FIC 2021

Forum International de la Cybersécurité

PROGRAMME

TABLES RONDES & SÉANCES PLÉNIÈRES
ROUND TABLES & PLENARY SESSIONS

7, 8 & 9 SEPTEMBRE 2021 | LILLE GRAND PALAIS

FORUM-FIC.COM

PLENARY SESSIONS

WEDNESDAY, SEPTEMBER 8TH

9am – 11:30am

P01 La prochaine pandémie sera-t-elle numérique ?
Will The Next Pandemic Be Digital?

La crise Covid a entraîné une accélération de la transformation numérique mais montre aussi notre dépendance croissante au numérique et le rôle systémique de celui-ci dans nos sociétés. Avec toutes les opportunités que cela génère mais aussi tous les risques associés. En a-t-on seulement pris conscience ? Pas sûr quand on voit certaines entreprises réduire leur budget cybersécurité… Comment gérer cet autre risque systémique ? Quels enseignements tirer de la crise Covid ? Faut-il préparer le pire pour espérer le meilleur ? « Le problème avec les experts, c'est qu'ils n'ont aucune idée de ce qu'ils ignorent. » Nassim Nicholas Taleb

The Covid crisis has led to an acceleration of the digital transformation but also shows our growing dependence on digital and its systemic role in our societies. With all the opportunities it generates but also all the associated risks. Have we even become aware of this? Not sure when we see some companies cutting their cyber security budgets… How can we manage this other systemic risk? What lessons can we learn from the Covid crisis? Is it necessary to prepare for the worst in order to hope for the best? "The problem with experts is that they do not know what they do not know." Nassim Nicholas Taleb

5:30pm – 7:30pm

P02 Nouvelle guerre froide dans le Cyberespace
A New Cold War In Cyberspace

Espionnage, guerre informationnelle, déstabilisations : le cyberespace est devenu le terrain d'affrontement favori des grandes puissances. Une guerre froide et un duopole sino-américain sont-ils inéluctables ? L'espace numérique va-t-il devenir l'otage de la confrontation entre les deux pays ? Alors qu'un monde multipolaire est en train d'émerger, l'Europe peut-elle constituer une 3ème voie entre les États-Unis et la Chine ? Dans un monde sans leadership incontesté, sans règles communes, avec de grands ensembles régionaux, comment relancer le multilatéral ? Faut-il craindre une fragmentation du cyberespace ? « Sans un système multilatéral fort, seuls les rapports de force comptent. » Jean-Pierre Raffarin

Espionage, information warfare, destabilization: cyberspace has become the favourite battleground of the great powers. Are a Cold War and a Sino-American duopoly inevitable? Will digital space become hostage to the confrontation between the two countries? At a time when a multipolar world is emerging, can Europe be a third way between the United States and China? In a world without undisputed leadership, without common rules, with large regional groupings, how can we relaunch multilateralism? Should we fear a fragmentation of cyberspace? "Without a strong multilateral system, only the balance of power counts," Jean-Pierre Raffarin said.

PLENARY SESSIONS

THURSDAY, SEPTEMBER 9TH

9am – 11am

P03 Les écosystèmes, clés de la résilience "cyber"
Ecosystems, The Key To "Cyber Resilience"

En matière de cybersécurité, la réponse est nécessairement collective. Pourtant la confiance entre États, entre États et entreprises, entre entreprises, entre centres de recherche et entreprises, entre éditeurs etc. ne se décrète pas, elle se construit grâce à des échanges, des coopérations, des normes communes etc. Alors que le multilatéralisme est en crise, comment renforcer la coopération au plan international ? En matière industrielle, comment structurer des écosystèmes de cybersécurité dynamiques ? Au sein des organisations, comment aligner l'ensemble des acteurs ? « Si tu veux aller vite, marche seul mais si tu veux aller loin, marchons ensemble » (Proverbe africain)

When it comes to cybersecurity, the response is necessarily collective. However, trust between States, between States and companies, between companies, between research centers and companies, between publishers, etc. cannot be decreed; it is built through exchanges, cooperation, common standards, etc. At a time when multilateralism is in crisis, how can we strengthen cooperation at the international level? In terms of industry, how can dynamic cybersecurity ecosystems be structured? Within organizations, how can all the players be aligned? "If you want to go fast, go alone. If you want to go far, go together" (African proverb)

3:30pm – 5:30pm

P04 Cloud européen : le rêve peut-il devenir réalité ?
European Cloud: Can The Dream Come True?

La maîtrise des infrastructures IT est perçue comme LE critère absolu de souveraineté en matière numérique. Mais celle-ci passe-t-elle forcément par la maîtrise du Cloud et des réseaux ? Peut-on maîtriser les données et leurs traitements sans maîtriser les infrastructures ? Peut-on retrouver notre souveraineté informationnelle sans maîtrise des couches "basses" ? L'Europe a enfin pris conscience de son retard numérique et semble s'être donné les moyens de ses ambitions, mais le volontarisme politique et normatif dont elle fait preuve sera-t-il suffisant ? Quelles sont les autres voies possibles ? Quels sont les leviers à mobiliser pour retrouver la maîtrise de notre destin numérique ? « Il faut allier le pessimisme de l'intelligence à l'optimisme de la volonté. » (Antonio Gramsci)

Mastery of IT infrastructures is seen as THE absolute criterion of sovereignty in digital matters. But does this necessarily involve mastering the Cloud and networks? Is it possible to control data and data processing without controlling infrastructures? Can we regain our information sovereignty without mastering the "lower" layers? Europe has finally become aware of its digital backwardness and seems to be given the means to achieve its ambitions, but will the political and normative voluntarism it has demonstrated be enough? What are the other possible ways forward? What are the levers to be mobilized to regain control of our digital destiny? "It is necessary to combine the pessimism of the Intellect with the optimism of the Will." (Antonio Gramsci)

WEDNESDAY, SEPTEMBER 8TH
12pm – 1pm

SÉCURITÉ ET STABILITÉ DANS LE CYBERESPACE
SECURITY AND STABILITY IN CYBERSPACE

TR

Chine : l'offensive tout azimut
China: an all-out offensive?

Désireuse de rétablir sa crédibilité et sa légitimité et de s'affirmer sur la scène internationale, la Chine s'est lancée depuis quelques années dans une offensive tous azimuts à laquelle la crise sanitaire et économique a donné un nouvel élan. Une offensive à la fois commerciale (législation sur le contrôle des exportations technologiques), diplomatique (soutien à la création à l'ONU de l'OEWG) politique (campagnes d'influence en ligne), technologique (déploiement de la 5G) ou encore normative (initiative « NewIP »), dans laquelle le numérique tient une place centrale. Mais quelles en sont plus précisément les ramifications et les objectifs ? Les craintes et accusations de ses adversaires et concurrents (espionnage, vol de données, désinformation…) sont-justifiées ? Peuvent-ils réagir, et si oui comment ?

Wishing to re-establish its credibility and legitimacy and to assert itself on the international scene, China has for some years now been engaged in an all-out offensive to which the health and economic crisis has given new impetus. This offensive has been at once commercial (legislation on the control of technological exports), diplomatic (support for the establishment of the OEWG at the UN), political (online lobbying campaigns), technological (roll-out of 5G), and normative (the "New IP" initiative), in which digital technology plays a central role. But what are its ramifications and objectives? Are the fears and accusations of its opponents and competitors (espionage, data theft, disinformation…) justified? Can they react, and if so, how?

TR

Les indices de maturité pays sont-ils utiles ?
Are "Country Maturity Indices" useful?

Qu'ils soient l'œuvre d'organisation privées ou d'entités publiques, qu'ils mesurent la maturité, la stabilité, la sensibilité aux problématiques de cybersécurité ou encore l'exposition aux cyber-risques, les indices destinés à classer les États sur leurs capacités à appréhender et répondre aux cyber-menaces se multiplient. Sur quels critères reposent leurs diagnostics, et que mesurent-ils vraiment ? Sont-ils même fiables ? Et quid de leur utilisation, ont-ils une réelle utilité ? Peuvent-ils par exemple être utilisés par le secteur de l'assurance ou de la finance pour évaluer la solidité d'un État ou d'une entreprise ?

Whether they come from private organisations or public entities, measure maturity, stability, sensitivity to cybersecurity issues, or assess exposure to cyber-risks, indices designed to rank states on their capacity to apprehend and respond to cyber threats are multiplying. On what criteria do they base their diagnoses, and what do they really measure? Are they even reliable? And are they really useful? For example, can they be used by the insurance or financial sector to assess the robustness of a state or a company?

WEDNESDAY, SEPTEMBER 8TH
12pm – 1pm

SÉCURITÉ OPÉRATIONNELLE
OPERATIONAL SECURITY

TR

Workplaces et outils collaboratifs : comment sécuriser ces “fenêtres sur l’entreprise” ?
Workplaces and collaborative tools: how can we secure such "access doors to the company"?

La généralisation du télétravail a consacré la tendance montante au développement d’espaces collaboratifs permettant de faciliter l’interaction, parfois en temps réel, entre les parties prenantes d’un projet, tant en interne qu’avec des clients, fournisseurs ou prestataires : plateformes d’échange et de partage de documents, suites logicielles en ligne, solutions de visioconférences, salles de travail virtuelles… Mais ce fonctionnement qui repose sur le partage de données hors du strict périmètre de l’entreprise, et avec des partenaires dont le respect des standards de sécurité n’est pas garanti, n’est pas sans risque en termes de fuite ou de vol de données. Comment combiner productivité, sécurité et fluidité de l’expérience utilisateur ? Comment gérer l’augmentation de la surface de vulnérabilité et la dispersion de données que génèrent ces outils ? Comment s’assurer du respect de la politique de sécurité de l’organisation ?

The widespread use of teleworking has led to a growing demand for collaborative spaces that facilitate interaction — sometimes in real time — between the various stakeholders in a project, be they colleagues or customers, suppliers, or service providers. Such spaces include document exchange and sharing platforms, online software suites, videoconferencing solutions, and virtual work rooms. However, this approach is not risk-free when it comes to data leakage or theft, as it involves the sharing of data outside the limited scope of the company and with partners whose compliance with security standards cannot be guaranteed. How can we combine productivity, security, and fluidity in the user experience? How can we cope with the increased vulnerability surface and the scattering of data induced by such tools? How can we ensure compliance with the organisation's security policy?

WEDNESDAY, SEPTEMBER 8TH
11:45am – 1:15pm

SÉCURITÉ OPÉRATIONNELLE
OPERATIONAL SECURITY

TR

EDR, SIEM/UEBA et NDR : le tiercé gagnant du SOC
EDR, SIEM/UEBA and NDR: the "Top 3" of SOCs

Les SOC commencent généralement par déployer un SIEM, puis un Endpoint Detection Response (EDR). Mais avec le développement du Cloud, du Bring Your Own Device (BYOD), de l'Internet des objets (IoT) et, de façon plus globale, de l'émergence de l'entreprise étendue, la surveillance du poste de travail et du périmètre ne suffisent plus. Selon le SANS Institute, l'EDR ne détecterait ainsi que 25% des tentatives d'attaque. Le SOC a donc besoin d'une meilleure visibilité en ajoutant à sa boîte à outils une solution NDR (Network Detection and Response). Comment mettre en oeuvre cette nouvelle "triade de visibilité" (Gartner) et optimiser à la fois les règles de sécurité et la prise en compte de l'environnement métier ? Quelles sont les solutions existantes ?

SOCs typically start by deploying a SIEM, and then an Endpoint Detection Response (EDR). But with the development of the Cloud, the 'Bring Your Own Device' (BYOD) approach, the Internet of Things (IoT) and, more generally, the emergence of the extended enterprise, workstation and perimeter monitoring are no longer sufficient. According to the SANS Institute, EDR would only detect 25% of attempted attacks. The SOC therefore needs better visibility by adding an NDR (Network Detection and Response) solution to its toolbox. How should this new "visibility triad" (Gartner) be implemented to both optimise security rules and take into account the business environment? What are the existing solutions?

WEDNESDAY, SEPTEMBER 8TH
12pm – 1pm

MANAGEMENT DES CYBER RISQUES
CYBER RISK MANAGEMENT

TR Le défi du multicloud
The multicloud challenge

Plus de 80% des organisations utilisent aujourd'hui plus d'un fournisseur de Cloud (Gartner). Les stratégies multicloud, si elles permettent de ne pas dépendre d'un fournisseur unique et d'améliorer la résilience des organisations, génèrent aussi de la complexité et de vrais angles morts en matière de sécurité. Comment décentraliser données et applications tout en maintenant une cohérence d'ensemble et une gouvernance centralisée en matière de sécurité ? Parmi les défis : la sécurité des conteneurs et des applications, la gestion des idées et des accès, la gestion des clés de chiffrement (HYOK ou BYOK), la segmentation des réseaux, la gestion des vulnérabilités, la gestion des incidents, la conformité aux politiques de sécurité internes et leur suivi… Quelles sont les bonnes pratiques ? Quels sont les outils et technologies utiles ?

More than 80% of organisations now use more than one Cloud provider (Gartner). Indeed, multicloud strategies can help to move away from single-vendor dependency and improve organisational resilience. But they also create complexity and real security blind spots. How can data and applications be decentralised while maintaining overall consistency and centralised security governance? Challenges include: container and application security, idea and access management, encryption key management (HYOK or BYOK), network segmentation, vulnerability management, incident management, compliance with and monitoring of internal security policies, etc. What are the best practices? What are the useful tools and technologies?

TR NIS : bilan et perspectives
NIS: assessment and perspectives

Adoptée en juillet 2016, la Directive NIS, qui a institué les Opérateurs de Services Essentiels (OSE), devrait être prochainement révisée par la Commission européenne. Si elle a permis aux États européens de gagner en maturité et a jeté les bases d'une coopération efficace via la création du Groupe de coopération NIS et du réseau des CSIRTs, elle doit aujourd'hui évoluer pour répondre aux enjeux de la transformation numérique et à l'évolution des menaces. Comment renforcer l'harmonisation entre les différents États européens ? Comment concilier la nature transverse du dispositif avec les réglementations sectorielles en préparation ? Au-delà des OSE, comment faire progresser la sécurité des écosystèmes, menacés par les attaques "par rebond" ? Comment améliorer la coopération transfrontalière ? Quelles sont notamment les prochaines étapes en matière de réponse à incident après la création récente du réseau CyCLONE (Cyber Crisis Liaison Organization Network) ?

Adopted in July 2016, the NIS Directive, which established Essential Service Operators (ESOs), is due to be revised by the European Commission shortly. While it has enabled European states to gain in maturity and has laid the foundations for effective cooperation through the creation of the NIS Cooperation Group and the CSIRTs network, it must now evolve to meet the challenges of digital transformation and threat evolution. How can we strengthen harmonisation between the different European states? How can we reconcile the cross-cutting nature of the system with the sectoral regulations in preparation? Beyond ESOs, how can we improve the security of ecosystems, which are threatened by rebound attacks? How can cross-border cooperation be improved? In particular, what are the next steps in terms of incident response after the recent launching of the Cyber Crisis Liaison Organization Network (CyCLONe)?

WEDNESDAY, SEPTEMBER 8TH
12pm – 1pm

LUTTE CONTRE LA CYBERCRIMINALITÉ
FIGHT AGAINST CYBERCRIME

TR

Ransomware : la pandémie guette-t-elle ?
Ransomware: is pandemic looming?

Le nombre d'attaques par ransomware a été multiplié par sept au premier semestre 2020. Dans un contexte marqué par l'explosion du télétravail et l'accélération de la transformation numérique, elles ciblent des organisations de toutes tailles et de tous secteurs, y compris des États. Au-delà de l'impact financier pour leurs cibles, certaines de ces attaques ont défrayé la chronique en paralysant des hôpitaux en pleine pandémie, au risque de faire des victimes humaines. Puisque les dispositifs techniques et les mesures organisationnelles prises par les organisations semblent insuffisantes pour endiguer le phénomène, certains États prennent des mesures controversées : les États-Unis ont ainsi annoncé des sanctions contre les organisations payant les rançons. Mais est-ce la bonne solution ? Quels moyens, techniques, humains, organisationnels, pour s'en prémunir ? Comment réagir lorsque l'on est victime ?

The number of ransomware attacks has increased sevenfold in the first half of 2020. In a context marked by the boom of teleworking and the acceleration of digital transformation, they target organisations of all sizes and all sectors, including states. Beyond the financial impact for their targets, some of these attacks have made headlines by paralysing hospitals in the midst of a pandemic, at the risk of human casualties. These increasingly numerous and sophisticated attacks resist traditional security approaches. Since the technical devices and organisational measures taken by organisations seem insufficient to stem the phenomenon, some states are taking controversial measures, such as the sanctions imposed in the United States on ransom-paying organisations. But is this the right solution? What are the technical, human, and organisational means available to guard against it? Is the fight against ransomware a lost battle?

WEDNESDAY, SEPTEMBER 8TH
12pm – 1pm

TRANSFORMATION DIGITALE
DATA SAFETY AND DIGITAL TRANSFORMATION

TR

Fin du Privacy Shield : quelles conséquences et quelles solutions ?
End of the Privacy Shield: what consequences and what solutions?

Dans un arrêt du 16 juillet 2020, la Cour de Justice de l'Union européenne a invalidé le Privacy Shield, dispositif largement utilisé tant par les entreprises américaines qu'européennes, pour transférer des données européennes aux États-Unis. La Cour a en effet estimé que les données européennes ne bénéficiaient pas aux États-Unis d'une protection équivalente. Quelles sont les conséquences opérationnelles pour les entreprises ? Les "clauses contractuelles type", également fragilisées par la décision de la CJUE, vont-elles permettre de maintenir ces transferts ? Quelles autres solutions ? Au plan stratégique, quel est impact sur les relations économiques transatlantique ? Cette nouvelle guerre économique sur la donnée va-t-elle contribuer à relocaliser les données en Europe et à accélérer le développement d'une industrie numérique européenne ?

In a ruling of 16 July 2020, the European Court of Justice has invalidated the Privacy Shield, a system widely used by both US and European companies to transfer European data to the US. The Court found that European data did not enjoy equivalent protection in the United States. What are the operational consequences for companies? Will the "standard contractual clauses", also weakened by the CJEU's decision, make it possible to maintain these transfers? What other solutions exist? At the strategic level, what is the impact on transatlantic economic relations? Will this new economic war on data contribute to the relocation of data in Europe and accelerate the development of a European digital industry?

WEDNESDAY, SEPTEMBER 8TH
4pm – 5pm

SÉCURITÉ ET STABILITÉ DANS LE CYBERESPACE
SECURITY AND STABILITY IN CYBERSPACE

TR

Gestion de crise cyber : quelle organisation au plan étatique et international ?
Cyber crisis management: how should we be organised at a national and international level?

La multiplication et la sophistication des cyber-attaques, y compris contre des structures étatiques, augmente le risque d'une crise d'ampleur susceptible de mettre à terre non seulement les organisations ciblées, mais plus largement des secteurs entiers, voire même les États eux-mêmes. Pour assurer la résilience de leurs sociétés, il revient donc aux États de mettre en place les outils et dispositifs garantissant, le cas échéant, une gestion de crise efficace permettant d'atténuer les dommages, de rendre la crise aussi courte que possible, et d'éviter qu'elle ne se répande et se diffuse. Comment construire les conditions de la résilience ? Quelle articulation entre les diverses agences gouvernementales concernées? Quelle contribution et quelle coopération avec le secteur privé ? Quel cadre règlementaire ? Face à une menace qui ne connaît pas de frontière, quelles peuvent être les modalités et dispositifs de coopération internationale ?

The multiplication and sophistication of cyberattacks – including against state structures – increases the risk of a crisis of such magnitude as to bring down not only the targeted organisations, but more broadly entire sectors and even states themselves. To ensure the resilience of their societies, states must therefore put in place, where appropriate, the tools and mechanisms required to effectively manage crises in order to mitigate damage, keep each crisis as short as possible, and prevent it from spreading. How can we build the conditions for resilience? How can the various government agencies concerned be linked? What contribution and cooperation can we have with the private sector? What regulatory framework should we have? Faced with a threat that knows no borders, what can be the modalities and arrangements for international cooperation?

WEDNESDAY, SEPTEMBER 8TH
3:45pm – 5:15pm

SÉCURITÉ ET STABILITÉ DANS LE CYBERESPACE
SECURITY AND STABILITY IN CYBERSPACE

TR

Vers un cyberespace multipolaire et fragmenté ?
Cyberspace: is the "multilateral approach" in danger?

Dans un monde de plus en plus digitalisé et dématérialisé, le cyberespace est devenu un théâtre de confrontation et d'affrontement entre des acteurs tant étatiques que privés. Ces luttes de pouvoir, de contrôle et d'influence de plus en plus dures font s'opposer des intérêts politiques, commerciaux, et stratégiques de plus en plus irréconciliables. À mesure que les antagonismes se creusent, le cyberespace se morcelle et se polarise. Longtemps maîtres du jeu, les États-Unis sont aujourd'hui défiés par la Chine sur toutes les composantes du cyberespace (infrastructures, technologies, couche informationnelle…). Dans le même temps, le secteur privé s'impose comme un acteur indispensable et incontournable de la régulation et de la sécurisation du cyberespace. Quelles conséquences de ces évolutions des rapports de forces sur la gouvernance de l'Internet ? Sur la stabilité du cyberespace ?

In an increasingly digitised and dematerialised world, cyberspace has become a theatre of battle and confrontation between both state and private stakeholders. These increasingly hard struggles for power, control, and influence lead to increasingly irreconcilable political, commercial, and strategic conflicts of interest. As the antagonisms deepen, cyberspace is becoming more fragmented and polarised. The United States – long-time masters of the game – is now being challenged by China on all the elements of cyberspace (infrastructure, technologies, information layer…). At the same time, the private sector is establishing itself as an indispensable and unavoidable player in the regulation and security of cyberspace. What are the consequences of these changes in the balance of power on Internet governance? On the stability of cyberspace?

WEDNESDAY, SEPTEMBER 8TH
4pm – 5pm

SÉCURITÉ OPÉRATIONNELLE
OPERATIONAL SECURITY

TR Cartographie du système d'information : pourquoi et comment ?
Information system mapping: why and how?

"La cartographie est un outil essentiel à la maîtrise du système d'information", souligne l'ANSSI qui a consacré au sujet l'un de ses guides pratiques. Mais cette tâche peut rapidement s'avérer lourde et complexe : multiplicité des objets et de leurs attributs, développement du "shadow IT", évolution permanente du système d'information etc. Comment mettre en place cette démarche de façon pérenne ? Quelles sont les étapes ? Quels sont les écueils à éviter ? Comment articuler les différentes vues nécessaires pour disposer d'une vision "métier", "applicative" et "infrastructures" ? Quelle granularité ? Comment assurer la mise à jour de la cartographie ? Quels outils utiliser ?

"Mapping is an essential tool for mastering information systems," emphasises ANSSI, which has devoted one of its practical guides to the subject. However, with the multiplicity of objects and their attributes, the development of "shadow IT", and the constant evolution of the information system, this task can quickly become cumbersome and complex. How can this approach be sustainably implemented? What are the stages? What pitfalls must we avoid? How can we articulate the different views required to have a "business", "application", and "infrastructure" vision? What granularity do we need? How can we keep the mapping up to date? What tools should we use?

TR *Indicators are not intelligence* : quels sont les apports de l'analyse contextuelle ?
Indicators are not intelligence: what are the contributions of contextual analysis?

Les IoC (ou indicateurs de compromission) ne sont souvent que des "observables" (hash, adresse mail, adresse IP, domaine internet, URL, clé de registre…) accompagnés de quelques métadonnées (ports, horodotage, protocoles…). Pour les rendre encore plus utiles et "actionnables" par la communauté, leur enrichissement avec des données techniques ou stratégiques est essentiel. C'est le rôle de l'analyse contextuelle et de la Threat Intelligence. Si rien ne remplace l'intuition de l'analyste, quels sont les méthodes et outils utilisables ? Quelles sont les bonnes pratiques en la matière ? Quels sont les "livrables" de cette contextualisation (flux d'IOC sectorisés alimentant le SOC, "course of action", playbook…) ?

IoCs (or Indicators of Compromise) are often only "observables" (hashes, email or IP address, internet domain, URL, registry key…) accompanied by some metadata (ports, time stamps, protocols…). To make them even more useful and "actionable" by the community, it is essential to enrich them with technical or strategic data. This is the role of contextual analysis and Threat Intelligence. Though nothing replaces the analyst's intuition, what methods and tools can be used? What are the best practices in this area? What are the "deliverables" of this contextualisation (sectorised IoC flows feeding the SOC, "course of action", playbook…)?

WEDNESDAY, SEPTEMBER 8TH
4pm – 5pm

SÉCURITÉ OPÉRATIONNELLE
OPERATIONAL SECURITY

TR *Cyber Threat Hunting* : quelles bonnes pratiques ?
Cyber Threat Hunting: what are the best practices?

Pour compléter les solutions et mesures de sécurité traditionnelles, le “cyber threat hunting” mise sur l’Humain pour s’attaquer aux menaces déjà présentes sur le réseau. Les attaquants peuvent en effet rester tapis plusieurs mois chez leurs cibles avant de passer à l’offensive en contournant les dispositifs en place. L’objectif est donc de les déstabiliser et de les débusquer en sortant des sentiers battus. Mais pour être efficace, une “chasse” doit être soigneusement organisée, de la préparation amont jusqu’aux actions correctives. Quelles en sont les principales étapes ? Quelles sont les compétences indispensables ? Quelles données fournir aux “hunters” ? Quels sont les outils utiles ? Comment mettre en place cette approche dans la durée ?

To complement traditional security solutions and measures, "cyber threat hunting" relies on human beings to tackle threats already present on the network. Indeed, attackers can remain hidden for several months in their targets' systems before going on the offensive by bypassing existing protections. The goal is thus to destabilise and flush them out by going off the beaten track. But to be effective, a "hunt" must be carefully organised – from upstream preparation to corrective measures. What are its main steps? What essential skills are required? What data should be provided to the "hunters"? What are the useful tools? How can this approach be implemented in the long run?

TR Quoi de neuf du côté des Threat Intelligence Platforms ?
What's new in the field of Threat Intelligence Platforms?

Les plateformes de "Threat Intelligence" permettent d’agréger, de normaliser, d’enrichir, de corréler, de visualiser et de partager des données d’origine diverse (données techniques d’origine interne ou externe, informations contextuelles sur les menaces, la “victimologie”…). Leur promesse est alléchante : permettre aux organisations d’évaluer en permanence leur niveau d’exposition, de raccourcir le temps de détection et de rendre actionnable le renseignement sur les menaces. Si elles ont progressé en maturité, elles restent des outils complexes, dont le déploiement est souvent délicat. Quelles sont les dernières nouveautés dans ce domaine ? Quels sont les apports de l’Intelligence artificielle et du Big Data ? Comment rendre ces plateformes plus intuitives en évitant le syndrome de la "boîte noire" ? Comment peuvent-elles permettre d’éviter les angles morts ? Comment peuvent-elles s’adapter au contexte métier des différents utilisateurs ?

Threat Intelligence Platforms make it possible to aggregate, standardise, enrich, correlate, visualise, and share data from various sources (technical data from internal or external sources, contextual information on threats, "victimology"…). Their tantalising promise is to enable organisations to constantly assess their level of exposure, shorten detection time, and make Threat Intelligence actionable. Although they have progressed in maturity, they remain complex tools that are often difficult to deploy. What are the latest developments in this field? What are the contributions of Artificial Intelligence and Big Data? How can these platforms be made more intuitive while avoiding the "black box" syndrome? How can they help avoid blind spots? How can they be adapted to the business context of the various users?

WEDNESDAY, SEPTEMBER 8TH
4pm – 5pm

MANAGEMENT DES CYBER RISQUES
CYBER RISK MANAGEMENT

TR

Comment s'assurer efficacement contre les cyberattaques ?
How can we insure effectively against cyberattacks?

Le coût médian des incidents de cybersécurité par entreprise a été multiplié par 6 en 2019 s'élevant de 9 000 € à 51 200 € (source : Hiscox). Les entreprises sont donc de plus en plus nombreuses à franchir le pas de l'assurance cyber. La souscription reste cependant complexe, notamment pour les ETI et PME, car elle suppose de s'être engagée dans une démarche d'analyse de risque permettant de cocher les bonnes options dans le contrat d'assurance. La comparaison entre les offres est par ailleurs difficile en raison des capacités et exclusions qui diffèrent d'un assureur à l'autre. L'exclusion des "actes de guerre" rend-elle les assurances inopérantes face à des attaques émanant potentiellement d'États ou de groupes sponsorisés (les assurances cyber n'auraient ainsi couvert que 3% des dommages causés par NotPetya) ? Quelles sont les garanties les plus courantes ? Comment couvrir les éventuels dommages causés au tiers ? Le remboursement éventuel des rançons en cas de ransomware est-il possible ? Qu'est-il prévu en termes d'indemnité pour pertes d'exploitation en cas d'interruption d'activité ? De frais de récupération des données et de remédiation ? De services de prévention et d'assistance ? Quelle collaboration entre les différents acteurs, tant du côté des assureurs que du client (courtier, DSI, DAF, RSSI, gestionnaire des risques) ?

The median cost of cybersecurity incidents per company has been multiplied by 6 in 2019, rising from €9,000 to €51,200 (source: Hiscox). More and more companies are therefore moving towards cyber insurance. However, underwriting remains complex, particularly for ETIs and SMEs, as it requires a risk analysis process to tick the right options in the insurance contract. Comparison between offers is also difficult because of the different capacities and exclusions of each insurer. Does the exclusion of "acts of war" make the insurance inoperative in the face of attacks potentially emanating from states or sponsored groups (in such case, cyber insurance would have covered only 3% of the damage caused by NotPetya)? What are the most common guarantees? How can potential damage caused to third parties be covered? Is it possible to reimburse ransoms in case of a ransomware attack? What compensation is foreseen for business interruption? Or for data recovery and remediation costs? Or for prevention and support services? What collaboration can exist between the various players, both on the insurers' side and on the client's side (broker, CIO, CFO, CISO, risk manager)?

WEDNESDAY, SEPTEMBER 8TH
4pm – 5pm

MANAGEMENT DES CYBER RISQUES
CYBER RISK MANAGEMENT

TR Comment sécuriser un environnement Cloud ?
How can we secure a Cloud environment?

Près de 80% des entreprises ont subi une fuite de données liée à leurs infrastructures de Cloud dans les 18 derniers mois (source : IDC/Ernetic). Causes principales : les erreurs de configuration des environnements de production, le manque de visibilité sur les accès et les activités ainsi qu'une gestion des identités et des accès souvent défaillante. Alors que ces infrastructures sont devenues une cible de choix pour les attaquants, quelles sont les priorités pour mieux les sécuriser ? Comment garantir la continuité de la politique de sécurité de l'entreprise dans le Cloud ? Quels sont les processus et outils à mettre en place ? Après le développement des Cloud Access Security Broker (CASB), quel est le rôle des solutions de Cloud Security Posture Management ?

Nearly 80% of companies have experienced a data leak related to their Cloud infrastructure in the last 18 months (source: IDC/Ernetic). The main causes are configuration errors in production environments, lack of visibility into access and activity, and faulty identity and access management. As these infrastructures have become a target of choice for attackers, what are the priorities for better securing them? How can we ensure the continuity of the company's security policy in the Cloud? What processes and tools need to be put in place? After the development of a Cloud Access Security Broker (CASB), what is the role of Cloud Security Posture Management solutions?

TR Comment faire de la conformité un pilier de la cybersécurité ?
How can we make compliance the cornerstone of cybersecurity?

Qu'elles soient transverses (LPM, NIS, RGS, RGPD, ISO 27001…) ou sectorielles (PCI DSS, PGSSI-S…), les obligations légales et réglementaires touchant à la cybersécurité ou à la protection des données personnelles sont de plus en plus nombreuses. Si elles sont d'abord des contraintes pour les organisations qui les mettent en oeuvre, elles peuvent aussi devenir des atouts. Au plan opérationnel, elles permettent de renforcer la maturité des organisations en fixant un cadre, notamment en matière d'évaluation des risques, et en "objectivant" la démarche de cybersécurité. En matière de communication, elles peuvent aussi contribuer utilement à la communication externe de l'entreprise, en temps de "paix" comme en tant de crise. Comment intégrer de la conformité "by design" dans les processus IT ? Quelles sont les "legal tech" utiles ? Comment valoriser ces démarches en termes de communication et de marketing ?

Whether cross-functional (French LPM and RGS, NIS, GDPR, ISO 27001, etc.) or sector-specific (PCI DSS, French PGSSI-S, etc.), legal and regulatory obligations relating to cybersecurity or the protection of personal data are becoming increasingly numerous. Though they are first and foremost constraints for the organisations that implement them, they can also become assets. At the operational level, they help to reinforce the maturity of organisations by setting a framework – particularly in terms of risk assessment – and by "objectivising" the cybersecurity approach. In terms of communication, they can also make a useful contribution to the company's external communication, in times of both "peace" and crisis. How can we integrate compliance "by design" into IT processes? What are the useful "legal techs"? How can these approaches be publicised in communication and marketing activities?

WEDNESDAY, SEPTEMBER 8TH
4pm – 5pm

LUTTE CONTRE LA CYBERCRIMINALITÉ
FIGHT AGAINST CYBERCRIME

TR

Soutien aux victimes et prévention des infractions... une approche peu explorée de la lutte contre la cybercriminalité
Supporting victims and preventing infractions: a little-explored approach in the fight against cybercrime

Puisqu'elle ne se limite pas à des attaques ciblées, la cybercriminalité touche tant les particuliers ou les collectivités locales que, plus largement, l'ensemble des acteurs économiques. Protéger les (potentielles) victimes en détectant et en prévenant ces menaces nécessite la mise en oeuvre d'actions de prévention toujours plus dynamiques : campagnes grand public, sensibilisation de proximité, détection ou recherche proactive de vulnérabilités dans les réseaux. Cette démarche repose sur la mobilisation d'une multitude d'acteurs, en proximité comme au niveau national. Elle suppose aussi une capacité d'adaptation constante aux évolutions de la menace, car comme ils l'ont démontré lors de la crise épidémique du Covid 19, les délinquants ont pour leur part su profiter de la désorganisation et de la vulnérabilité des organisations et des sociétés pour multiplier leurs attaques.

Since it is not limited to targeted attacks, cybercrime affects both individuals and local authorities and, more broadly, all economic stakeholders. To protect (potential) victims by detecting and preventing cyber threats, it is necessary to implement ever more dynamic prevention actions, such as general public campaigns, local awareness raising, and proactive search or detection for vulnerabilities in networks. This approach is based on the mobilisation of a multitude of players, both locally and at national level. It also presupposes a constant capacity to adapt to changes in the threat. Indeed, as demonstrated during the Covid-19 pandemic, criminals have been able to take advantage of the disorganisation and vulnerability of organisations and societies to multiply their attacks.

WEDNESDAY, SEPTEMBER 8TH
4pm – 5pm

TRANSFORMATION DIGITALE
DATA SAFETY AND DIGITAL TRANSFORMATION

TR

Énergie : le cyberrisque systémique ?
Energy: is cyber risk systemic?

Sociétés pétrolières et gazières, producteurs d'électricité, réseaux de distribution d'eau et d'électricité… : de plus en plus numérisée, l'industrie énergétique est une cible attractive pour les attaquants, que ceux-ci soient des groupes sponsorisés par des États souhaitant déstabiliser un adversaire ou des activistes s'opposant à des modèles énergétiques jugés dépassés. Les faits en témoignent : les attaques contre les systèmes industriels (Operational Technology ou OT) progressent de 2 000 % par an (source : IBM X-Force Threat Intelligence Index 2020). À côté de la mise en place d'un cadre réglementaire européen général relatif à la protection des infrastructures essentielles (directive NIS), différentes réglementations sectorielles ont vu le jour. Mais beaucoup reste à faire au plan opérationnel. Et il y a urgence : la transition énergétique passera par le numérique, et donc par la cybersécurité, ou ne passera pas.

The energy industry, with its numerous oil and gas companies, electricity production companies, and water and electricity distribution networks, is increasingly digitised, making it an attractive target for attackers, whether they are state-sponsored groups seeking to destabilise an adversary or activists opposing energy models deemed obsolete. The facts speak for themselves: attacks against industrial systems (Operational Technology, or OT) have been increasing by 2,000% per year (source: IBM X-Force Threat Intelligence Index 2020). In addition to the implementation of a general European regulatory framework for the protection of critical infrastructure (NIS directive), various sector-specific regulations have been released. But much remains to be done at the operational level. And there is urgency: energy transition will either go through digital – and therefore cybersecurity – or it will not.

THURSDAY, SEPTEMBER 9TH
12:45pm – 1:45pm

SÉCURITÉ ET STABILITÉ DANS LE CYBERESPACE
SECURITY AND STABILITY IN CYBERSPACE

TR Mercenaires et marchands d'armes, le nouveau farwest numérique
Mercenaries and arm dealers: the new digital far-west

La recrudescence des cyber-attaques d'origine étatique cache un autre phénomène : la multiplication de groupuscules, individus ou entreprises vendant leur expertise et leurs compétences en piratage au plus offrant pour mener, dans l'ombre, des attaques que les États ne peuvent pas assumer publiquement ou dont ils n'ont simplement pas les moyens ou les capacités. Ces « cyber-mercenaires » encouragent aussi une véritable course à l'armement et la prolifération d'« armes cyber » qui participent de la déstabilisation du cyberespace. Qui sont-ils et quels sont les États suspectés d'avoir le plus souvent recours à leurs services ? Sont-ils responsables des attaques et dommages qu'ils causent au nom d'autrui ? En l'absence de cadre juridique dédié, comment sanctionner leurs activités ? Et comment enrayer le développement d'armes de guerre cyber ?

The surge in state-originated cyberattacks hides another phenomenon: the multiplication of small groups, individuals, or companies selling their hacking expertise and skills to the highest bidder to carry out – in the shadows – attacks that states cannot publicly support or for which they simply do not have the means or capabilities. These "cyber mercenaries" also encourage a real arms race and the proliferation of "cyber weapons" that contribute to the destabilisation of cyberspace. Who are they and which states are most likely to use their services? Are they responsible for the attacks and damage they cause on behalf of others? In the absence of a dedicated legal framework, how can their activities be punished? And how can the development of cyber warfare weapons be stopped?

TR Comment lutter contre les fake news ?
How to fight against fake news

Désinformation, mésinformation, propagation de rumeurs, « intox »… les déclinaisons de la manipulation d'information sont nombreuses. Qu'elles soient conçues à des fins politiques (campagnes d'influence), diplomatiques (déstabilisation des processus électoraux), ou encore commerciales ; qu'elles aient pour objectif de promouvoir ou de dénigrer, les fake news menacent aujourd'hui les systèmes démocratiques. Si le phénomène n'est pas nouveau, la crise sanitaire lui a donné un grand coup d'accélération. Les fake news sont alors devenues un enjeu de santé publique. Mises au service de projets terroristes sur les réseaux sociaux, elles s'imposent aussi comme un nouvel enjeu sécuritaire. Comme ses causes, les réponses sont à la fois technologiques, techniques, politiques, règlementaires et sociétales… Quelles sont aujourd'hui les solutions les plus efficaces, et à quelles conditions?

Disinformation, misinformation, rumour spreading, fake news…there are many ways of manipulating information. Whether they are designed for political (lobbying campaigns), diplomatic (destabilisation of electoral processes), or commercial purposes, whether their aim is to promote or denigrate, fake news is currently threatening democratic systems. The phenomenon is not new, but the health crisis has given it a major boost. Fake news has therefore become a public health issue. Used by terrorist projects on social networks, it has also become a new security issue. Both its causes and the responses to it are at once technological, technical, political, regulatory, and societal… What are the most effective solutions today, and under what conditions?

THURSDAY, SEPTEMBER 9TH
12:45pm – 1:45pm

SÉCURITÉ OPÉRATIONNELLE
OPERATIONAL SECURITY

TR Comment sécuriser le travail à distance ?
Is it possible to secure teleworking?

La crise sanitaire et le télétravail généralisé ont provoqué différentes réactions. Chez les entreprises qui avaient déjà massivement recours au Cloud, ce n'est finalement que le dernier maillon de la chaîne encore au sein de l'entreprise, l'utilisateur, qui a été externalisé sans trop de difficultés. Chez celles qui n'avaient pas fait, ou ne pouvaient pas faire, la bascule "Cloud", le VPN a été la planche de salut, non sans difficultés et concessions en termes de cybersécurité. Phénomène ponctuel ou vraie tendance sociétale, le télétravail devrait en tout cas entraîner un recours croissant aux approches Zero Trust associant authentification forte, sécurisation des flux, contrôle du niveau de sécurité des terminaux pour permettre l'accès aux réseaux et applications depuis n'importe où.

The health crisis and widespread teleworking have provoked different reactions. For companies that already had massive recourse to the Cloud, it was actually only the last link in the chain that remained within the company – the user – that was outsourced without too many difficulties. For those who had not made, or could not make, the switch to the Cloud, the VPN was the lifeline, but it came with difficulties and concessions in terms of cybersecurity. Whether a one-off phenomenon or a real societal trend, teleworking should in any case lead to increasing use of Zero Trust approaches combining strong authentication, securing of flows, control of the level of security of terminals to allow access to networks and applications from anywhere.

TR IoT : le cauchemar "cyber" ?
Is IoT a "cyber" nightmare?

Système de santé, appareils domestiques intelligents, équipements de réseau électrique, systèmes industriels… : l'internet des objets fait désormais partie de notre vie quotidienne, professionnelle ou privée. Or la plupart de ces objets, dont le nombre devrait atteindre 20 milliards en 2024, ne sont pas ou peu sécurisés. Une récente étude de la société Palo Alto Networks révèle ainsi que 98% du trafic des objets connectés utilisés dans un environnement professionnel ne sont pas chiffrées. Pire : 57% d'entre eux comprendraient des vulnérabilités, générant un risque systémique préfiguré par le botnet Mirai (2016). Les défis sont multiples : former les concepteurs et développeurs de ces objets, intégrer de la sécurité "by design" lors du développement des futurs objets, superviser leur sécurité après leur mise en service, développer des bonnes pratiques et définir des standards, mettre à jour les firmware des objets déjà déployés etc.

Healthcare systems, intelligent domestic appliances, power network equipment, industrial systems… the Internet of Things has become part of our daily life, whether at work or at home. Yet most of these objects, whose number is expected to reach 20 billion in 2024, are unsecured or poorly secured. A recent study by the Palo Alto Networks company reveals that 98% of the traffic of connected objects used in a professional environment is not encrypted. Worse: 57% of them are said to contain vulnerabilities, generating a systemic risk prefigured by the Mirai botnet (2016). The challenges are manifold: training the designers and developers of these objects; integrating security "by design" during the development of future objects; supervising their security after they have been put into service; developing best practices and defining standards; updating the firmware of objects already deployed, etc.

THURSDAY, SEPTEMBER 9TH
12:45pm – 1:45pm

MANAGEMENT DES CYBER RISQUES
CYBER RISK MANAGEMENT

TR

Cloud: l'interopérabilité, passage obligé vers la souveraineté numérique ?
Cloud: is interoperability a necessary step towards digital sovereignty?

Si l'Europe investit fortement dans le digital, ses données et les applications associées sont aujourd'hui majoritairement hébergées chez des "hyperscalers" étrangers, principalement américains ou chinois. Cette situation présente pour certains un risque de dépendance industrielle et stratégique pour l'Europe, et ce d'autant qu'elle n'est pas en mesure de répondre seule à la croissance exponentielle de ses besoins. Il est essentiel pour l'Europe de garantir la sécurité et de la réversibilité de ses données, mais aussi l'interopérabilité des solutions utilisées et donc des services associés, pour conserver son indépendance et son autonomie. L'enjeu est de taille: s'il est sans doute déjà trop tard pour faire émerger une véritable industrie du cloud européenne capable de concurrencer les géants chinois et américains, il n'est pas trop tard en revanche pour bâtir un solide écosystème européen de la donnée et des services numériques. Au plan juridique, il s'agit par exemple, à l'instar de Gaia-X, d'établir des normes et standards partagés. Au plan technique, il convient notamment de mettre en place des processus partagés, des conteneurs et modèles de données communs, des API etc.

While Europe spends a lot of money on digital technology, its data and associated applications are mostly hosted by foreign — mainly American or Chinese — "hyperscalers". This situation poses a risk of industrial and strategic dependence for Europe, especially given its inability to meet on its own the exponential growth of its needs. To maintain its independence and autonomy, Europe must guarantee the security and reversibility of its data, but also the interoperability of the solutions used and therefore of the associated services. The stakes are high: while it is probably already too late to create a true European cloud computing market to compete with Chinese and American leaders, it is not too late to build a robust European ecosystem of data and digital services. From a legal point of view, it consists in following the example set by Gaia-X and establishing shared norms and standards. From a technical point of view, there is a need for the implementation of shared processes, common data models and containers, APIs, etc.

TR

Collaborer pour prendre de meilleures décisions en cybersécurité
How can we collaborate to make better cybersecurity decisions?

Qu'elles viennent des systèmes de sécurité, des applications ou de flux d'information externes, les remontées d'information et alertes envoyées au SOC sont de plus en plus nombreuses. La submersion menace même parfois, ce qui peut affecter l'efficacité du dispositif et la prise de décision. Il est donc essentiel d'améliorer l'intelligence collective en développant le partage de la situation opérationnelle, la contextualisation et hiérarchisation des alertes, l'orchestration et suivi de la réponse à incidents, l'utilisation de "playbooks", l'automatisation de certains processus… Comment renforcer le travail collaboratif au sein du SOC ? Entre le SOC et les autres fonctions IT ? Quelles sont les bonnes pratiques en la matière ?

Whether they come from security systems, applications, or external information flows, the information feedback and alerts sent to the SOC are increasingly numerous. This can even lead to submersion, which can affect decision making and the effectiveness of the system. It is therefore essential to improve collective intelligence by developing the sharing of the operational situation, the contextualisation and prioritisation of alerts, the orchestration and monitoring of incident response, the use of "playbooks", the automation of certain processes, etc. How can we strengthen collaborative work within the SOC? And between the SOC and other IT functions? What are the best practices in this area?

THURSDAY, SEPTEMBER 9TH
12:45pm – 1:45pm

LUTTE CONTRE LA CYBERCRIMINALITÉ
FIGHT AGAINST CYBERCRIME

TR Comment une coalition internationale peut faire tomber des réseaux cybercriminels : retour d'expérience
Feedback: the dismantling of criminal networks by an international coalition

En juillet 2020, le démantèlement du réseau EncroChat par les autorités policières et judiciaires françaises et néerlandaises, soutenues par Europol et Eurojust, signe un nouveau succès de la coopération internationale en matière de lutte contre la cybercriminalité. Cette affaire, très médiatisée, est cependant loin d'être le seul exemple d'opération conjointe réussie, tant au niveau européen qu'international. Sur quels dispositifs de coopération bilatéraux et multilatéraux peuvent s'appuyer ces coalitions ? Quel cadre pour définir les rôles et responsabilités respectives des États et des organisations internationales ? Pour faciliter le partage d'information ? Et quel rôle pour les États ?

In July 2020, the dismantling of the EncroChat network by the French and Dutch police and judicial authorities, supported by Europol and Eurojust, marks a new success for international cooperation in the fight against cybercrime. This case received a lot of media attention, but it is far from being the only example of a successful joint operation, both at European and international level. What bilateral and multilateral cooperation mechanisms can these coalitions rely on? What framework should we use to define the respective roles and responsibilities of states and international organisations? To facilitate information sharing? And what role should states play?

TR Quel cadre juridique pour l'échange transfrontier de données dans le cadre d'une enquête ?
What legal framework should we use to regulate cross-border data exchange?

Le succès de l'opération Encrochat en juillet 2020 a rappelé qu'il était primordial, dans le cadre de coopérations policières et judiciaires transfrontalières, de permettre aux enquêteurs de partager et d'échanger des données de façon fluide et en toute sécurité. De fait, les outils règlementaires encadrant l'échange transfrontaliers de données dans le cadre d'une enquête sont nombreux et variés : bilatéraux (MLAT), ou multilatéraux, régionaux (E-Evidence, Cloud Act), ou internationaux (Convention de Budapest)…Comment s'articulent tous ces dispositifs ? Dans leur état actuel, permettent-ils aux enquêteurs d'échanger efficacement les données et preuves indispensables aux enquêtes ?

The success of the Encrochat operation in July 2020 reminded us how essential it is – in the context of cross-border police and judicial cooperation – to enable investigators to share and exchange data seamlessly and securely. In fact, there are many regulatory tools governing the cross-border exchange of data in the context of an investigation: bilateral (MLATs), multilateral, regional (E-Evidence, Cloud Act), and international (Budapest Convention). How do all these mechanisms fit together? In their current state, do they enable investigators to efficiently exchange the data and evidence required by investigations?

THURSDAY, SEPTEMBER 9TH
12:45pm – 1:45pm

TRANSFORMATION DIGITALE
DATA SAFETY AND DIGITAL TRANSFORMATION

TR

Cybersécurité et automobile : accélération en vue
Cybersecurity in automotive: full speed ahead

Un véhicule contient aujourd'hui en moyenne 150 cartes électroniques et 100 millions de lignes de code. Une tendance qui va encore se renforcer avec le développement des véhicules connectés et autonomes. Les défis en termes de protection des données personnelles et de cybersécurité sont multiples : sécurité des systèmes embarqués, utilisation de protocoles sans fil peu sécurisés faute d'authentification, maintien en conditions de sécurité tout au long du cycle de vie, supervision… Pour y répondre, différents travaux de normalisation ont été engagés : le règlement WP-49 élaboré dans le cadre de l'UNECE (United Nations Economic Commission for Europe) s'imposera dès 2024 aux constructeurs français. L'International Organization for Standardization (ISO) travaille également sur le standard ISO/SAE 21434 "véhicules routiers - Ingénierie de la sécurité" qui définira des exigences en matière de cybersécurité "by design". Point sur les travaux en cours avec les différents acteurs du domaine.

Today, a vehicle contains an average of 150 electronic cards and 100 million lines of code. A trend that will further increase with the development of connected and autonomous vehicles. This creates many challenges in terms of personal data protection and cybersecurity: security of onboard systems, use of wireless protocols that are not very secure due to lack of authentication, maintenance of security conditions throughout the life cycle, supervision, etc. To overcome these challenges, various standardisation projects have been launched, among which the WP.49 regulation drawn up within the framework of UNECE (United Nations Economic Commission for Europe), which will be binding on French manufacturers from 2024 onwards. The International Organization for Standardization (ISO) is also working on the ISO/SAE 21434 standard entitled "Road vehicles – Cybersecurity engineering", which will define requirements in terms of cybersecurity "by design". Update on work in progress with the various players in the field.

TR

E-santé et télémédecine : quelle sécurité pour ces nouveaux usages ?
E-health and telemedicine: what are the security measures required for these new functions?

La e-santé et la télémédecine ont fait un bond spectaculaire avec la crise sanitaire : de 40 000 actes en téléconsultation au mois de février 2020 à 150 000 par semaine en septembre 2020. Une tendance lourde qui va de pair avec le développement des attaques ciblant le monde de la santé : au total 478 incidents ont été déclarés en 18 mois entre octobre 2017 et février 2018 auprès de la Cellule d'accompagnement cybersécurité des structures de santé (ACSS). Les risques sont multiples (intégrité des données, confidentialité, disponibilité, traçabilité des échanges) et concernent tous les maillons de la chaîne : les équipements médicaux, les flux de communication, les systèmes d'information mais aussi l'Humain, personnel de santé et patients. Comment renforcer la sécurité de ces nouveaux usages ? Quelles sont les priorités ? Quel cadre réglementaire ? Quelles bonnes pratiques ?

E-health and telemedicine have taken a spectacular leap forward with the health crisis: from 40,000 medical teleconsultations in February 2020 to 150,000 per week in September 2020. A strong trend that goes hand in hand with the development of attacks targeting the health sector: a total of 478 incidents were reported in 18 months between October 2017 and February 2018 to the French ACSS (Cyber Security Support Unit for Healthcare Structures). The risks are manifold (data integrity, confidentiality, availability, traceability of exchanges) and concern all the links in the chain: medical equipment, communication flows, information systems, but also people, i.e., healthcare staff and patients. How can the security of these new uses be reinforced? What are the priorities? What is the regulatory framework? What are the best practices?