui se développe, gagne en compétences et en moyens d'années en années. Elles sont constamment à la recherche de solutions afin de sécuriser leurs infrastructures et l'accès à leurs données qui sont une cible de choix pour les cybercriminels.

Il est bon de rappeler que la majorité des fraudes ayant pour conséquence une perte financière (détour-nement de fonds) sont souvent dues au manque de prudence des particuliers ou des entreprises qui ne sont pas toujours conscients du développement de cette cybercriminalité.

Il y a des conseils à respecter scrupuleusement : on ne donne jamais à un tiers, ou suite à une demande par mail, ses identifiants bancaires, ni surtout son code d'accès à sa banque en ligne, car des escrocs peuvent se faire passer pour un organisme bancaire ou un e-commerçant dans le but d'obtenir ces données confidentielles (technique dite du « phishing »). De même, on ne se sépare pas de sa carte bancaire et on n'achète pas sur les sites internet non sécurisés. Côté entreprises, il faut s'équiper de solutions informatiques sécurisées et former régulièrement son personnel contre les fraudes dites « au Président » ou « aux faux ordres de virements ».

L'augmentation des risques de cyberattaque doit amener tout le monde à revoir sa façon de penser et d'agir, et notamment le législateur. La volonté de permettre à de nouveaux acteurs d'intervenir sur le marché des paiements ne peut se faire au détriment de la sécurité. Les infrastructures de paiement nécessitent des investissements très importants et sans cesse renouvelés par les banques pour améliorer sans cesse leur efficacité et le niveau de sécurité. La sécurité d'une chaîne de paiements est celle de son maillon le plus faible.

La course à l'innovation et l'ouverture du marché à la concurrence ne doivent pas se faire au détriment de la sécurité car les clients ont le droit de continuer à avoir confiance dans la sécurité de leurs données personnelles et de leurs fonds. Cette confiance, c'est une richesse et une fierté pour le secteur bancaire.

C'est pourquoi dans les batailles en cours (mise en œuvre de nouvelles directives telles que la Directive sur les Services de Paiements - DSP2), et à venir, les banques se battront et ne transigeront pas sur les questions de sécurité.»

Olivier Vallet,
PDG de DOCAPOST

« En matière de sécurité numérique bancaire et financière, la collecte de données de la clientèle est essentielle : le KYC (Know Your Customer). Il n'est pas question d'usages ou de cibles marketing, mais surtout d'un dispositif numérique qui vise à vérifier l'identité du client en question. Les banques sont les premières utilisatrices de ce type de dispositif. Toutefois, elles ne sont pas les seuls organismes à avoir besoin de sécuriser les liens et échanges. Des mesures de précaution sont aussi prises par les petites comme les grandes entreprises, dès lors qu'il s'agit de prévenir différents fléaux liés à la digitalisation des usages, comme la fraude financière, l'usurpation d'identité, voire le blanchiment d'argent. L'objectif est donc de s'assurer de la véracité et de l'intégrité des documents transmis lors d'une souscription.

Jusqu'à présent, ce dispositif de KYC pouvait être très coûteux pour les entreprises et organismes bancaires. En effet, en plus de devoir répondre à une réglementation européenne assez lourde, la gestion des dossiers pouvait aussi amener à une gestion RH interne coûteuse et compliquée. Pour exemple, certains organismes vérifient encore les passeports à la main, ce qui est chronophage et génère des coûts importants. Aujourd'hui, avec l'instauration de solutions automatisées, fiables, à même de prendre en charge la gestion des dossiers et la probité des pièces justificatives, nous proposons aux entreprises de gagner un temps précieux et d'optimiser leur investissement financier. De cette façon, les informations dites «sensibles» sont automatiquement remontées au service dédié, qui peut ainsi traiter ces données. Là encore, des solutions numériques sûres ont donc été conçues afin de rationaliser la gestion du KYC et nous accompagnons régulièrement nos clients dans cette démarche .»

La sécurisation de la mobilité et des transports

De quoi parle-t-on ?

Les moyens de transports tels que les voitures ou les trains sont indispensables à notre quotidien. De plus en plus connectés, ils sont équipés de nouvelles technologies et de nouveaux services toujours plus innovants. Ces technologies permettent aux transports d'échanger en continu des données avec une pluralité d'entités : des centres de services spécialisés, des systèmes de géolocalisation, avec d'autres transports ou encore avec divers dispositifs d'infrastructure.

Les industries électrotechnologiques jouent donc désormais un rôle de premier plan dans le domaine de la mobilité et apportent grâce à leurs innovations de nouveaux services aux solutions classiques de transport pour améliorer leur qualité, leur confort ainsi que leur sécurité. Pour autant, l'intégration de ces innovations constitue autant de nouveaux points d'entrée pour les attaques numériques, et un nouveau défi en termes de sécurisation des usagers et de leur environnement.

La technologie au service de la sécurité des usagers de la route

De plus en plus de véhicules sont désormais connectés et cette tendance de fond s'accélère.

Plus de 600 millions de voitures équipées de services embarqués seront en circulation dans le monde d'ici à 2020 selon une étude récente *.

Ces aménagements bénéficient aux utilisateurs en augmentant leur confort de conduite et en assurant leur sécurité grâce à des outils et services de prévision et d'anticipation des dangers.

Au-delà, les innovations technologiques dans ce domaine permettent désormais d'anticiper la commercialisation prochaine de véhicules toujours plus autonomes grâce à des systèmes de plus en plus performants d'aide à la conduite. Les avantages attendus de ce type de voitures sont ainsi de réduire considérablement le risque d'accidents, de réguler plus efficacement le trafic routier et de réduire le taux de pollution.

Munis d'une multitude de capteurs et de caméras, les véhicules connectés peuvent calculer eux-

mêmes la distance de sécurité à respecter avec les autres véhicules l'environnant. Ils avertissent et réagissent face à un danger imminent (un piéton traverse une chaussée non éclairée, une voiture arrive à grande vitesse etc.) : le véhicule change automatiquement de trajectoire ou freine immédiatement sans intervention du conducteur.

Technologiquement équipés, ils peuvent également détecter les lignes tracées sur le sol en cas d'inattention de la part du conducteur ou de somnolence ou encore permettre l'ouverture des portes à distance et la programmation de services internes au véhicule via une application spécifique sur le smartphone du conducteur.

Cependant, équiper un véhicule de nouveaux produits et solutions de sécurité numérique implique aussi d'assurer le véhicule contre les risques induits par ces nouvelles technologies. C'est pourquoi l'on peut constater dans certains cas des réticences à leur intégration, ces coûts supplémentaires liés aux assurances des véhicules peuvent retenir certains utilisateurs d'y avoir recours.

Toutefois, et malgré ces réserves, ce marché reste en plein essor, il devrait atteindre 350 milliards de dollars en 2020, et convainc de plus en plus de constructeurs automobiles, d'éditeurs de logiciels, de géants du web et d'équipementiers à investir dans ce secteur.

**Etude réalisée par le cabinet Ptolemus consulting*

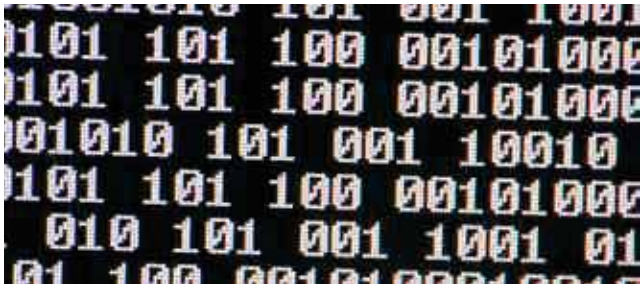
Véhcules connectés : de nouvelles portes d'entrées pour les cyberattaques

Ces nouveaux produits, outils et services technologiques innovants introduisent également de nouvelles vulnérabilités face aux risques cyber, en multipliant les surfaces d'attaques possibles à l'encontre des véhicules toujours plus connectés.

L'enjeu réside dans le fait d'assurer la protection des outils connectés intégrés dans le véhicule afin d'éviter toute attaque numérique et toute atteinte à la sécurité de l'usager ou d'un tiers par un pirate informatique ou un individu mal intentionné. Les menaces sont réelles et les motivations multiples : elles peuvent être liées à la sécurité, à la vie privée de l'usager ou à des motifs financiers.

Ainsi, la prise de contrôle à distance du véhicule peut menacer le conducteur et ses passagers en gérant sa vitesse ou en l'immobilisant, les données personnelles et sensibles communiquées au véhicule peuvent être transmises ou volées et la localisation de l'appareil peut être tracée. Ces exemples constituent autant de risques dont un usager peut être victime si la sécurité numérique du véhicule n'est pas optimale.

De surcroit, si la sécurité des dispositifs propres au véhicule doit être assurée, des facteurs supplémentaires entrent dans ce paysage : les paramètres externes au véhicule.

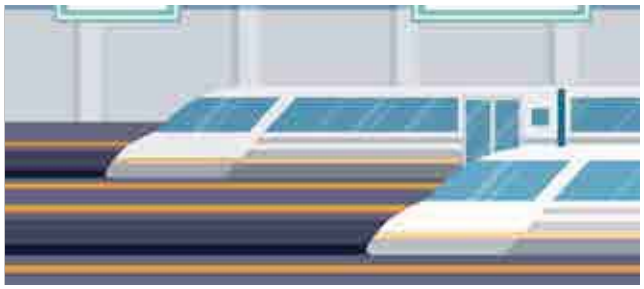


La sécurité de l'usager peut en effet être entravée par des surfaces et des moyens avec lesquels le véhicule interagit, liés à son environnement : des bornes pour recharger le véhicule, le réseau téléphonique, un data center ou encore un réseau *cloud*, son réseau WIFI, des puces téléphoniques embarquées, le *bluetooth*, ou encore via la prise USB.

C'est donc tout un écosystème qui doit être pris en considération dans le processus de sécurisation des véhicules connectés.

Un réseau ferroviaire sécurisé

Le train est l'un des moyens de transport préféré des français. En 2014, 102 milliards de voyageurs ont pris le train sur le territoire français et 32,2 milliards de tonnes de marchandises ont été transportées par cette voie*.



De plus en plus connectés, des cas d'attaques à la sécurité numérique du réseau ferroviaire ont déjà été observés dans le monde. Tout comme pour le piratage numérique d'une voiture, les motivations relatives à l'atteinte d'un train peuvent être de nature multiple.

Un pirate peut vouloir contrôler la trajectoire d'un train via le contrôle commande, le système de pilotage des installations en interférant par exemple dans l'aiguillage ferroviaire afin de déstabiliser le réseau ou encore en brouillant les systèmes embarqués permettant de maintenir une vitesse sécuritaire du train. Une telle attaque peut également relever de la volonté de revendiquer un message social ou politique par exemple en prenant le contrôle des panneaux de signalisation en gare et afficher son propre texte. Le pirate peut aussi maîtriser l'appareil via sa connexion wifi embarquée et ainsi modifier les paramètres du trajet initial du train.

La pluralité de ces scénarios constitue autant d'enjeux à considérer et à prendre en compte dans l'élaboration, la fabrication, et la mise en place des matériels et systèmes ferroviaires dans l'objectif d'assurer la sécurité des passagers, des employés, des équipements et des infrastructures.

Par ailleurs, la garantie de systèmes fiables et sécurisés permet d'une part, une optimisation conséquente du fonctionnement global des réseaux, des équipements et de la signalisation ferroviaires et induit, d'autre part, une maitrise considérable des coûts pour les opérateurs et les exploitants dans ce secteur.

Points de vue

Gérard Matheron,
Vice-Président de la FIEEC
Président d'ACSIEL-Alliance Electronique
VP R&D et Affaires Publiques, STMICROELECTRONICS

« La sécurité des passagers et la sûreté de fonctionnement dans les transports de masse constituent l'enjeu majeur des opérateurs ferroviaires dans le futur.

Cela passera par une fiabilisation accrue des équipements et matériels roulants et de la signalisation ainsi que par la refonte des infrastructures ferroviaires. Pour une meilleure gestion des matériels des approches de maintenance prédictive de ces installations devront être mises en œuvre.

En ce qui concerne la sécurité des personnes, des systèmes de reconnaissance d'identité biométrique devront être déployés à grande échelle, dans le transport aérien comme pour le ferroviaire. Enfin, la cybersécurité des infrastructures et des matériels liés aux moyens de transport devra être garantie.

C'est à ce prix que les transports de masse pourront faire face aux défis de la mobilité croissante des personnes. »

Coralie Héritier,
CEO d'IDNOMIC

« Avec la croissance exponentielle du big data et du marché des objets connectés, il devient primordial de clairement identifier et protéger les données sensibles tout en garantissant l'identité numérique des objets ainsi que la confidentialité et l'intégrité de l'information.

Dans les systèmes automobiles coopératifs, l'intelligence est partagée. Les véhicules communiquent les uns avec les autres et avec l'infrastructure. Cette communication permet d'accroître considérablement la qualité et la fiabilité des informations échangées, pour offrir aux utilisateurs toujours plus de services, pour fluidifier le trafic et ainsi réduire les émissions de gaz à effet de serre, et pour accroître la sécurité routière.

Ces facultés additionnelles des véhicules constituent une évolution majeure et sans précédent pour laquelle ces systèmes communicants ont besoin de sécurité et de confiance numérique, assurées par la mise en place d'une PKI (Public Key Infrastructure).

Celle-ci permet de répondre à une problématique de dimensionnement à grande échelle afin d'être en capacité de distribuer des milliards de certificats électroniques pour identifier et protéger les communications des stations embarquées ITS (Intelligent Transport System). Les certificats de sécurité déployés garantissent l'authenticité des messages utilisés par la voiture et apportent des services de confidentialité en protégeant l'identité et l'accès aux données du véhicule.

C'est tout l'enjeu des projets d'innovation auxquels IDnomic contribue aux côtés d'industriels du secteur automobile, des pouvoirs publics et de plusieurs instituts de recherche, et ce dans un contexte de coopération pour la définition et la mise en œuvre de standards européens. »

Louis Nègre,
Président de la FIF (Fédération des Industries Ferroviaire)

« Les systèmes de transport deviennent de plus en plus connectés et interconnectés avec leur environnement. Il s'agit d'une rupture technologique majeure qui permet tout à la fois de réelles avancées (automatisation, optimisation de l'exploitation et de la maintenance, information pour les utilisateurs…), mais qui représentent également de nouveaux points d'entrée pour les cyberattaques. Les systèmes de transports peuvent êtres ciblés à travers de multiples canaux communs à tous les types de mobilité avec des conséquences très diverses: prise de contrôle, piratage des équipements de billettique ou de contrôle d'accès, perturbation des réseaux de communication par le réseau wifi ou bluetooth, vol de données des clients. Il apparait ainsi crucial de traiter ces nouvelles menaces et notamment de s'assurer que l'architecture et la sécurité intrinsèque des systèmes et des infrastructures de transport soient pensées en intégrant les principes de sécurité numérique dès la phase de conception des projets. »

PARTIE 3 :

Dimensions nationale, européenne et internationale

Une étroite collaboration franco-allemande "Industrie du Futur - *Industrie 4.0:* *The Digitisation of Industry at the Heart of our Economy and Society*"

Joint Position
6th of July 2016, Paris

Once again, the French-German partnership has the potential to become the engine for our common European project: the digitisation of industry at the heart of our economy and society. With respect to the developing European Digital Single Market, the French-German cooperation on Europe's digital agenda has constantly given significant impulses over the last months. In October 2015, a common declaration has been signed by the French Minister of Economic Affairs Emmanuel Macron and his German counterpart Sigmar Gabriel supporting a European Digital Single Market and intensifying French-German collaboration on research, innovation and business development. Only few months later, at the Hannover Fair 2016, the French national platform Alliance Industrie du Futur and the German Plattform Industrie 4.0 have agreed on a shared action plan of cooperation to improve pooling and sharing of national digital capabilities.

Based on these past French-German efforts, the Federation of Electrical, Electronic and Communication Industries (FIEEC) and the German Electrical and Electronic Manufacturers' Association (ZVEI) want to reaffirm this digital partnership by giving impulses and guidance to political decision makers. The French and German Electrical and Electronic Industries are a major, dynamic and innovative industrial sector of excellence in Europe. FIEEC and ZVEI are representing more than 4 600 companies of the manufacturing and engineering industries with 1,249 million employees and 278.5 billion euros of annual turnover. Membership encompasses global leaders as well as globally active small and medium size enterprises. As users and technology suppliers, our industries play a unique leadership role in the digital transformation of the European economy and society. This transformation process embodies great opportunities as well as various challenges, which need to be addressed effectively and in a collaborative manner. FIEEC and ZVEI are strongly persuaded that national initiatives such as Industrie du Futur in France and Industrie 4.0 in Germany are forward-looking projects to bundle capacities, while creating a fruitful environment of sharing best practices and innovation. At the same time, we need more cross-border and European cooperation of these national projects to face common challenges and to avoid fragmentation. The French-German cooperation on the digital transformation is one of the most promising bilateral synergies across the European Union and is a lighthouse partnership program for other Member States.

Our industries highlight the importance of an ambitious European industrial digital strategy, which should ensure an adequate regulatory framework that allows economic growth, creates new jobs, and speeds up market-driven innovations. Moreover, on behalf of our member companies, both associations are strongly committed to send a clear message to European decision makers to take industrial stakeholders into account for making full use of Europe's digital potentials. With respect to this industrial perspective, both associations agree on the following points addressing the regulatory framework for digitising Europe's industry, guidelines on the responsible use and management of data, the urgent need of a European cybersecurity strategy as well as open and industry-driven standard setting procedures.

Executive Summary

FIEEC and ZVEI decided to work closely on common objectives and challenges of the digital transformation of our industries. Therefore, FIEEC and ZVEI have agreed on several joint messages and positions:

- Both industry associations are strongly committed to a further development and harmonisation of the European Digital Single Market.
- Cross-border cooperation is essential in order to avoid fragmentation and digital silo structures within European Member States.
- We want to create trust and confidence in a digital future by a regular and open dialogue with any stakeholder involved.
- The needed level of trust and confidence can only reached via a secure and safe data and cybersecurity infrastructure.
- We strongly believe that existing and future policy decisions applying to any field should take the dynamic process of the digitisation into account.
- The concept of digital self-determination is a guiding principal to guarantee responsible management of personal and non-personal data.
- Cybersecurity is a prerequisite of the digital transformation. Therefore, we want to promote the concept of industrial security (security-by-design security) in company with IT-security.
- The standardisation procedures concerning cyber-physical products, processes and services are rapidly changing. We need open, close-to-the-market, industry-driven standards which apply to the global market.
- An efficient market surveillance to create a level-playing field with our non-European competitors is also a major issue for our industries.

1. Digitising our Industries

The digitisation of our industries is a key priority on the national, European and global agenda. The internet of things has multiple implications and major effects on products, processes and services. The bigger picture shows that European electronic and electrical industries are holding leadership positions in producing and applying digital technologies. Our companies are users and suppliers of digital products. A future digital scenario, in which our industries are keeping this world-leading position, requires a clear vision about objectives and specific industry needs. One of the most important objectives is the evolvement and further harmonization of the European Digital Single Market. The full harmonisation would not only bring additional growth, jobs and investments to Europe's economy, but also an additional revenue to Europe's industry as €110 billion of revenue per annum could get capitalised. Europe's manufacturing industry is an essential cornerstone of our economic strengths and global competitiveness. Product quality and European standards are at high level. The electrical engineering industry in particular is a trendsetter for technological progress and innovation. This is why our industry needs to be better heard in the political process. We are a strong partner for building a digital Europe, to support our economies and to make them more competitive on the global market. Both, FIEEC and ZVEI are standing united to tackle challenges and to make a digital Europe happen.

2. Guidelines on the Responsible Use and Management of Data

Digitisation is spreading rapidly across all areas of the economy and society. Data is being generated on a large scale and in great variety. Linking and analysing of big data can bring great benefits, but also gives rise to risks which many people see as a cause for concern.

ZVEI and FIEEC are taking these concerns very serious. A priority task of government and business is to create trust in the digital world. It is imperative that this trust will be maintained, because confidence in the responsible use of data is the basis for the emergence of new, data-driven services and business models. Growing interconnectedness is leading to new business models within industries as well.

These models are based on the exchange of sensitive data in a value creation network, data which concerns companies' proprietary knowledge and expertise. Confidence in the responsible handling of data is the prerequisite here. ZVEI and FIEEC are entirely aware of this trust building challenge. The companies of the German electrical industry and the French electrical, electronic and digital industries strongly advocate responsible data protection and a safe and secure data infrastructure. Therefore, both associations support a legal framework which allows data-driven business models to emerge in our countries and generate trust in new technologies. Both associations are committed to the essential principal of digital self-determination. We support all efforts which are empowering a secure and safe data infrastructure regardless of personal or non-personal data transaction.

The collection and processing of personal data for new business models must be handled responsibly. The companies of the French and German electrical, electronic and digital industries therefore advocate prudent and careful use of personal data and industrial data for corporate purposes and, to this end, will develop examples of best practice. The electrical industry sees this as an opportunity to develop a common culture of the use of data which is guided by clear values and should not only apply to the European level but also on a global scale. Such a commitment to data related values will enhance competitiveness and will generate a trusted digital environment.

Commitment to Digital Self-Determination

The French and German electrical, electronic and digital industries make an explicit commitment to digital self- determination. Digital self-determination is based on the principle of transparency and defines the full capability of controlling self-generated data along the entire data lifecycle.

Dialogue as the Necessary Approach to Finding Solutions

New, data-driven products and services are customized to meet the individual needs of people and companies. They make day-to-day life easier and bring tailored benefits to the customer. At the same time, however, the fear of abuse remains. ZVEI and FIEEC aim to address these concerns through an active dialogue. As new issues in the use of data arise, for example linking or anonymizing data, ZVEI will engage in an active dialogue in order to create a common understanding. In France, FIEEC has a strong cooperation with the French data protection authority (CNIL) in order to define together the recommendations concerning the protection of personal data. One conformity pack has already been published on "smart grids and personal data" and a new one in under development concerning "Silver economy and personal data".

Rejection of a Monopoly on Technical Data

Our organizations reject a monopoly on technical data. Digitisation should be designed to allow data to be shared without any blanket transfer, analysis or selective visibility of such data being required. Framework conditions of this kind would force customer relationships into rigid channels and would make both market entry and innovation harder. Flexible formation of customer relationships – throughout the value creation network – will play a decisive role in determining the economic order in the future. It is thus very important to launch a debate on the free and fair use of data and how to guarantee flexibility in customer relationships. In this respect the free flow of data is of utmost importance, in order to raise the potential of the digital economy. Data portability has to be assured with respect of innovation in a European framework.

3. Guidelines for a European Cybersecurity Concept

Cybersecurity is not only a basic need to help building trust in the digital world but also a prerequisite of the entire digital transformation of our industries. It is the ultimate objective of a European Cybersecurity Architecture to guarantee a safe and secure communication network both for the consumer and business side.

Building up trust on both the consumer and business side requires a competitive and high quality market of cybersecurity products and services. Our companies require specific cybersecurity design products and concepts that apply not only to B2C or B2B but also to device-to-device connection. In the near future, factories, any kind of devices or products, complex constructions or even entire value chains will be connected. The more virtual interfaces will be connected the higher will be the risk for security. The threat of cross-border cyberattacks, spying and manipulation by states, criminal networks of terrorists or individuals is constantly growing and needs to get the full attention of the political level. It should be of high concern for our governments to protect citizens from attacks against critical infrastructure such as energy, water, transport systems, healthcare etc. On the industry side, cybersecurity needs to apply to any device or virtual gateway. This asks for a bottom up approach of cybersecurity innovation, which can be defined as industrial security encompassing the shop and the office floor. Industrial security means security-by-design which has to be installed on hard- and software. We support the concept of giving identification and security trusted labels to every single device within complex or interconnected systems and processes. FIEEC and ZVEI are appreciating the creation of the cybersecurity PPP which will further develop the field of B2B cybersecurity towards a European approach.

Strengthening Networking on Security-Related Issues

Today, the companies of the electrical, electronic and digital industries are already interconnected with their customers, suppliers and employees. In the interest of promoting data security, ZVEI fosters an intensive exchange of information on security-related issues through discussion platforms based on mutual trust, cooperation on the development of guidelines, and the involvement of experts from government agencies. The goal is to establish an ongoing exchange of information between manufacturers, integrators and operators. In France, FIEEC works closely with public authorities, especially the National Agency for the Security of Information Systems (ANSSI) and the Committee for the Security sector (COFIS) to promote cybersecurity.

Willingness to invest to ensure a culture of security

Given the importance of data protection and security, companies must be willing to make long-term investments in measures needed to ensure it. Our organizations therefore call for their members to establish a culture of security that starts with senior management. The prerequisites for this are:

- making information security a top-level priority,
- implementing and evaluating risk-based, staged solutions (both in terms of technology and in organizational terms) on an ongoing basis,
- sharing information, for example in the framework of the government initiative “Alliance for Cyber Security” (“Allianz für Cybersicherheit”).

Cooperation on security incidents

Cooperation between companies and government agencies on a basis of mutual trust makes a valuable contribution toward strengthening risk awareness and data security. This applies in particular to situations in which security incidents have already occurred. ZVEI and FIEEC will strive to heighten this awareness in the electrical, electronic and digital industry.

4. Standardisation

The breath-taking pace of advanced technologies perpetually penetrating our economy and society will require flexible and on time applied standards of best performance. FIEEC and ZVEI agreed that norms and standards are of high importance with respect to the digitisation of industry. The EU Commission's priorities on ICT standardisation is a good starting point to further develop the dialogue with our industry as they are developing standards along their products, processes, services and new business models. This is the place where standards have to be developed in cooperation with industrial internet standardisation fora. Members of FIEEC and ZVEI need industry-driven, open as well as bottom-up standardisation procedures. Standardisation should be constituted like a publicprivate-
partnership between the economy and the public authority. FIEEC and ZVEI take the risk very serious that consortia standardisation setting could risk needed coherence of the standardisation system as a whole. Standardisation should always address the international market competition, with a completing, pro-active and constructive procedural management between law making and standardisation appears to be necessary. The digitisation of our economy and society equally requires a radical digitisation of standardisation. Standard-to-machine approaches and the wide connection and acceleration of processes have to stand in focus of the standardisation procedures. Pro-active standardisation could help to catch trends in time and react more flexible. We do not need cemented catalogues of standards but an open development in line with the global market environment. A reduction of complexity of standards will also lead to a reduction of time consuming standards processes. Law making is providing the basic demands, but standards are providing precise definition. The European Single Market is not the ultimate achievement of standardisation, but a starting point to address international standardisation settings.

***

FIEEC and ZVEI will continue to work together on all dimensions of the digitalisation of our society and economy. Both associations are committed to the Digital Single Market strategy of the European Union and take their responsibility as strong partners respectively this revolutionary and challenging process.

FIEEC
FEDERATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

French-German Joint Declaration

ZVEI: Die Elektroindustrie

July 6th 2016

Paris FRANCE

Europe is at a crossroads. One the one side, international cooperation and the digitalization of our world is going ahead with high speed. Both trends are leading to a need of further integration and unity of Europe in order to stay globally competitive. At the same time, Europe's single market with a seamless, barrier-free, cross border transfer of capital, goods, services and citizens, has become one of the most powerful economic regions in the world. This European success story reflects the key values of our EU undertaking. On the other side, political trends at EU Member State level go in the other direction as some parts of the European population wish for a more protected environment and lack fundamental trust into the future. After the UK vote to leave the EU, today's call for a new vision of a united Europe has never been heard so clearly in the European Union's history. Politicians across Europe will have to work together to draw the picture of a future Europe that generates trust, that appeals to the younger generation, that attracts the best talents, investments and business from around the world and that plays a strong international role, both economically and politically.

I° The French and German Electrical, Electronic and Digital Industries, key actors of the digital transformation of Europe

The French and German Electro-technical and Electronics Industries as organized in FIEEC and ZVEI, believe in Europe and in the project of the European Union. For our more than 4 600 member companies – representing large, small and medium-sized enterprises - and their over 1,249 million employees, an integrated Europe stands for common values, peace, freedom, security, growth and future wealth.

The digitisation is at the heart of our economy and society. It is a main driver of our future and we have to master these opportunities. The digital economy will create new lead markets for Europe, such as industry, energy, mobility, health and building – with new business models and jobs.

The French and German Electro-technical and Electronics Industries are strongly committed to contribute to the debate on the digitisation of the economy with ideas and solution proposals that offer Europe new opportunities at global scale. As key actors of the digital transformation, we are responsible partners to the politics and society and we take our role seriously.

II° A stronger partnership between public authorities and industry to succeed in the digital transformation

The French and German Electro-Technical and Electronics Industries call on the policy leaders in Europe to jointly promote with us:

- The improvement of the Internal Market especially through an integrated Digital Single Market taking fully into account the competitiveness of our industries at global level;
- An Industrie du futur / Industrie 4.0 check as part of the innovation principle for all future legislation and regulation;
- A business-friendly regulatory environment, fostering the development of the digital economy and Industrie du futur / Industrie 4.0 solutions, enabling companies and new businesses to flourish;
- A business-oriented standardization system based above all on industry needs;
- An efficient market surveillance to create a level-playing field with our non-European competitors;
- A European trade policy taking into account our global business activities and allowing free and fair market access on the basis of a multilateral trade strategy;
- The reinforcement of digital security and trust at all levels;
- The establishment of a cybersecurity culture and guidelines for a European cybersecurity concept;
- A framework combining the protection of personal data and industrial data, taking into account innovation capacities;
- The development of the skills needed for the digital age.

III° FIEEC and ZVEI recommend on Digital Economy with respect to data, cybersecurity and standardisation

The French and German Electro-Technical and Electronics Industries have on the occasion of their joint conference on 6th July 2016 in Paris developed a set of ideas related to Industrie du futur / Industrie 4.0 and the Digital Economy, with detailed recommendations on the use of data, cybersecurity and standardisation which they would like to present to the political decision-makers today.

Gilles SCHNEPP
FIEEC President

Michael ZIESEMER
ZVEI President

FIEEC and ZVEI, both members of ORGALIME their European association, are one of the major technological sectors in Europe representing 4 600 companies, 1,249 million employees and a turnover of 278,5 billion euros.

La directive « *Network Information And Security* » (NIS)

Messages Clés

- La directive européenne NIS a été publiée en juillet 2016 et devra être transposée dans les Etats membres de l'UE d'ici le 9 mai 2018.
- L'objectif de cette directive est d'instaurer un « niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union Européenne » afin de pallier les attaques informatiques et leurs impacts souvent destructeurs.
- Elle cible essentiellement les « Opérateurs de Services Essentiels » (OES) ainsi que les « Fournisseurs de services numériques » sur lesquels elle fait peser de nouvelles obligations (obligation notamment d'améliorer leur capacité à résister aux cyberattaques, de notifier un incident etc.),
- En cas de non-respect de cette directive, il appartient à l'Etat membre de sanctionner l'entreprise en cause de façon discrétionnaire (efficace, proportionnée et dissuasive).

1. Contenu

La directive NIS couvre 7 secteurs d'activités : l'énergie, les transports, les banques, les infrastructures financières, la santé, l'eau et les infrastructures digitales.

Il appartiendra aux Etats membres de notifier quelle entreprise constitue un « opérateur de service essentiel» dans le cadre de ces secteurs à l'aide de 3 critères spécifiques mentionnés par la directive :

1. L'entité doit fournir un service essentiel pour le maintien des activités sociétales et/ou économiques.
2. La fourniture de ce service dépend de systèmes de réseau et d'information.
3. Un incident aurait des effets perturbateurs considérables sur la prestation de ce service.

La directive prévoit également :

➔ Le renforcement des exigences de sécurité concernant les « Opérateurs de Services Essentiels » (OES) et des « Fournisseurs de services numériques » (ex : marchés en ligne, moteurs de recherche ou encore fournisseurs de services Cloud). Ces acteurs devront ainsi prendre des mesures de prévention des risques, s'assurer de la sécurité des réseaux et des systèmes informatiques et devront être capables de notifier et de gérer les incidents dont elles pourraient faire l'objet.

Pour déterminer si un incident doit être notifié par un OES, la directive indique 3 paramètres à prendre en compte :

- Le nombre d'utilisateurs affectés.
- La durée de l'incident.
- La zone géographique touchée.

A noter : Les exigences imposées aux OES seront plus contraignantes que les exigences applicables aux fournisseurs de services.

Les définitions d'OES et d'Opérateurs d'Importance Vitale (OIV) en France sont équivalentes, bien que la définition relative aux OES soit plus étendue que la définition réservée aux OIV.

Pour rappel, les OIV sont des opérateurs reconnus par l'Etat comme exerçant des activités dont le dommage, l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait de quelque manière que ce soit d'avoir des conséquences majeures sur les capacités de survie de la Nation ou sur la santé ou la vie de la population. Plus de 200 sont recensées en France (source : ANSSI). Cette liste pourrait être étendue par l'ANSSI en charge de la transposition de cette directive.

➔ Les coûts nécessaires à l'implémentation de ces mesures n'ont pas été clairement déterminés. L'ANSSI a ainsi affirmé que les « fournisseurs de services (devront être) capables de mettre en oeuvre ces différentes mesures à des coûts acceptables ».

2. Actions/ Position FIEEC

La FIEEC, en lien avec ses partenaires et notamment Orgalime, a suivi avec attention les travaux menés sur cette directive. Notre profession veille de manière accrue à sa transposition notamment en promouvant des exigences réglementaires et des systèmes de certification au niveau européen.

La FIEEC souhaite également attirer l'attention quant à la définition des opérateurs de service essentiels. Eu égard à son contenu, cette définition cible des acteurs très variés en nature et en taille dont l'impact «sociétal» en cas de compromission serait différent et devrait justifier de mesures adaptées. La définition des OIV et SSIV faite par la Loi de Programmation Militaire ne concerne qu'une infime partie de ces acteurs relevant du plus haut niveau de sécurité (domaine souverain) et pour lesquels la directive prévoit que les dispositions (de publication des incidents notamment) ne s'appliquent pas. Il convient donc d'être vigilant sur la manière dont l'ANSSI entend décliner cette directive NIS en dehors de la Loi de Programmation Militaire.

Par ailleurs, il conviendrait de préciser le procédé selon lequel cette directive s'appliquera aux opérateurs de services essentiels opérant depuis l'extérieur de l'Union. Ce manque de clarté est également constaté relativement à la méthode d'harmonisation à mettre en place afin que chaque état membre puisse appliquer la directive NIS aux acteurs qui opèrent dans plusieurs pays.

Quant aux mentions attraites à la publication des incidents de sécurité et à la mise à disposition de l'information en vue de la protection des autres acteurs, il serait intéressant de pouvoir ouvrir un dialogue avec l'ANSSI afin de s'informer sur le procédé de leur mise en œuvre.

Pour consulter la directive NIS : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Pour consulter l'arrêté du 10 juin 2016 relatif aux OIV « Produits de santé » : https://www.legifrance.gouv.fr/eli/arrete/2016/6/10/PRMD1608293A/jo

Pour consulter l'arrêté du 17 juin 2016 relatif aux OIV « Alimentation » : https://www.legifrance.gouv.fr/eli/arrete/2016/6/17/PRMD1612419A/jo

Pour consulter l'arrêté du 17 juin 2016 relatif aux OIV « Gestion de l'eau » : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032749580&categorieLien=id

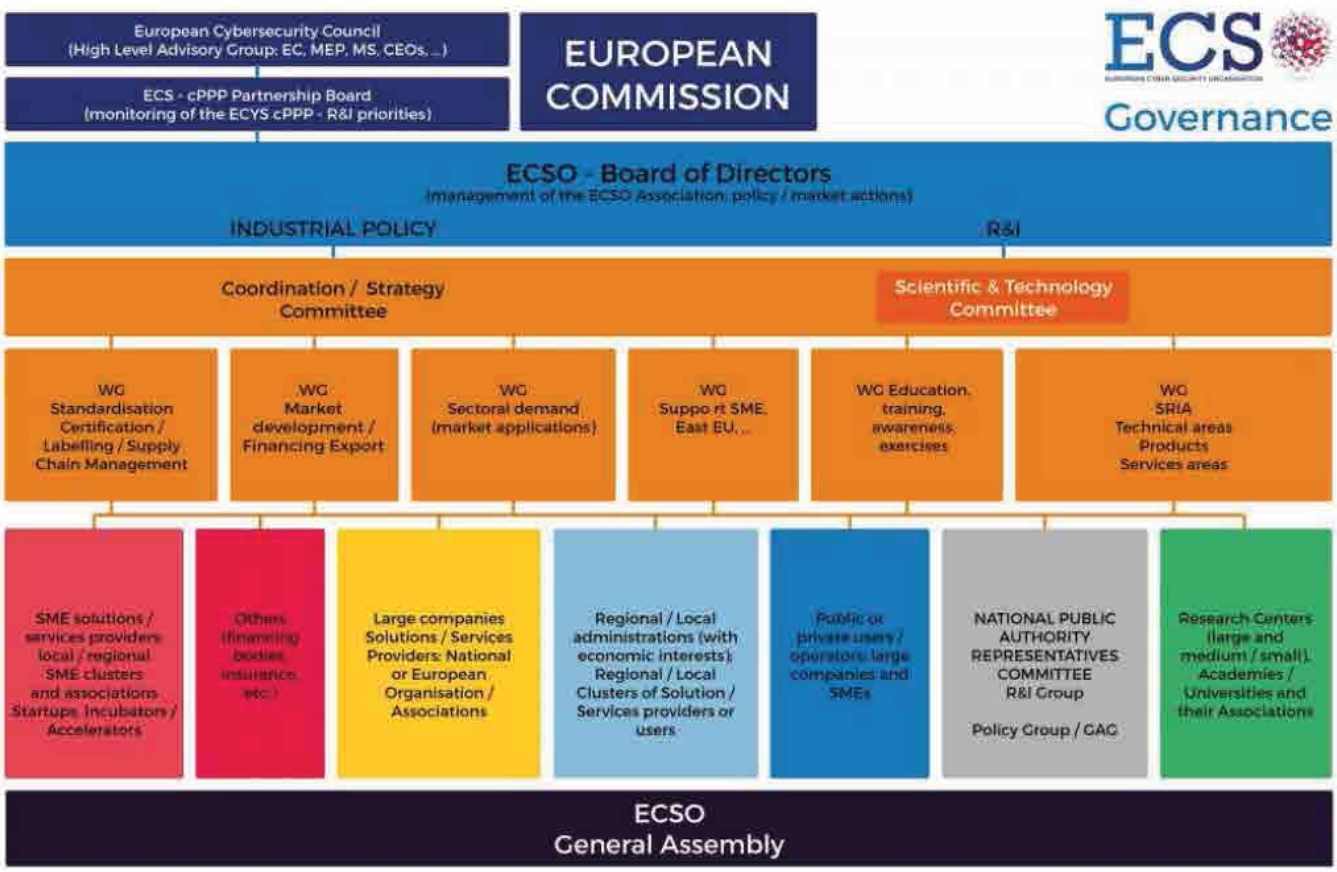
CYBERSECURITY PUBLIC-PRIVATE PARTNERSHIP (LE CPPP CYBERSÉCURITÉ)

Messages clés

- Ce partenariat public-privé est un contrat créé à l'initiative de l'UE et conclu le 5 juillet 2016 entre la Commission européenne et l'ECSO, une association européenne créée pour porter ce cPPP et représentant un large panel d'acteurs (industriels, représentants des Etats membres, centres de recherche, clusters etc).
- Son objectif est de stimuler la coopération entre les Etats membres de l'UE, les acteurs industriels et les utilisateurs dans les processus de recherche et d'innovation et de renforcer la compétitivité du marché européen de la cybersécurité (notamment dans les secteurs de l'énergie, de la santé, des transports ou encore de la finance).
- En additionnant les investissements de l'UE et les apports des partenaires privés, ce partenariat devrait générer 1,8 milliard d'euros d'investissements d'ici 2020 dont 450 millions de fonds publics investis dans le cadre du programme Horizon 2020.

1. Contenu

Organisation de l'ECSO :



- La France est fortement représentée au sein de l'ECSO notamment via l'ANSSI, qui a été désignée comme membre du Comité des Directeurs de l'ECSO mais aussi via une forte présence d'ACN (élection de Philippe Vannier et d'Alexis Caurette (Atos), de François Lavaste (Airbus Defence and Space).
- Ce cPPP a 3 objectifs stratégiques principaux :
  - » Assurer la présence et la croissance des industriels européens impliqués dans la cybersécurité sur le marché international.
  - » Assurer la protection du marché unique numérique européen face à la cybermenace.
  - » Créer une offre européenne solide en cybersécurité basée sur les principes de compétitivité et de concurrence équitable.
- Afin de développer ce marché européen, le cPPP vise également à :
  - » Faciliter l'accès au financement pour les petites entreprises actives dans le domaine de la cybersécurité (notamment via le plan d'investissement de l'UE).
  - » Mobiliser et lever des fonds publics et privés pour pouvoir contribuer au développement et à la mise en œuvre d'orientations européennes en cybersécurité, de réglementations et de normes spécifiques (et de servir de relais pour la mise en œuvre d'autres législations européennes telles que la directive NIS, le règlement eIDAS etc.).
  - » Accélérer la mise sur le marché des solutions innovantes en cybersécurité.
  - » De démontrer l'importance des enjeux de la cybersécurité, d'accroître leur connaissance et celle des solutions existantes auprès des décideurs publics, des entreprises et des citoyens.
  - » La mise en place d'un cadre européen de certification pour les produits de sécurité des TIC est envisagée d'ici fin 2017.

2. Actions / Positions FIEEC

Plusieurs acteurs de la FIEEC, dont notamment ACN, ont participé à l'ensemble des travaux préparatoires ayant conduit au lancement de ce cPPP, directement et à travers l'Orgalime.

Cette initiative est pleinement soutenue par notre profession qui participe activement aux travaux menés dans ce cadre.

Pour consulter le contrat de partenariat public-privé cybersécurité : http://www.ecs-org.eu/documents/contract.pdf

Pour plus d'informations sur le contenu du cPPP : http://www.ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf

Pour consulter la liste des membres de l'ECSO : http://www.ecs-org.eu/documents/ecso-glossary.pdf

Le Réglement « *Electronic Identification and Signature* » (eIDAS)

Messages clés

- Adopté en juillet 2014 et entré en vigueur le 1er juillet 2016, eIDAS est un règlement européen qui abroge et remplace la directive sur les signatures électroniques en vigueur depuis 1999.
- Son objectif est de mettre en place un environnement règlementaire fiable permettant des interactions sécurisées entre le monde des entreprises, les citoyens et les autorités publiques et de faciliter l'émergence du marché unique numérique.
- Il concerne essentiellement les autorités publiques des Etats membres de l'UE et les prestataires de services de confiance établis sur le territoire de l'UE.

1. Contenu

Le règlement est divisé en 2 volets :

1. A propos de l'identification électronique

Ce cadre juridique autorise la reconnaissance mutuelle des moyens d'identification utilisés par les Etats membres de l'Union Européenne (ce champ s'applique uniquement au secteur public) dans un objectif de simplification et de réduction des coûts. Chaque Etat membre doit reconnaître les moyens d'identification électronique issus des systèmes d'identification électronique des autres Etats membres, à condition que le système en question respecte certaines conditions et ait été notifié à la Commission européenne. Il appartient à chaque pays de décider quels systèmes d'identification électronique notifier à la Commission européenne et de préciser le niveau de garantie de la transaction (faible, substantiel ou élevé).

Cette reconnaissance mutuelle des moyens d'identification électronique par les Etats membres sera obligatoire dès le 29 septembre 2018.

2. A propos des signatures électroniques :

- Les règles existantes quant aux sceaux et aux signatures électroniques visent à être harmonisées.
- Cette réglementation permet la traçabilité de l'identité électronique de chaque individu et autorise des tierces parties à interroger ces systèmes gratuitement en ligne.
- La signature électronique ainsi que les services de vérification restent recevables comme éléments de preuve dans le cadre d'une action en justice.

Cette réglementation introduit 3 niveaux de fiabilité des signatures :

- La signature électronique,
- La signature électronique avancée,
- La signature électronique qualifiée.

Le règlement opère une distinction entre les services qualifiés de confiance et les services non qualifiés, et ce, via la création d'un label destiné aux fournisseurs de services de confiance garantissant le

respect de la réglementation eIDAS.

En France, l'ANSSI a été désignée comme organe de contrôle, elle délivre et retire ce certificat aux prestataires de services de confiance (des référentiels d'exigences applicables aux différents services de confiance ont été publiés). Ce niveau de fiabilité est le seul à pouvoir garantir la reconnaissance mutuelle de sa validité par l'ensemble des Etats membres de l'UE.

Par ailleurs, l'ANSSI, chargée de la mise en œuvre de ce règlement, prévoit la création d'un certificat délivré aux prestataires de services de confiance permettant de garantir leur conformité à la réglementation eIDAS.

2. Actions / Positions FIEEC

Cette initiative est pleinement soutenue par notre profession qui participe activement aux travaux menés dans ce cadre.

Pour consulter le règlement eIDAS : http://eur-lex.europa.eu/legalcontent/FR/TXT/?uri=CELEX%3A32014R0910

Le Règlement « General Data Protection Régulation » (GDPR)

Messages clés

- Le GDPR est un règlement européen publié en mai 2016. Il entrera en application dans les Etats membres de l'UE le 25 mai 2018.
- L'objectif de ce règlement est de renforcer la protection des données personnelles dans tous les Etats membres de l'UE.
- Il cible un large scope d'entreprises : les entreprises collectant, gérant et/ou stockant des données ainsi que leurs sous-traitants s'ils exercent une activité sur le territoire de l'UE et traite des données personnelles au sens large : informations des employés, des clients, partenaires, prospects, données dans les ordinateurs, terminaux mobiles, serveurs etc.
- Il protège davantage le citoyen (instaure un droit à l'oubli, un droit à la portabilité des données etc.) et fait peser de nouvelles obligations sur les entreprises de traitement des données et leurs sous-traitants (instaure la mise en place d'une analyse d'impact sur la vie privée etc.).
- En cas de non-respect de ce règlement, les entreprises peuvent se voir infliger le paiement d'une lourde amende pécuniaire pouvant aller jusqu'à 4% de leur chiffre d'affaires mondial annuel.

1. Contenu

Ce règlement, remplaçant la directive 95/46/CE, a été introduit afin de conférer un niveau équivalent de protection des données personnelles dans tous les Etats membres de l'Union Européenne, de rapprocher les législations nationales pour supprimer les obstacles à la transmission transfrontalière des données, et de donner aux citoyens le contrôle de leurs données personnelles.

Protection renforcée des citoyens :

- Renforcement général des droits des citoyens : renforcement du droit d'information sur la manière dont les données sont traitées, création de nouveaux droits tels que le droit à la portabilité des données, droit à l'oubli (droit pour un individu de demander le retrait ou l'effacement de toute information ou donnée qui lui porte préjudice), droit à la limitation du traitement des données.
- Lorsque le traitement repose sur le consentement de la personne et non l'exécution d'un contrat ou encore d'une mission d'intérêt public, ce consentement des personnes concernées doit être éclairé, libre et informé.

Obligations supplémentaires pesant sur les entreprises à partir du 25 mai 2018 :

- Mise en place d'une analyse d'impact sur la vie privée (ou Privacy Impact Assessment) du traitement réalisé par le professionnel, et notamment une évaluation des risques et des mesures à mettre en place pour préserver les droits et les libertés des individus concernés.
- Obligation de désigner un DPO (Délégué à la Protection des Données) en charge de la surveillance de la conformité des mesures de protection mises en place au sein de l'entreprise aux normes européennes.

- Signalement des fuites de données sous 72H (le délai court à partir du jour où l'entreprise a connaissance de cette fuite): formalités à respecter auprès de la CNIL pour la France (indiquer la nature de la fuite, ses conséquences, les mesures prises ou à prendre en aval).

Sanctions :

- En cas de non-respect des dispositions, le règlement prévoit une sanction pécuniaire pouvant aller jusqu'à 20 000 000 € d'amende ou 4% du chiffre d'affaires annuel mondial total de l'entreprise mise en cause ((en pratique, les autorités nationales tiendront compte de la nature, la gravité, la durée de la violation, de l'application de code de conduite ou de mécanisme de certification approuvé).
- Les entreprises devront offrir la plus grande transparence aux citoyens concernant la manière dont les données récoltées sont traitées. L'information doit être «concise, transparente, intelligible et dans une forme aisément accessible en utilisant un langage clair ».

2. Actions / Position FIEEC

La FIEEC a suivi avec attention la genèse de ce texte et s'attache désormais à préparer en collaboration étroite avec la CNIL, l'entrée en application du Règlement prévue pour mai 2018. En effet, il est essentiel que les acteurs de notre profession se préparent à la mise en œuvre pratique des nouvelles mesures. Un premier colloque d'information a eu lieu avec la CNIL le 22 juin 2016 et la FIEEC participe activement à tous les travaux en cours en vue de contribuer à l'élaboration d'un cadre harmonisé.

Pour consulter le GDPR : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Le projet de règlement « *ePRIVACY* »

Messages clés

- La Commission européenne a présenté en janvier 2017 une proposition de règlement ePrivacy en matière de respect de la vie privée pour toutes les communications électroniques. Elle vise à remplacer la directive européenne «Vie privée et communications électroniques » de juillet 2002.
- Ce règlement compléterait le Règlement Général sur la Protection des Données (GDPR). Il serait d'ailleurs applicable concomitamment au GDPR, soit dès le 25 mai 2018. Si le contenu de ces deux textes convergent en matière de données personnelles, c'est le règlement ePrivacy qui s'appliquerait dans les communications électroniques. Toutefois, en cas de vide juridique dans le règlement ePrivacy, c'est le GDPR qu'il conviendrait de respecter.
- Son objectif est d'assurer la protection de la confidentialité des communications électroniques des citoyens et de leurs données se trouvant dans leurs ordinateurs, tablettes et smartphones. Il vise à instaurer des règles communes à l'ensemble des Etats-membres de l'Union Européenne afin de renforcer la confiance des citoyens dans le Marché unique numérique.
- Ce règlement ePrivacy a pour ambition de renforcer la protection des données des citoyens notamment en élargissant son champ d'application aux fournisseurs de communications électroniques « over-the-top » et en protégeant les métadonnées (lieu, date, heure de l'envoi/réception du message etc.) en plus du contenu des communications.
- Il prévoit également des mesures de simplification relatives aux cookies ou au démarchage réalisé par les entreprises commerciales.

1. Contenu

Elargissement du champ d'application de la directive de 2002 à de nouveaux acteurs

- Le champ d'application du projet de règlement s'appliquera aux fournisseurs de communications électroniques « *over-the-top* » en plus des opérateurs de télécommunications traditionnels ciblés par la directive de 2002.

Elargissement du champ des données protégées

- Les communications électroniques envoyées via les ordinateurs, les tablettes ou encore les smartphones des citoyens feront l'objet d'une confidentialité renforcée.
- Les données visées sont les données contenues dans le corps des messages et courriers électroniques mais comprennent également les métadonnées, telles que l'heure de l'envoi ou de la réception du message, le lieu de l'envoi du message etc. Pour accroître la compétitivité et le développement du Marché unique numérique, ce règlement permettrait aux opérateurs de télécommunications traditionnels de pouvoir utiliser ces métadonnées afin qu'ils puissent améliorer ou créer de nouveaux services (si l'utilisateur consent à donner accès à ses métadonnées). Il prévoit toutefois leur anonymisation ou leur suppression si l'utilisateur n'a pas consenti à leur diffusion ou leur utilisation.

- Face à l'accroissement de l'utilisation des objets connectés, le règlement prévoit également de s'appliquer aux données échangées de machine à machine (MtoM) afin de promouvoir et de sécuriser l'internet des objets.

Simplification des réglages des cookies et création de nouvelles mesures relatives au démarchage commercial

- Le texte prévoit des dispositions spécifiques à l'égard des cookies. Leur système d'acceptation ou de refus tend à être simplifié : aucun consentement ne sera préalablement requis pour les cookies qualifiés de non intrusifs utilisés pour améliorer les recherches de l'internaute. Les utilisateurs pourront modifier les paramètres relatifs aux cookies pour éviter de ne devoir systématiquement cliquer sur « accepter » ou « refuser » les cookies.
- La proposition de la Commission européenne vise également à renforcer les mesures relatives aux appels marketing. Elle prévoit que les usagers devront nécessairement donner leur consentement préalable pour recevoir des appels commerciaux automatiques, des SMS ou des emails.
- Les entreprises à l'origine de telles démarches commerciales ne pourront plus appeler en mode « anonyme ». Elles devront afficher leur numéro de téléphone ou utiliser un préfixe identifiable par l'interlocuteur.

Contrôle du respect des mesures de cette proposition de règlement et sanctions prévues

- Le respect de ces nouvelles règles sera contrôlé par les mêmes autorités indépendantes nationales en charge du respect du règlement GDPR, soit la CNIL en France.
- Ce règlement entrera en vigueur 20 jours après sa publication au JOUE et sera applicable le 25 mai 2018.
- Les sanctions en cas de violation de ce règlement sont des sanctions administratives. L'article 23 prévoit pour le contrevenant de payer une amende dont le montant peut atteindre 10 millions d'euros ou de verser 2% du chiffre d'affaire annuel mondial de l'entreprise réalisé l'année précédente. En cas de violation du principe de confidentialité des communications, du non-respect du traitement des données de communications électroniques ou de leur délais d'effacement, le montant de l'amende peut atteindre 20 millions d'euros ou être équivalent à 4% du chiffre d'affaire annuel mondial réalisé l'année précédente. D'autres sanctions peuvent être appliquées à la discrétion des Etats-membres de l'Union Européenne, à condition d'être efficaces, proportionnelles et dissuasives.

2. Position de la FIEEC

Notre profession attend de ce règlement de savoir concilier la protection des données des utilisateurs avec les intérêts des acteurs de l'industrie du numérique en leur permettant de continuer à développer leurs activités et de contribuer à rendre le marché numérique européen toujours plus innovant.

3. Documents de référence

Pour consulter le projet de règlement ePrivacy : http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241

Pour consulter le communiqué de presse publié par la Commission européenne : http://europa.eu/rapid/press-release_IP-17-16_en.htm

Pour consulter l'infographie relative au projet de règlement ePrivacy : https://ec.europa.eu/digital-single-market/en/news/stronger-privacy-rules-electronic-communications

Les biens à double usage

Définition des biens à double usage

Les biens à double usage sont définis par l'article 2 du règlement européen 428/2009 comme étant « les produits, y compris les logiciels et les technologies, susceptibles d'avoir une utilisation tant civile que militaire ; ils incluent tous les biens qui peuvent à la fois être utilisés à des fins non explosives et entrer de manière quelconque dans la fabrication d'armes nucléaires ou d'autres dispositifs nucléaires explosifs ».

1. Les enjeux et la réglementation des biens à double usage

Compte-tenu de leur spécificité, les exportations des biens et technologies dits «à double-usage» (BDU) sont soumises à un contrôle mis en œuvre par l'Etat pour lutter contre l'accumulation déstabilisante d'armes dans certaines régions du monde.

Les biens à double usage soumis à une autorisation d'exportation sont listés dans l'Annexe I du règlement européen 428/2009. Cette liste s'applique aux biens exportés par les Etats-membres de l'Union Européenne vers n'importe quel pays du monde. Certains biens peuvent toutefois être interdits d'exportation ou être soumis à des mesures restrictives d'exportation eu égard au pays destinataire ou à l'utilisation finale du bien selon des considérations géopolitiques (des biens ont par exemple étaient mis sous embargo vers l'Iran avant la levée partielle des sanctions à l'encontre de ce pays).

Pour savoir si un bien entre dans ce cadre réglementaire dédié, des listes sont établies par des régimes de contrôle. Ces régimes sont des instances internationales comme l'Arrangement de Wassenaar qui compte près de 40 pays signataires et dont le contrôle porte sur les biens industriels.

Si un bien est listé, alors l'entreprise souhaitant l'exporter doit soumettre une demande de licence d'exportation auprès de l'autorité nationale concernée. En France, cette autorité spécialisée est le Service Des Biens à Double Usage (SBDU), rattaché à la Direction Générale des Entreprises. Cette procédure est obligatoire pour les biens ciblés, sous peine d'être sanctionné administrativement et/ou pénalement.

Le document de référence en matière des biens à double usage est le Règlement européen 428/2009. C'est ce texte qui fait aujourd'hui l'objet de débats entre la Commission européenne qui souhaite le réviser et les industriels. En effet, des travaux sont actuellement en cours visant à renforcer ce règlement dont les nouvelles dispositions pourraient alourdir les obligations pesant sur les industriels exportateurs de biens à double usage. Des discussions autour de l'introduction d'une clause de due diligence ou encore de l'extension du champ de la « *catch all clause* » sont ainsi en cours entre les acteurs concernés : institutionnels, industriels et législateurs.

2. Santions

En cas de violation de la réglementation en vigueur, plusieurs types de sanctions sont prévus. Le Code des douanes prévoit ainsi des sanctions pénales à l'égard de tout fait d'importation ou d'exportation sans déclaration lorsqu'il s'agit de produits prohibés. Selon l'article 38.1 du code susmentionné, un produit est considéré comme prohibé lorsque son exportation est interdite ou soumise à restriction ou à des formalités particulières. L'article 414 du code prévoit ainsi une peine d'emprisonnement pouvant atteindre 3 ans, de la confiscation de l'objet de la fraude, des moyens de transport et de l'objet ayant servi à masquer la fraude. Cette peine peut être complétée par le paiement d'une amende dont montant est compris entre 1 et 2 fois la valeur de l'objet de la fraude.

Le Code pénal prévoit également des sanctions dans les cas les plus graves dont certaines atteintes aux intérêts fondamentaux de la Nation. L'article 411-6 prévoit ainsi des sanctions pouvant atteindre 15 ans de détention criminelle et 225 000 euros d'amende.

Des sanctions administratives et pénales spécifiques à l'exportation des biens à double usage intégrant de la cryptographie sont également prévues. Tout manquement à la réglementation peut être puni jusqu'à deux ans d'emprisonnement et de 30 000 euros d'amende.

3. Actions / Position FIEEC

La FIEEC s'est saisi de ces enjeux à travers la création il y'a près de 20 ans d'une commission ayant pris la forme d'un syndicat : le SIEPS, le Syndicat des Industries Exportatrices de Produits Stratégiques.

Le SIEPS a en effet pour mission de suivre et d'influencer l'évolution des réglementations en la matière. Il interagit avec les administrations françaises et les instances européennes chargées des questions de biens à double usage. Associé à ce récent débat, il a ainsi décidé de publier une position en réaction au texte de révision rédigé par la Commission européenne.

Cette représentation est ainsi essentielle pour pouvoir porter la voix de nos professions dans le domaine des biens à double usage et défendre au mieux les intérêts de nos industriels.

L'industrie française exportatrice de produits stratégiques reconnait en effet le travail conséquent effectué par la Commission européenne en proposant une toute nouvelle réglementation pour l'exportation des biens à double usage mais elle considère que le résultat n'est pas à la hauteur des propositions, des attentes et des simplifications /améliorations espérées et des indications exprimées par l'industrie, suite à une série d'enquêtes et de questionnements effectués par la Commission et ses consultants.

Ce positionnement et le rôle du SIEPS sont ainsi essentiels car ils portent la voix de nos professions dans le domaine des biens à double usage et défendent au mieux les intérêts de nos industriels.

Pour consulter le règlement 428/2009 : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:fr:PDF

Propositions du CICS (Conseil des Industries de la Confiance et de la Sécurité)

Innovation et investissements publics – sur trois ans :

- Investir un milliard dans l'innovation technologique ;
- Porter à un milliard par an les investissements en matériels et services technologiques pour les missions de sécurité de l'Etat.

La sécurité socle indispensable à toute vie sociale et économique

- Inscrire la politique publique de sécurité au sein des politiques publiques comme domaine particulier et essentiel ;
- Piloter et coordonner l'ensemble des dépenses de sécurité de l'Etat dans une perspective pluriannuelle.

Satisfaire les besoins en s'appuyant sur les possibilités d'accélérer les investissements et l'innovation

- Inciter les acheteurs publics à utiliser toutes les dispositions permises par le droit pour accélérer les investissements ;
- Relever l'objectif actuel (2% en 2020) d'achats publics innovants pour les PME de sécurité.

Renforcer les investissements publics et privés dans les solutions de sécurité incontournables

- Développer les labels de confiance et mettre en place des incitations fiscales pour l'équipement des entreprises en solutions de cybersécurité de confiance et labellisés par l'ANSSI ;
- Mettre en place une politique d'accompagnement des entreprises pour le renforcement de la protection des sites sensibles ;
- Déployer des documents d'identité, CNI et permis de conduire, de nouvelle génération, électroniques et sécurisés dès 2018 ;
- Mettre en œuvre un système d'identification électronique et une politique « public-privé » de déploiement des usages de ce système, qui fassent de la France le pays leader au sein de l'UE et permettent la construction d'un internet de confiance ;
- Développer une politique d'incitation pour la mise en place de solutions évoluées de sécurité urbaine et de gestion de crise dans la ville connectée ;
- Renforcer, lors de grands événements, la capacité de coopération et d'interopérabilité technique des acteurs à tous les échelons, avec en perspective les jeux olympiques de 2024.

Dans le contexte post-Brexit, relancer des initiatives européennes ambitieuses en matière de sécurité et de souveraineté

- La France doit jouer un rôle de leader pour développer une politique européenne de souveraineté en matière de sécurité et les conditions d'une base industrielle de sécurité européenne forte et indépendante ;
- Lancer des grands programmes capacitaires européens en matière de sécurité, notamment pour la cybersécurité et la gestion des frontières.

Développer notre ambition sur les ruptures majeures – La France championne de l'Internet de confiance

- Mettre en place un cadre réglementaire et une politique d'innovation qui autorisent et encouragent l'usage des nouvelles technologies ;
- Conduire des expérimentations innovantes de confiance avec des données réelles (plateformes / *openlabs*).

Elever l'efficacité de la sécurité et la résilience du pays par une gouvernance claire et unifiée

- Créer des commissions spécialisées sur la sécurité à l'Assemblée nationale et au Sénat ;
- Mettre en place une gouvernance transverse plus structurée entre les principaux ministères en charge de la sécurité ;
- Créer une agence nationale en charge des programmes de sécurité.

La sécurité* est un instrument de la liberté publique et un domaine où l'attente de tous se fait plus pressante à mesure que s'aggrave la perception des menaces. Nous avons ainsi besoin de mieux lutter contre un terrorisme qui s'exacerbe, mais aussi de rehausser le niveau de protection et de résilience contre les dangers traditionnels (risques naturels, technologiques, criminalité), et enfin d'assurer la sécurité dans l'univers numérique, socle d'une nouvelle économie. Ce nouvel enjeu commande de pouvoir proposer des outils performants pour la protection des citoyens et celle de leur vie privée et des libertés. La réponse à ces besoins sollicite les pouvoirs publics, les chercheurs et les industriels, elle peut être source d'innovations, de création de valeur et d'emplois, mais elle appelle de la part de l'Etat une gouvernance unifiée et une action renforcée pour franchir une étape décisive.

C'est la raison pour laquelle les industriels français de la sécurité, grands groupes, ETI, PME et start-tups, réunis au sein du CICS, tiennent à profiter du débat national ouvert à l'occasion de la campagne électorale pour formuler publiquement leurs propositions en faveur d'une politique ambitieuse et d'un renforcement de l'action publique dans le domaine de la sécurité. Cette politique vise la sécurité de la nation comme le leadership mondial de la filière d'excellence des industries de sécurité.

1. La sécurité est le socle indispensable à toute vie sociale et économique

La reconnaissance de son caractère unique, incontournable et stratégique doit s'accompagner de dispositions concrètes en termes de gouvernance, de financement et d'objectifs. Il faut réserver à la sécurité un traitement qui combine la même vision pluriannuelle que celle donnée au domaine de la défense par les lois de programmation et un niveau de financement au moins aussi favorable que celui des domaines civils les plus privilégiés. Au-delà des paroles, il faut relever les budgets et les ambitions, donner une véritable impulsion. Une stratégie public-privé et une politique industrielle de la sécurité doivent être établies sur ces bases et démontrer la vision, la volonté et l'engagement communs de l'Etat et du secteur privé.

A cette fin, le CICS recommande :

- **d'inscrire la politique publique de sécurité au sein des politiques publiques comme domaine particulier et essentiel ;**
- **de piloter et coordonner l'ensemble des dépenses de sécurité de l'Etat dans une perspective pluriannuelle.**

** Le CICS se réfère à la sécurité au sens de la protection contre les actes malveillants et de la gestion de crises (sécurité intérieure, sécurité urbaine, protection des transports, des infrastructures, contrôle des flux et protection des frontières, sécurité du numérique, lutte contre la fraude et la contrefaçon, protection des entreprises, …).*

2. Satisfaire les besoins en s'appuyant sur les possibilités d'accélérer les investissements et l'innovation

L'évolution des usages et des technologies, comme des menaces, génère des besoins qu'il faut satisfaire le plus vite possible dès qu'ils sont avérés et biens instruits. Le droit offre de nombreuses formules pour permettre des réponses très rapides. Ainsi, le service d'alerte et d'information des populations (SAIP), s'appuyant sur internet et les applications mobiles, a pu être mis en place très rapidement. Ces dispositions sont aujourd'hui encore peu utilisées et il est souhaitable que Etat les exploite toutes pour accélérer les investissements. Il convient également de renforcer l'impact des PME innovantes en leur permettant de prendre une plus grande part dans les achats publics, et d'utiliser les dispositions légales permettant de restreindre les consultations sur les achats de sécurité sensibles.

A cette fin, le CICS recommande :

- **que les acheteurs publics utilisent toutes les dispositions permises par le droit pour accélérer les investissements ;**
- **de relever l'objectif actuel (2% en 2020) d'achats publics innovants pour les PME de sécurité.**

3. Renforcer les investissements publics et privés dans les solutions de sécurité incontournables

Sous quelque forme que puissent se matérialiser les agressions dont nous sommes menacés, deux domaines qui constituent autant de créneaux de vulnérabilité appellent une amplification des efforts déjà engagés :

- Cybersécurité : Le secteur économique lui-même doit renforcer son niveau d'équipement, particulièrement en cybersécurité. Il faut mettre en place des programmes capacitaires ambitieux et des dispositifs d'incitation pour accroitre l'investissement des entreprises dans leur protection et renforcer la politique de labels qui distingue les produits et acteurs de confiance.
- Sites sensibles : indispensables à la continuité de la vie économique, ces sites doivent élever leur niveau de protection. Adaptée à la menace et à la réalité de chaque site, celle-ci va intégrer de nouveaux outils innovant telle que des services d'alerte prédictive. Il est nécessaire d'aider les entreprises opératrices de sites à s'équiper au juste niveau et de façon évolutive.

A cette fin, le CICS recommande :

- **de développer les labels de confiance et mettre en place des incitations fiscales pour l'équipement des entreprises en solutions de cybersécurité de confiance et labellisées par l'ANSSI ;**
- **de mettre en place une politique d'accompagnement des entreprises pour le renforcement de la protection des sites sensibles.**

D'autres domaines appellent également une politique d'investissement très attendue :

- Identité : Les services de l'Etat sont encore trop peu équipés en technologies à l'état de l'art, en net décalage avec les pays comparables, par exemple en matière de solutions d'identité essentielles notamment pour la lutte contre le terrorisme. Une identité sûre est et sera un enjeu de toute première importance. Des initiatives sont indispensables pour assurer que tous les Français disposent d'une identité forte, sûre et simple à utiliser.
- Ville sûre : les nouveaux usages et technologies pour la ville connectée tout à la fois présentent des risques et offrent de nouvelles possibilités pour une sécurité plus étendue dans le respect

des libertés. La sécurité urbaine est plus que jamais un thème d'avenir et un domaine où l'investissement va apporter des résultats très concrets pour les citoyens.

- Grands événements : la France n'a plus à démontrer sa capacité d'organisation de grands événements. L'ambition affichée de l'Etat et des territoires à les accueillir régulièrement oblige à une adaptation radicale des capacités de coopération et de coordination entre tous les acteurs d'un territoire. 100 ans après les jeux de Paris, dans un monde durablement instable, le point d'orgue des Jeux Olympiques de 2024 pourrait donner l'occasion à la France d'organiser les jeux les plus sûrs de l'histoire.

A cette fin, le CICS recommande :

- **de déployer des documents d'identité, CNI et permis de conduire, de nouvelle génération, électroniques et sécurisés dès 2018 ;**
- **de mettre en œuvre un système d'identification électronique et une politique « public-privé » de déploiement des usages de ce système, qui fassent de la France le pays leader au sein de l'UE et permettent la construction d'un internet de confiance ;**
- **de développer une politique d'incitation pour la mise en place de solutions évoluées de sécurité urbaine et de gestion de crise dans la ville connectée ;**
- **de renforcer, lors de grands événements, la capacité de coopération et d'interopérabilité technique des acteurs à tous les échelons, avec en perspective les jeux olympiques de 2024.**

4. Dans le contexte post-Brexit, relancer des initiatives européennes ambitieuses en matière de sécurité et de souveraineté

A l'image de la directive récente sur la protection des données personnelles, les nouveaux enjeux de la sécurité revêtent une dimension politique et économique qui appelle un dépassement du niveau national et un traitement au niveau européen. Par ailleurs, le nouveau contexte post Brexit permet de relancer des initiatives fortes en matière de sécurité et de souveraineté. Ce constat doit avoir deux conséquences :

- Alors que la présence française à Bruxelles est encore trop timide, il faut proposer des initiatives fortes et développer par une action coordonnée des services de l'Etat et des acteurs industriels, en lien avec d'autres Etats-membres aux positions proches des nôtres, une capacité à influencer le processus décisionnel européen.
- Il faut peser sur Bruxelles pour qu'en plus de l'élaboration nécessaire d'un cadre réglementaire, l'Europe se dote, pour la protection de ses citoyens et le développement de son industrie, de politiques d'équipement ambitieuses susceptibles de servir de catalyseur à l'émergence de nouvelles technologies souveraines. Il s'agit de développer les solutions et les capacités industrielles et opérationnelles dont nous avons besoin à l'échelle européenne (traitement des flux aux frontières, souveraineté numérique, …). Pour assurer la sécurité numérique européenne, les impératifs communs de confiance doivent être élevés par l'instauration de labels européens et d'obligations réglementaires.

A cette fin, le CICS recommande :

- **que l'Etat joue un rôle de leader pour développer une politique européenne de souveraineté en matière de sécurité et les conditions d'une base industrielle de sécurité européenne forte et indépendante ;**
- **de lancer des grands programmes capacitaires européens en matière de sécurité, notamment pour la cybersécurité et la gestion des frontières.**

5. Développer notre ambition sur les ruptures majeures – La France championne de l'Internet de confiance

Comme l'ensemble de l'économie, la sécurité est actuellement transformée par des ruptures en matière d'usages, de technologies, d'organisation ou de nouveaux impératifs : Internet des objets, véhicules connectés, villes intelligentes et sûres, Blockchain, robotique, … Ces changements profonds auxquels nous n'échapperons pas sont porteurs de risques et d'opportunités majeures. Nos concurrents l'ont bien compris et mettent en place des dispositifs très puissants pour nous prendre de vitesse et s'assurer de positions dominantes. Nous devons donc intensifier nos efforts à l'échelle nationale et européenne, pour nous organiser autour d'ambitions clés, telles que prendre une position de leader en protection des données professionnelles comme personnelles ou développer des capacités souveraines en matière d'intelligence de la donnée (Big data, deep learning, alerte prédictive).

Il faut oser le droit en permettant aux faits de le précéder et permettre à la France de proposer des solutions de sécurité innovantes dans un temps beaucoup plus court ainsi que des réponses plus rapides à l'émergence de nouvelles menaces. Il faut assouplir les cadres juridiques et réglementaires pour permettre le développement et l'expérimentation de solutions innovantes, aujourd'hui trop contraintes par des précautions de principe excessives, la crainte des textes juridiques ou d'une censure d'autorités administratives (CNIL, CNCTR, ANTS, DGAC…). Le CICS est ainsi en mesure de proposer des expérimentations de confiance.

A cette fin, le CICS recommande :

- **de mettre en place un cadre réglementaire et une politique d'innovation qui autorisent et encouragent l'usage des nouvelles technologies, notamment de la biométrie, pour les applications de sécurité publique (par exemple l'analyse vidéo dans les lieux publics) au moins au même niveau que dans les autres pays européens ;**
- **conduire des expérimentations innovantes de confiance avec des données réelles (plateformes / openlabs) dans lesquelles des dispositifs techniques et procéduraux peuvent garantir une bonne sécurité des données personnelles sans préjudice de leur déploiement opérationnel pouvant nécessiter une évolution des textes juridiques.**

6. Elever l'efficacité de la sécurité et la résilience du pays par une gouvernance claire et unifiée

Il n'appartient pas à l'industrie de prescrire l'organisation de l'Etat, elle ne s'interdit cependant pas de livrer son opinion sur ce point important. Le dialogue inauguré depuis 2013 au sein du COFIS (comité de la filière des industries de sécurité), présidé par le Premier ministre, entre les pouvoirs publics, les industriels et leurs partenaires du domaine de la recherche constitue une avancée importante pour défragmenter le domaine de la sécurité. La pratique de trois années de ce partenariat montre qu'il manque incontestablement au dispositif étatique de gouvernance de ce domaine, encore marqué par de fortes frontières ministérielles, une instance permettant de s'exprimer avec une autorité débouchant sur la mise en œuvre d'actions transverses (impulsion à donner à la politique publique de sécurité, budgets de recherche, programmes d'équipement).

A cette fin, le CICS recommande :

- **créer des commissions spécialisées sur la sécurité à l'Assemblée nationale et au Sénat ;**
- **de mettre en place une gouvernance transverse plus structurée entre les ministères chargés de la justice, de l'intérieur, des douanes, des transports, de l'environnement et de la recherche, en rassemblant les objectifs et indicateurs d'une véritable politique de sécurité combinant l'action publique et privée y compris dans la gouvernance de la R&D, de l'investissement et de la mise en œuvre des solutions ;**
- **de créer une agence nationale en charge des programmes de sécurité.**

Annexes

FIEEC - QUI SOMMES-NOUS ?

Marchés clés

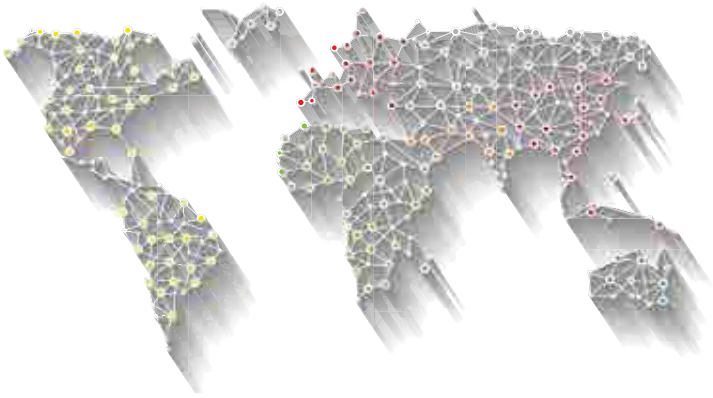
- Efficacité énergétique
- Industrie du futur
- Bâtiments
- Sécurité
- Objets connectés
- Automobile
- Ferroviaire
- Aéronautique

Chiffres clés

Source : Insee 2013

Les électrotechnologies exportent vers :

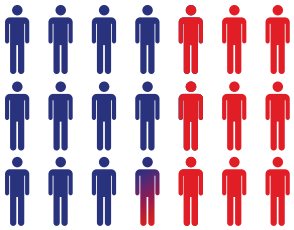
15% Amérique
9% Afrique
56% Europe
5% Proche & Moyen-Orient
14% Asie
1% Australie



Une industrie tournée vers l'innovation et la R&D

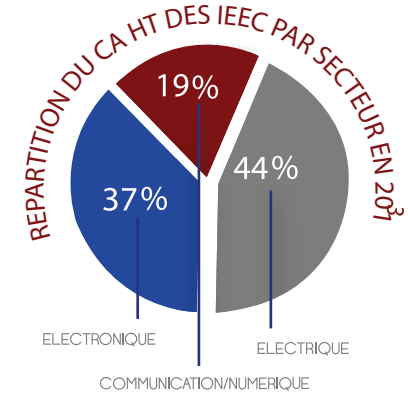
120 000 chercheurs en R&D dont

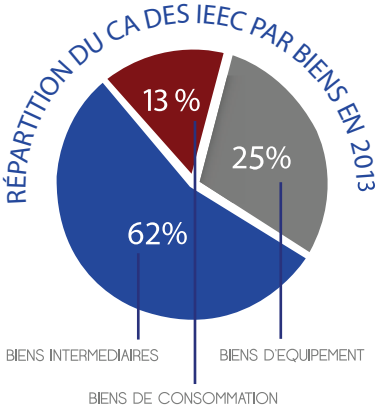
56% FIEEC — **44% Autres industries**

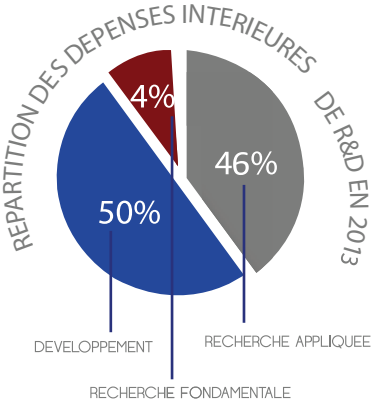


47 %

C'est la part des dépenses intérieures en R&D (Production et Services) des IEEC dans les dépenses en R&D de l'industrie en 2013







Représentation

100 milliards € de CA

3 000 entreprises

400 000 salariés

42% d'exportation sur le CA industriel

R&D

9% du CA du secteur consacré à la R&D

Les syndicats et membres associés de la FIEEC

Syndicats membres

Membres associés

Remerciements

Ce dossier a été rédigé par Anaïs Régnier (Chargée de mission affaires publiques) sous la direction de Yoann Kassianides (Directeur délégué, Communication et innovation).

Nous adressons nos plus vifs remerciements à l'ensemble des Délégués Généraux, des membres du Conseil d'Administration et des syndicats membres de la FIEEC pour leur collaboration et leur implication, sans qui la réalisation de ce dossier n'aurait pu être possible. Nous remercions également les experts en sécurité numérique des entreprises de nos professions qui ont donné de leur temps pour faire part de leurs expériences et de leurs connaissances :

ADAM Guillaume - FIEEC - Chef de Service Affaires européennes et numériques

ANTOINE Patrick - SYNDICAT DE LA MESURE - Président

ARPAGIAN Nicolas - ACN - ORANGE CYBERDEFENSE - Directeur de la stratégie et des affaires publiques

ARVIDSSON Viktor - AFNUM - ERICSSON France

AUDRY Laurent - AFNUM - FUJIFILM - Directeur des divisions Pro/Minilab//Afrique & Laboratory

BAL Jean-Louis - SER - Président

BALLOTEAU Pierre - ACN - AIRBUS - Responsable Commercial Grands Comptes

BARBAT-LAYANI Marie-Anne - FBF - Directrice Générale

BARRE Gilles - Président de l'AIGCEV

BAUDON Frédéric - AFNUM - OLYMPUS France - Responsable Juridique

BERANGER Vincent - SYNDICAT DE LA MESURE - Délégué Général

BERNARD Franck - AFNUM - FUJIFILM - Directeur Division Grand Public

BERTRAND Patrick - VP Numérique FIEEC

BEURDELEY Camille - GIFAM - Délégué Générale

BOISTARD Isabelle - ACN - Directrice Déléguée

BONICEL Jean-Pierre - SYCABEL - PRYSMIAN Group - Directeur

BONNINGUE Gérard - ACN - IMPRIMERIE NATIONALE

BOUVEROT Anne - VP Confiance et sécurité numérique FIEEC

BRETON Sophie - VP Bâtiment FIEEC - Présidente IGNES - HAGER France - Directeur Général

BRIARD Antonin - GIMELEC - Délégué Bâtiment - Automatismes et systèmes d'information

BRUN Jean-Michel - GIMELEC - SCHNEIDER ELECTRIC - Technology strategy - Product Security Office - Lead Global Cyber Security Architect

BRUNET Arnaud - AFNUM - SONY - Directeur des Relations Extérieures et des Affaires Juridiques

BRUNET Lionel - SYNDICAT DE L'ECLAIRAGE - Délégué Général

BURNOTTE Eric - Président SNESE - ALLIANSYS - Directeur Général

CALVEZ Christophe - ACN - AIRBUS - Head of Product Security Office

CANALS Agusti - ACN - CS (Communication & Systèmes) - Directeur d'Unité Fonctionnelle

CARON Alexandre - ACN - APICEM - Chef de projet/RSSI

CAURETTE Alexis - ACN - ATOS - Directeur Cyber

CHARRIERE Marc - Président de la Commission Numérique FIEEC- NOKIA - Directeur des Relations Institutionnelles

CHARVIN Yves - ACN - SAFRAN - Directeur Juridique

CHERY Richard - Président FGME - SONEPAR - Conseiller Exécutif

CLEMOT Olivier - VP ACN - OT MORPHO - Directeur Centre d'Ingénierie pour le Numérique

CLERMONT Matthieu - ACN - GEMALTO - Security Marketing Manager for Automotive & New Mobility Services

COUSIN Pascale - SNITEM - Directrice des Affaires Techniques

COUSIN Régis - FFMI - Président

CRETIER Richard - SNESE - Délégué Général

CROUE Jean-Marie - Syndicat du luminaire/GIL - Président

DARMON Marc - Président du CICS - THALES - DGA de l'Activité Systèmes d'Information et de Communication Sécurisés

DE BRAY Laurent - Président du Syndicat de l'éclairage - PHILIPS France - Directeur Général

DE FLEURIEU Antoine - GIMELEC - Délégué Général

DE GALZAIN Jean-Noël - HEXATRUST - Président - WALLIX - PDG

DE NONANCOURT Michel - SNESE - ALLIANSYS - Président

DEHAIS Eric - ACN - OPPIDA - Directeur Général

DESHAYES Kristel - FIEEC - Responsable Communication

DENIZOT Laurent - ACN - EGIDIUM TECHNOLOGIES - Président Directeur Général

DEPIERRE Franck - ACN - STORMSHIELD

DEPINAY Jean-Loup - ACN - OT MORPHO - Program Manager R&D funding

DIAKITE Ladji - SYCABEL - Responsable Règlementation Technique, Normalisation

DIARD Bertrand - Président TECH'IN France - INFLUANS - COO

DOUDOU Sabbah - IGNES - Directeur des Affaires Publiques

DU BOULLAY Charles - ACN - CDC ARKHINÉO - Président DUBAS Alain - AFNUM - CICSO - Directeur commercial sécurité

DUQUESNE Jean-Marc - GICAT - Délégué Général

ELKON Stéphane - AFNUM - Délégué Général

FALQUE-PIERROTIN Isabelle - CNIL - Présidente

FERNANDEZ Pascal - Président SPDEI - AVNET - Vice-Président

FLOREN Patrick - Président SYNAFEL - SEMIOS - PDG

FRANÇOIS Pierre-Louis - UNICLIMA - GROUPE ATLANTIC - Président

FRISQUET François - Président UNICLIMA - FRISQUET SA - PDG

GARZA Alice - TECH IN FRANCE - Chargée de mission Affaires Publiques

GASQUY Mathieu - AFNUM - WESTERN DIGITAL - Senior Director

GENDREAU Philippe - GICAT - Délégué Général Adjoint Sécurité

GERAUD DE LESCAZES Frédéric - Afnum - CISCO - Secretary General, Director Government Affaires & Community Relations

GERVAIS Stéphane - SNESE - LACROIX Group - Directeur Innovation Stratégique

GILBERT Eric - ACN- CS (Communication & Systèmes) - Responsable offres Sécurité et Sureté des Systèmes

GODEREAUX Pascal - AFNUM - KODAK Cluster Service - Director

GOURLET Christel - FBF - Advisor, Direction systèmes et moyens de paiement

GOUYET Hervé - ELECTRICIENS SANS FRONTIERES - Président

GRAVIER Emmanuel - FFIE - Président

GRONIER Antoine - HEXATRUST - Chargé de mission

GUEDON Jean-Yves - ACN - OT MORPHO - Directeur du développement

HAGER Daniel - IGNES - HAGER - Président du directoire

HELUIN Sarah - AFNUM - Ericsson France - Business Development Manager

HERITIER Coralie - HEXATRUST - IDNOMIC - PDG

HEYDEMANN Christel - VP Branche électrique - SCHNEIDER ELECTRIC France - Président

HUCK Didier - SIEPS - TECHNICOLOR - VP Public Affairs and Corporate Social Responsibility

HOOGSTOEL Thierry - SPDEI - AVNET - Directeur

JACOUTON Laure -SPAP - Présidente - PANASONIC - Key Account Category Manager

JARRY Nathalie - SNITEM - Responsable Communication Institutionnelle et Relations Presse

JOURDE Eric - FIEEC - Délégué Général

KARAM Georges - AFNUM - Président - SEQUANS COMMUNICATIONS - Président

KASSIANIDES Yoann - FIEEC- Directeur Délégué, Communication/Innovation - ACN - Délégué Général

KIRCHNER Florent - CEA - Chef du Laboratoire de Sûreté et Sécurité des Logiciels - ACSIEL

LACROIX Guy - SERCE - Président

LAHBABI Pierre - ACN - SAFRAN MORPHO - Directeur de la Stratégie

LAMOUCHE Didier - ACN - OT MORPHO - Président du directoire

LANEN Olivier - IGNES - Responsable Métier Sécurité électronique, Normalisation produits

LANG Jonathan - AFNUM - OLYMPUS - Attaché du Président

LANGHEIM Jochen - ACSIEL - STMICROELECTRONICS - Vice President, Advanced Systems R&D Programs Automotive Business Unit, EMEA Region

LANOË Ingrid - TECH IN FRANCE - Affaires Publiques

LAVASTE François - ACN - AIRBUS - Head of Digital Security

LAVIGNE Benoît - IGNES - Délégué Général

LE FLOCH Yves - ACN - SOGETI- Directeur du développement

LE ROUX Pascal - Président du Comité de liaison Sécurité Numérique FIEEC - CDVI - Directeur Général - IGNES

LE ROY Eric - SNITEM - Directeur Général

LE STRAT Marie-Pierre - Syndicat du luminaire - VP - RYCKAERT – Dirigeante

LEGRAIN Marie - AFNUM - NIKKEN France - Gérante

LEVET Jacques - FIEEC - Directeur Affaires Techniques

LOHNHERR Alexander - GIFAM - Président - MIELE SAS - Directeur Général

LUCAS Jacques - CNOM - VP et Délégué Général au Numérique

MACAIRE Julie - FIEEC - Chef de Service Affaires Juridiques

MAHALAL Ilan- ACN - GEMALTO - Project Manager

MASSICOT Jean-Pierre - ACN - ADVANCED TRACK & TRACE - CEO

MATHERON Gérard - VP Branche électronique FIEEC - ACSIEL - Président - STMICROELECTRONICS Crolles - VP R&D et Affaires Publiques

MAUPAS Hanene - ACN - SAFRAN STARCHIP - VP Sales & Marketing

MAURO Roberto - AFNUM - SAMSUNG - Directeur Stratégie et Développement

MAYER Stéphane - GICAT - Président

MERLE Alain - CEA LETI - Docteur - ACSIEL

MITTELBACH Klaus - ZVEI - CEO

MONATE Benjamin - TECH IN FRANCE - TRUST IN SOFT - Founder & CTO

MONGIN Roland - FGME - Délégué Général

MONIER Florence - FIEEC - Directrice Energie & Environnement

MOUILLE Stéfane - ACN - GEMALTO - Directeur Stratégie des applications mobiles et expert identité numérique

MURCIA Corinne - ACN - SURYS - Directeur Affaires Stratégiques et Relations Institutionnelles

NAPAR Jean-Daniel - ACR - Président - SIEMENS - Chief Technology Officer

NEGRE LOUIS - FIF - Président

NERBONNE Sophie - CNIL - Directrice de la conformité

OLLE Florence - SNITEM - Responsable Affaires Réglementaires

OUIN Jean-Paul - UNICLIMA - Délégué Général

PARRA Camille - TECH IN FRANCE - Responsable

des Affaires Publiques et Réglementaires

PAUMIER Régis - SYCABEL - Délégué Général

PERKER KRAKOVICH Maud - AFNUM - FUJIFILM - Juriste

PERROCHON Pascal - FIEEC - Directeur Affaires Internationales

PETAT Valérie - GIMELEC - Attachée de Direction Relations Institutionnelles

PHILBER-GRONDEL Pascale - AFNUM- KODAK - Directrice Division Photo

PIC Marc – ACN - SURYS Group - CTO (dpty) Digital Activities

PILLOT Jean-Marie - ACN - CS (Communication & Systèmes) - VP Business Development

PIN Claude - ACSIEL - INTEL - EMEA Global Public Policy Manager

POUPARD Guillaume - ANSSI - Délégué Général

PRANGE Mathieu - SYCABEL - SILEC CABLE - Chef de produits Câbles a fibres optiques

PRAT Laurent - SYNDICAT DE L'ECLAIRAGE - SECURLITE - Président

PROVE Baudouin - AFNUM - SIGMA PHOTO - Directeur Général

PROVE Foucault - AFNUM - SIGMA PHOTO - Responsable Grand Comptes

PRUNET Jean-Christophe - ACSIEL - ROHDE & SCHWARZ - Président

PUZO Joseph - VP Innovation FIEEC - ACSIEL - AXON' CABLE - PDG

QUEMARD Jean-Pierre - ACN - Président

RADISSON Sarah - AFNUM - MANFROTTO - Managing Director

RADVANYI Charlotte - AFNUM - SAMSUNG - Public Affairs Manager

RAGUENES Jérôme - FBF - Directeur de département numérique, systèmes et moyens de paiement

RAGUIN Paul - SNESE - EOLANE - Président du Directoire

RAIMBAULT Sylvie - SYNAFEL - Déléguée Générale

RAMEZ Michel - ACSIEL - HYPERTAC SA - SMITHS CONNECTORS - Vice-président Marché Rail

RASCLARD Hervé - FIRIP - Délégué Général

REGNAULT Stéphane - SNITEM - Président - VYGON - Président du Directoire

REGNIER Anaïs - FIEEC - Chargée de mission affaires publiques

REGNIER DUFOUR Christine - AFNUM - MICRON - Regional Sales Manager

REMONT Luc - GIMELEC - Président - SCHNEIDER ELECTRIC - Directeur Général des Opérations internationales

RENOUIL Luc - HEXATRUST - BERTIN - Directeur du développement et de la communication

RIFAUX Philippe - FFIE - Délégué Général

RIVIERE Loïc - TECH IN FRANCE - Délégué Général

RIZZO Gilles - ACSIEL - Délégué Général

ROBIN Julie - AFNUM - SONY - Affaires Publiques

ROCHE Elisabeth - AFNUM - LUMIERE IMAGING - Responsable Finances Administration

ROESCH Alexandre - SER - Délégué Général

ROLLAND William - SNITEM - Responsable sectoriel et e-santé

ROUJANSKI Jacques - Dékégué Général - CICS

ROUQUET Thierry - TECH IN FRANCE - SENTRYO - Président Directeur Général

ROUVIERE Gilles - FIEEC - Directeur Délégué, Adjoint au Délégué Général - SPDEI - Délégué Général

ROUYER André - GIMELEC - Chef de Projet

SAGAN Zbigniew - ACN - ADVANCED TRACK & TRACE – Chief technology officer

SALOMMEZ Gérard - VP Branche biens de consommations durables FIEEC - GIFAM - GROUPE SEB France - Vice-Président

SCHNEPP Gilles - FIEEC - Président - LEGRAND - Président Directeur Général

SEBAG Jacques - HEXATRUST - DENYALL SAS - CEO

SIAT Jérôme - SIRMELEC - Président - ALPHITAN - Directeur Général

SOUPARIS Hugues - ACN - SURYS - Président

STANTCHEV Pentcho - GIMELEC - SCHNEIDER ELECTRIC - Business Development - Strategy & Business Development France Operations

TAILHADES Philippe - GIMELEC -Directeur Marketing Technique

TARDIF Laurent - VP Finances FIEEC - SYCABEL - Président - PRYSMIAN GROUP - Président de la Région Europe Sud

THIERCELIN Eric - ACSIEL - Chargé de Mission

TROCHU Florent - ACR - Délégué Général

TUAL Jean-Pierre - ACN - GEMALTO - Director, industrial relations

VALACHS Anne - SERCE - Directeur Général

VALLEE Philippe - ACN - GEMALTO - Directeur Général

VALLET Olivier - ACN - DOCAPOST - Président Directeur Général

VANNIER Philippe - ACN - BULL - CEO - ATOS - Group Advisor for Technology

VIALLIX Alain - ACN - NOKIA - Directeur Affaires Publiques

VILLIE Bertrand - AFNUM - SONY Mobile Communications - Directeur Services Clients

VROMMAN Laurent - ACN - AIRBUS - Chief of Staff

WEDRYCHOWSKA Anne-Charlotte - FIEEC - Chef de service développement durable - SPAP - Déléguée Générale

WUIDART Sylvie - ACN - STMICROELECTRONICS - Director, Security Expert - Lobbying & Standardization - Strategic Planning ,Microcontrollers and Digital ICs Group

ZERO Sandro - SIEPS - Président - Studio Zero Export Control - Président

FIEEC

FEDERATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

FIEEC - Fédération des Industries Electriques, Electroniques et de Communication

www.fieec.fr

@FIEEC FIEEC

La FIEEC soutient les travaux du CICS Conseil des Industries de la Confiance et de la Sécurité et du Cofis

Juillet 2017