cyber sécurité : Chaire grands événements publics
Fondation Université Bretagne Sud

Conférence
Jeudi 16 mai 2024

RAPPORT D'EVENEMENT

Cybercriminalité : Paris 2024 enjeux et défis de la sécurisation de l'espace numérique

01 *Introduction*

Le jeudi 16 mai dans la cadre du cycle de conférences organisé par la chaire Cybersécurité des Grands Evènements Publics, Myriam Quéméner était invitée à intervenir sur le thème « **Cybercrimenalité : Paris 2024, enjeux et défis de la sécurisation de l'espace numérique** ». Magistrate, docteur en droit, avocate près la Cour d'appel de Paris et spécialiste de la cybercriminalité, elle a abordé entre autre les sujets suivants :

- l'évolution de la cybercriminalité et coopération internationale,
- les évolutions législatives en matière de cybersécurité,
- les mesures spécifiques pour les Jeux Olympiques,
- l'encadrement des fausses nouvelles et défis juridiques
- et la coopération entre secteurs public et privé.

Cet évènement s'est déroulé à la Préfecture du Morbihan avec le soutien du Groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres (GICAT).

La chaire Cybersécurité des Grands Evènements Publics est portée par la fondation de l'UBS dont une des missions est de réunir le monde universitaire et les acteurs socio-économiques autour de questionnements communs tel que la cybersécurité.

www-fondation.univ-ubs.fr

02

Monsieur Pascal Bolot
Préfet du Morbihan

En introduction, Monsieur le Préfet du Morbihan, Pascal BOLOT a mis en exergue plusieurs points clés. Il a rappelé tout d'abord que les attaques cybernétiques ont un spectre très large et qu'elles évoluent de l'escroquerie classique à des attaques sophistiquées souvent liées à des enjeux géopolitiques, menées par des États ou leurs proxys. Même si la Coupe du monde de rugby s'est par ailleurs bien déroulée, les prochains Jeux Olympiques et Paralympiques, ainsi que les élections européennes, représentent des cibles potentielles, nécessitant une vigilance accrue en matière de cybersécurité.

Les cyberattaquants améliorent continuellement leurs compétences, notamment en intégrant l'intelligence artificielle, ce qui crée un environnement complexe et potentiellement dangereux. En réponse, des efforts significatifs sont déployés tant au niveau national que local. Le département du Morbihan a mis en place des initiatives avec des audits de sécurité dans 90 communes. Une équipe spécialisée de la Gendarmerie Nationale travaille auprès des entreprises locales pour promouvoir des pratiques de sécurité d'hygiène numérique, des mesures de prévention, visant à renforcer la résilience des infrastructures critiques.

L'environnement universitaire joue un rôle crucial dans cette dynamique, avec des formations dédiées à la cybersécurité. Un forum départemental a attiré plus de 400 participants, et un exercice de gestion de crise a été réalisé avec des étudiants. L'ouverture d'un Campus DataSciences & CyberSécurité est prévu pour 2025, visant à renforcer cette filière.

Enfin, Monsieur le préfet a souligné la volonté collective de faire du Morbihan un département leader en matière de cybersécurité et de formation, en saluant les efforts de tous les acteurs impliqués.

Il remercie Mme Quéméner, magistrate spécialiste de la cybercriminalité, d'avoir accepté de venir évoquer les défis de la judiciarisation des cybercriminels afin de souligner la complexité des investigations.

03

Virginie Dupont
Présidente de l'Université Bretagne Sud

Virginie Dupont, Présidente de l'Université Bretagne Sud a exprimé sa satisfaction à participer à cette conférence dédiée aux enjeux de sécurisation de l'espace numérique dans le cadre des Jeux Olympiques 2024, qui se dérouleront principalement à Paris et sur l'ensemble de notre territoire. Une soirée qui clôture la deuxième édition de "L'Instant Cyber", organisée sur le campus par le collectif cyber de proximité de Vannes, qui a rassemblé plus de 350 personnes cette même journée. Elle a félicité tous les organisateurs pour son succès.

Elle a rappelé que cette conférence, organisée par la chaire Cybersécurité des Grands Événements Publics, était d'une importance particulière pour notre pays, alors que nous nous préparons à accueillir le monde entier. La protection des infrastructures numériques des Jeux est, selon elle, essentielle pour garantir la sécurité des athlètes, des spectateurs, ainsi que pour préserver l'intégrité des données et des systèmes informatiques impliqués.

La cybersécurité est devenue un pilier central de la préparation des grands événements internationaux. Les cyberattaques peuvent cibler les systèmes de billetterie, les réseaux de communication, les plateformes de diffusion, ainsi que les infrastructures critiques comme les transports et l'énergie. Une approche proactive et collaborative est indispensable pour prévenir, détecter et répondre efficacement à ces menaces.

La chaire Cybersécurité des Grands Evénements Publics, portée par la Fondation de l'Université Bretagne Sud, a été créée pour organiser des espaces d'échange afin de relever ces défis complexes.

Virginie Dupont a également à remercié le GICAT pour son soutien, représenté ce soir-là par son délégué général adjoint, Monsieur Gérard Lacroix.

Enfin la présidente a tenu à réaffirmer l'engagement de l'Université Bretagne Sud à rester à l'avant-garde en matière de formation, de recherche et d'innovation dans le domaine de la cybersécurité afin de transformer les défis numériques en opportunités et d'assurer un environnement cyber plus sûr.

04

Myriam Quéméner
Magistrat - Docteur en droit

Myriam Quemener a ouvert son intervention en exprimant sa gratitude envers les organisateurs de la conférence pour l'invitation. Elle a souligné son engagement de longue date dans la lutte contre la cybercriminalité, un domaine dont l'importance ne cesse de croître.

Évolution de la cybercriminalité et coopération internationale

La Magistrate a abordé dans un premier temps l'évolution de la cybercriminalité, expliquant que les menaces sont passées de simples escroqueries à des attaques sophistiquées ayant des implications géopolitiques. Elle a salué l'amélioration notable de la coopération internationale en matière de cybersécurité, en citant des affaires emblématiques telle que l'affaire Sky ECC. Ce type d'affaire est traité à la Cour d'appel de Paris, et nécessite une mobilisation considérable des services en France et à l'étranger, démontrant l'importance d'une collaboration transfrontalière efficace.

Évolutions législatives en matière de cybersécurité

Myriam Quéméner a ensuite détaillé les évolutions législatives françaises en matière de cybersécurité, soulignant des lois clés comme la loi Informatique et Liberté de 1978, modifiée pour s'aligner sur le RGPD, et la loi Godfrain de 1988, qui a été une pionnière dans la criminalisation des actes de cyber-délinquance. Elle a également évoqué des législations plus récentes, telles que les outrages en ligne, visant à encadrer les comportements délictueux sur Internet. Elle a mentionné la nouvelle loi sur la sécurisation de l'espace numérique, introduisant des infractions spécifiques pour les fake news et les outrages en ligne, indépendamment du contexte électoral.

Importance de la cybersécurité pour les Jeux Olympiques 2024

En soulignant l'importance de la cybersécurité dans la préparation des grands événements internationaux comme les Jeux Olympiques, l'intervenante a mentionné les multiples cibles potentielles pour les cyberattaques, y compris les systèmes de billetterie, les réseaux de communication, les plateformes de diffusion et les infrastructures critiques. Elle a insisté sur la nécessité d'une approche proactive et collaborative pour prévenir, détecter et répondre efficacement à ces menaces.

Sensibilisation et formation continue

Madame Quéméner a mis en avant l'importance de la sensibilisation et de la formation continue, non seulement pour les professionnels de la cybersécurité mais aussi pour le grand public. Elle a souligné que la sensibilisation dès le plus jeune âge est essentielle pour inculquer des réflexes de cybersécurité. Elle a salué les efforts de plateformes comme cybermalveillance.gouv.fr, qui joue un rôle crucial dans la sensibilisation et l'accompagnement des victimes de cyberattaques.

Mesures spécifiques pour les Jeux Olympiques

L'intervenante a discuté des mesures spécifiques mises en place pour sécuriser les Jeux Olympiques, comme les caméras augmentées et les scanners corporels. Elle a précisé que ces dispositifs sont encadrés par la loi, sans recours à la reconnaissance faciale, et sont utilisés de manière limitée dans le temps pour des objectifs précis, comme la détection d'objets abandonnés ou de comportements suspects. Elle a insisté sur l'importance de ces mesures dans le contexte actuel de menaces accrues.

Encadrement des fausses nouvelles et défis juridiques

Elle a abordé la question des fausses nouvelles (fake news), en expliquant les législations mises en place pour encadrer ce phénomène. Elle a cité la loi de décembre 2018 et la loi récente sur la sécurisation de l'espace numérique, qui introduit une infraction spécifique pour les fake news hors contexte électoral. Elle a également souligné les défis juridiques posés par la cybercriminalité, nécessitant une spécialisation des magistrats et des procédures adaptées, comme l'enquête sous pseudonyme et la captation de données à distance.

Coopération entre secteurs public et privé

M.Quéméner a insisté sur la nécessité d'une coopération étroite entre les secteurs publics et privés dans la lutte contre les cybermenaces. Elle a reconnu les défis institutionnels mais a affirmé que des efforts continus sont déployés pour améliorer cette collaboration. Elle a mentionné des initiatives locales et nationales visant à renforcer cette coopération, y compris des exercices de crise et des réunions de coordination.

En conclusion, l'intervenante a réaffirmé l'importance de développer un maillage territorial efficace et de promouvoir la transparence et la communication des entreprises victimes de cyberattaques. Elle a encouragé une plus grande spécialisation des magistrats dans la lutte contre la cybercriminalité et a appelé à une vigilance continue face aux évolutions technologiques et législatives. Elle a salué l'excellence des initiatives locales et nationales en matière de cybersécurité et terminé son propos en soulignant que malgré les défis posés par la cybercriminalité, les efforts conjoints de sensibilisation, de législation et de coopération internationale permettront de transformer les défis numériques en opportunités et de garantir un environnement numérique plus sûr pour tous.

Y a t-il assez de magistrats aguerris et formés pour répondre à ces attaques pour certaines devenues quasi-industrielles ?

"Les effectifs doivent être renforcés mais il existe d'ors et déjà des réponses spécifiques mises en place pour traiter ce contentieux qui explose. Il existe la section J3 du parquet de Paris qui s'est étoffée dernièrement . Il faut aussi indiquer que dans les procédures souvent complexes et à dimension internationale, des juges d'instruction très spécialisés sont saisis .
Des formations sont dispensées à l'Ecole nationale de la magistrature , parfois en lien avec le barreau de Paris. Les magistrats qui traitent ces affaires peuvent aussi faire des stages dans les services de police et de gendarmerie spécialsés ainsi qu'auprès des douanes .
Les magistrats du siège doivent aussi de plus en plus se spécialiser. Par exemple, à la Chambre d'instruction, j'avais beaucoup d'affaires d'appel de saisie de cryptoactifs qui nécessite des connaissances assez techniques sur leur fonctionnement .
Quand on évoque la création éventuelle d'un parquet national en matière de criminalité organisée, je préférerais, pour ma part, que soit créé un parquet dédié à la cybercriminalité d'envergure que l'on nomme parfois comme étant le haut du spectre. Il y a une prise de conscience très nette au niveau étatique, mais il faut monter en puissance tant au niveau des magistrats du parquet que du siège .

En matière de haine sur internet et de cyber-harcèlement, il existe désormais une infraction spécifique pour réprimer ce comportement ; ces affaires sont traitées par un pôle dédié au parquet de Paris . On commence à avoir de plus en plus de condamnations.
Par ailleurs, on arrive à démanteler des réseaux à l'instar d'affaires emblématiques comme celles dénommées " En crochat " et "Sky ECC" . Il s'agissait d'applications hyper chiffrées devenues, le moyen de communication privilégié des plus gros criminels pour contourner les forces de l'ordre. L'enquête a démarré parce que cette application était vendue dans des "arrières boutiques" sans autorisation. Les services d'enquête ont pu établir que ces applications étaient utilisées pour des trafics de stupéfiants d'envergure et des affaires criminelles . C'est un travail de coopération renforcée avec l'ensemble des acteurs et une coopération public/ privé qui a permis ces coups de filet très importants."

05 *Anne Le Hénanff*
Députée du Morbihan

Madame la députée a débuté son discours en exprimant son enthousiasme à l'idée de réagir après Madame Quéméner. Elle a ensuite présenté le rôle du législateur dans la lutte contre la cybercriminalité, un sujet dont tous les acteurs de la société doivent se préoccuper.

Objectifs du législateur

L'action législative dans ce domaine est guidée par quatre objectifs majeurs : encadrer, réguler, sanctionner et contrôler. Elle a indiqué qu'un nombre croissant de lois intègrent désormais des dispositions en matière de cybersécurité et cybercriminalité, des textes qui auparavant ne les mentionnaient pas.

Exemples de législation récentes

- Loi sur la sécurité des Jeux Olympiques
- Loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI) : Adoptée en avril 2023, cette loi stipule que les entités victimes de cyberattaques doivent déclarer l'attaque dans les 72 heures pour prétendre à une indemnisation assurancielle. Cela vise à accélérer la montée en compétence des organisations en matière de cybersécurité.
- Loi de programmation militaire 2024-2030

Madame Le Hénanff a détaillé la Loi de programmation militaire 2024-2030, sur laquelle elle a beaucoup travaillé pour accroître les prérogatives de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Elle a mentionné deux actions majeures :

- Filtrage et blocage des noms de domaine : L'ANSSI peut désormais filtrer, bloquer, voire suspendre des noms de domaine chez des hébergeurs en cas de menace à la défense et à la sécurité nationale.
- Signalement des vulnérabilités par les éditeurs de logiciels : les éditeurs doivent signaler toute vulnérabilité critique ou incident sur leurs systèmes d'information dans les 48 heures.

Débats sur la protection des libertés individuelles

Anne Le Hénanff a souligné les débats suscités par ces mesures, en particulier l'équilibre entre la protection des libertés individuelles et la nécessité de surveillance. Elle a insisté sur la légitimité de l'ANSSI et son cadre strict d'opérations, avec des agents habilités et des données collectées uniquement à des fins de sécurité nationale.

Rapport sur la cyberdéfense et transposition de la directive NIS2

Elle a mentionné le rapport sur la cyberdéfense publié en janvier 2024, co-écrit avec le député d'Ille et Vilaine, Frédéric Matthieu, et en a recommandé sa lecture. Il a été fait mention de la directive NIS2, qui exigera la mise en conformité de 12 000 à 15 000 entités françaises avec des normes de cybersécurité accrues. Elle a averti que cette transition serait coûteuse et complexe, nécessitant une adaptation sur trois ans, similaire à celle de la mise en œuvre du RGPD.

En conclusion, Anne Le Hénanff a insisté sur la nécessité d'une coopération européenne pour réussir cette transition. Elle a réaffirmé que le travail d'équipe avec les partenaires européens est crucial pour relever les défis de la cybersécurité, terminant sur une note d'optimisme quant à la capacité collective de surmonter ces obstacles.

06

David Robo, Maire de Vannes Président de Golfe Morbihan Vannes Agglomération

Monsieur le Président a commencé son discours par une remarque humoristique en réfutant les propos de Monsieur le Préfet, affirmant qu'il n'y avait pas "d'affranchis" dans la salle et exprimant sa gratitude d'avoir Anne Le Hénanff à ses côtés depuis plus de dix ans, une pionnière dans le domaine de la cybersécurité sur leur territoire.

Monsieur Robo a détaillé l'expérience de la ville de Vannes dans la gestion des problématiques de cybersécurité, soulignant qu'ils avaient traité ces questions bien avant de nombreux autres territoires, y compris dans des villes de taille moyenne comme la leur. Il a mentionné un incident survenu il y a 18 mois dans une commune voisine, où une cyberattaque a paralysé les systèmes municipaux, mettant en lumière la vulnérabilité des petites collectivités locales face à ces menaces.

Monsieur Robo a évoqué plusieurs initiatives importantes pour renforcer la cybersécurité et promouvoir l'innovation numérique, notamment la création du Campus DataSciences & CyberSécurité (ouverture prévue à la rentrée 2025). Situé près du siège de GMVA, ce campus numérique représente un investissement de plus de 20 millions d'euros. A 3 ans, l'objectif est d'accueillir 1 000 étudiants. Ce nouvel équipement vise à créer un écosystème dynamique qui bénéficiera aux entreprises locales et aux collectivités pour fournir des services de cybersécurité. Il a également mentionné le rôle crucial des élus nationaux et locaux dans la défense et le soutien des collectivités locales, tout en remerciant Anne Le Henanff pour son engagement et ses efforts dans ce domaine.

07

Inès Dos Anjos, Présidente de l'association HACK2G. Apprentie ingénieure cyberdéfense à l'ENSIBS

En tant qu'étudiante à l'ENSIBS (en alternance en cyberdéfense), elle a souligné l'importance d'intégrer le dynamisme et le regard des jeunes dans le domaine de la cybersécurité.
Elle a évoqué le partenariat en cours entre l'association HACK2G, la préfecture du Morbihan et la Gendarmerie nationale pour accompagner et former les collectivités. Cette nouvelle convention de partenariat associe 90 communes qui ont répondu à une enquête sur leur maturité en cybersécurité. L'objectif est d'aider ces collectivités à mettre en œuvre les recommandations et à se protéger, réagir contre les cyberattaques croissantes. Hack2G2 apportera son expertise sur ces questions.
Inès Dos Anjos a également décrit sa mission chez Diamteam à Brest où elle fait son alternance. Elle construit des scénarios basés sur les modes opératoires des groupes de cyberattaquants et anime des exercices de gestion de crise pour divers publics.
À seulement 21 ans, elle joue un rôle clé dans la formation et la préparation des collectivités locales contre les cybermenaces.

07 *Gérard Lacroix, Délégué général adjoint à la sécurité du GICAT*

Monsieur Lacroix, après avoir remercié Myriam Quéméner pour son intervention et souligné l'importance de la lutte contre la cybercriminalité, a rappelé que la cyberdéfense n'est pas de la science-fiction mais une réalité vécue au quotidien par les acteurs de la défense et de la sécurité.

Représentant le groupement des industriels de défense et de sécurité terrestres et aéroterrestres (GICAT), il a insisté sur l'état de guerre permanente dans le cyberespace, citant les conflits en Ukraine et en Palestine. Il a appelé à une prise de conscience et à une mobilisation générale de toutes les forces et intelligences du pays pour maintenir la position de la France sur la scène internationale.

L'intervenant a aussi salué les 460 entreprises membres du GICAT, telles que Thales, Airbus, Atos et Orange, qui jouent un rôle crucial dans cette lutte en fournissant les moyens nécessaires à l'État pour contrer les ingérences étrangères.

Il a conclu en réaffirmant le soutien continu du GICAT à l'Université Bretagne Sud (UBS) qui devrait s'accentuer, et en félicitant la ville de Vannes pour son intuition et son avance dans la réflexion sur la cybersécurité. Il a enfin cité le dramaturge Henry Bernstain :
« *L'intuition est l'intelligence qui a commis un excès de vitesse* » pour souligner les actions menées à Vannes depuis déjà dix dans le domaine.

07

Remerciements

La chaire Cybersécurité des Grands Evénéments Publics tient à remercier chaleureusement :

- Monsieur le Préfet, Pascal Bolot
- Les équipes de la Préfecture du Morbihan
- Les intervenant.e.s
- Le GICAT, mécène de la chaire
- Et toutes les personnes présentes lors de cette conférence.

Crédit photos : Préfecture du Morbihan

Contact Chaire Cybersécurité des Grands Evénements Publics :
Salah SADOU - porteur de la Chaire
salah.sadou@univ-ubs.fr

Contact Fondation UBS :
fondation@univ-ubs.fr
www-fondation.univ-ubs.fr

Fondation :
Université Bretagne Sud