LES JEUX OLYMPIQUES DE PARIS 2024 : UN DÉFI DE CYBERSÉCURITÉ MONDIAL

FAUSTINE DORINET
20 MARS 2024

Crédit photo : Les anneaux olympiques devant la Tour Eiffel, pour célébrer l'organisation par Paris des JO 2024 - Getty Images

DEFINSEEC.COM DEFINSEEC@GMAIL.COM 07 83 51 70 94

LES JEUX OLYMPIQUES DE PARIS 2024 : UN DÉFI DE CYBERSÉCURITÉ MONDIAL

Les Jeux olympiques et paralympiques de Paris 2024 s'annoncent comme un événement d'envergure mondiale, se déroulant du 26 juillet au 11 août 2024. Avec la participation de 15 000 athlètes venant de 206 nations, répartis sur 22 villes et 40 sites de compétition, ces jeux englobent 878 épreuves dans 54 sports différents. Attirant l'attention de plus de 10 millions de spectateurs sur place et de 4 milliards de téléspectateurs à travers le monde, cet événement médiatique offre une vitrine sans précédent. Cependant, cette visibilité extraordinaire attire également les cybercriminels, qui voient dans les Jeux une opportunité pour mener des attaques en ligne. La menace est d'autant plus accrue avec le contexte géopolitique actuel.

Stratégie de Cybersécurité

Face à cette menace, les organisateurs des Jeux de Paris 2024 ont mis en place une stratégie de cybersécurité. Cette stratégie repose sur plusieurs piliers, dont la sensibilisation, la formation et l'entraînement du personnel impliqué dans l'organisation des jeux. En effet, la numérisation croissante des Jeux olympiques et paralympiques les expose à un large éventail de menaces cyber.

Pour contrer ces dangers, Elisabeth Borne a confié à l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) la responsabilité de piloter la stratégie de prévention des cyberattaques pour les Jeux. Un budget d'un peu plus de 10 millions d'euros a été alloué à l'agence par la loi relative aux Jeux olympiques pour faire réaliser des audits de sécurité. La stratégie de cybersécurité des JO repose sur cinq axes principaux :

- Parfaire la connaissance des menaces cyber pesant sur les Jeux ;
- Sécuriser les systèmes d'information critiques ;
- Protéger les données sensibles ;
- Sensibiliser l'écosystème des Jeux ;
- Se préparer à intervenir en cas d'attaque cyber affectant les Jeux.

Ainsi, l'ANSSI, en collaboration avec différentes structures, dont la Délégation Interministérielle aux Jeux Olympiques et Paralympiques (DIJOP) et le ministère de l'Intérieur et des Outre-Mer (MIOM), déploie des actions spécifiques pour sécuriser les systèmes d'information critiques. Des audits de cybersécurité et des accompagnements techniques sont menés pour une cinquantaine d'acteurs critiques impliqués dans les Jeux.

Affiche de l'ANSSI pour les jeux olympiques de 2024 Jeux olympiques et paralympiques de Paris 2024 : l'ANSSI dans les starting-blocks | ANSSI (cyber.gouv.fr)

Partenariats et Technologie

Pour renforcer la cybersécurité, la ville de Paris a également établi des partenariats avec des entreprises spécialisées telles que Atos ou Cisco. Les deux entreprises apportent leur expertise et leurs technologies pour identifier et contrer les cybermenaces potentielles. Atos se charge également de l'hébergement des données sensibles des jeux, assurant ainsi leur sécurité et leur confidentialité. Ensemble, les entreprises et Paris 2024 ont développé un centre opérationnel de sécurité dédié aux jeux, chargé de surveiller en permanence les activités en ligne suspectes. Ce centre utilisera des technologies avancées, telles que l'intelligence artificielle, pour détecter et contrer les menaces potentielles.

Le **Comité International Olympique** (CIO) a également pour partenaire Alibaba, géant du commerce en ligne chinois. Il devrait délivrer des solutions de cloud pour l'évènement. Ce partenariat pose questions, notamment sur la protection des données personnelles et la souveraineté numérique des Etats, surtout dans un contexte géopolitique instable.

La cybersécurité est un défi mondial, c'est pourquoi les organisateurs des jeux échangent également des informations et collaborent avec d'autres pays et organisations pour partager les meilleures pratiques en matière de cybersécurité. Cette coopération permettra de renforcer la protection des jeux contre les attaques en ligne.

Préparation et Sensibilisation

En prévision des Jeux, plusieurs exercices de crise de des s**imulations d'attaques** sont organisés pour préparer les équipes à réagir en cas de cyberattaques. Ces entrainements ont aussi pour but de tester et d'améliorer le dispositif de protection. L'ANSSI propose également des exercices "clé en main" adaptés au niveau de maturité des acteurs des Jeux, afin de renforcer leur préparation face aux menaces cyber.

Un vaste plan de **sensibilisation** est aussi envisagé, visant à informer et former plusieurs centaines d'acteurs de l'écosystème des Jeux sur les menaces cyber et les bonnes pratiques de cybersécurité. De fait, les erreurs humaines représentent 95% des cas de cyberattaques.

Des séminaires de sensibilisation ont été organisés par les différents acteurs de la cybersécurité des JO, pour les collaborateurs de l'organisation, les fournisseurs ou les prestataires. Les athlètes auront des affiches à dispositions indiquant les gestes à suivre pour plus de cybersécurité.

LES JEUX OLYMPIQUES DE PARIS 2024 : UN DÉFI DE CYBERSÉCURITÉ MONDIAL

Trois familles de risques ont été identifiées lors des tests, et doivent faire l'objet d'une attention particulière de la part de tous, mais aussi de sensibilisation :

- Les opérations, afin que la diffusion, l'écosystème billettique et le réseau fonctionnent de manière optimale.
- Les professionnels des Jeux : ce sont principalement les membres du comité d'organisation, ainsi que les journalistes, athlètes et partenaires dont l'activité numérique doit être sécurisée.
- Enfin, l'organisation Paris 2024, dont les revenus sont numérisés et donc fortement exposés.

Les Risques Identifiés

Lors des JO de Londres, plus de 212 millions de cyberattaques sont relevées dès le jour de la cérémonie d'ouverture, marquée par de multiples offensives comme un déni de service distribué sur l'infrastructure électrique. Les Jeux Olympiques de Tokyo en 2021 ont enregistré eux plus de quatre milliards d'incidents cyber, soit 815 par seconde. Un chiffre impressionnant, mais Paris redoute **jusqu'à huit à dix fois plus d'incidents cyber**. Ces risques concernent tous les systèmes informatiques sans exception : les systèmes centraux de l'organisation, la billetterie, les salles de presse, les systèmes d'entrée dans les stades, les retransmissions télévisées et les infrastructures critiques (électrique, communication, transport).

À quelques semaines du coup d'envoi, Paris 2024 et un de ses partenaire, Atos, se préparent à tous les scénarios. Les attaques ont déjà commencé contre des sites tels que le portail des volontaires ou la billetterie, mais elles n'ont pas encore eu de conséquences majeures. **Christophe Thivet,** responsable de la sécurité des jeux chez Atos, évoque la possibilité d'interruption de compétitions ou de cérémonies d'ouverture. On peut aussi imaginer des attaques contre le chronométrage ou le système antidopage, voire le transport ou la billetterie, précise **Vincent Strubel** (directeur de l'ANSSI). D'autres genre d'attaques, d'intensité moindre, sont également à prendre en compte : des surcharges de systèmes (rendre des sites web inaccessibles), vols de donnés, arnaques en lignes ou détournements de comptes sur les réseaux sociaux.

Un **centre opérationnel technologique** sera installé au siège de Paris 2024 et supervisé par Atos, à Saint-Denis, pour évaluer et contrer en temps réel les cybermenaces. L'équipe de cette tour de contrôle va, le moment venu, surveiller en continu ce qui se passe sur les systèmes d'information, mais aussi sur Internet pour essayer de détecter, traiter et remédier les attaques et les menaces dont les JO vont inévitablement faire l'objet.

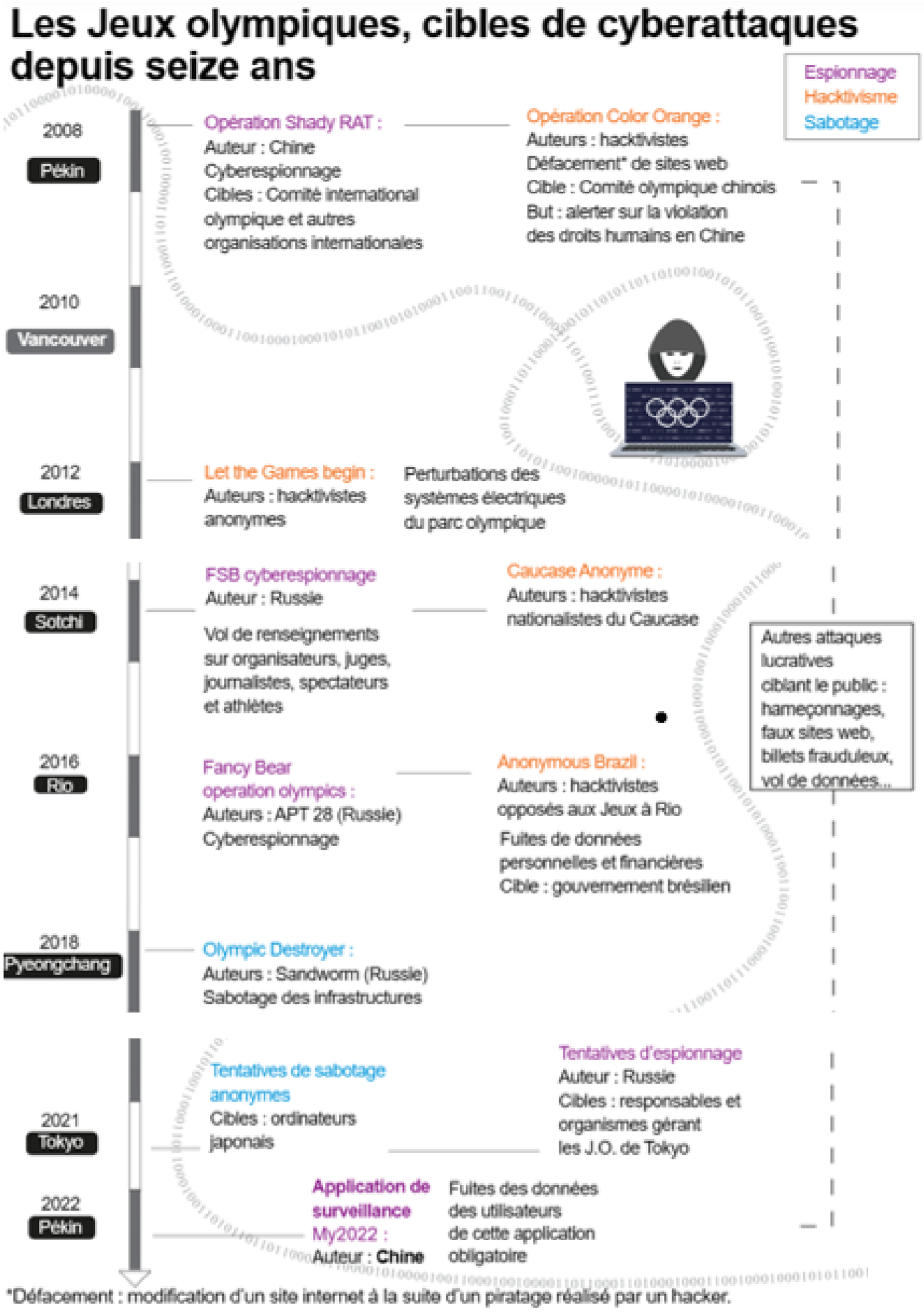
Franz Regul (directeur de la cybersécurité de Paris 2024) à gauche aux côtés d'Éric Greffier (directeur des affaires et de la technologie chez Cisco) réunis en plateau lors de l'événement Champions en Scène organisé à la Seine Musicale lundi 25 septembre 2023.
Des plans de sécurisation de voirie des JO Paris 2024 dérobés (MAJ) (lemondeinformatique.fr)

LES JEUX OLYMPIQUES DE PARIS 2024 : UN DÉFI DE CYBERSÉCURITÉ MONDIAL

A Paris, le Comité d'Organisation des Jeux Olympiques (Cojo) identifie trois grandes menaces :

- La mise en danger des personnes. Par exemple, un mouvement de foule dans un stade dont un pirate informatique aurait réussi à éteindre les lumières.
- Les activistes représentent un risque majeur aussi, menaçant l'image et les revenus de l'événement ainsi que ceux de la France, en raison de leur capacité technique et de leur intérêt pour cet événement mondial.
- Le risque de sabotage des opérations. Concrètement, cela pourrait prendre la forme d'une perturbation des retransmissions des épreuves olympiques en direct par exemple.

L'ANSSI alerte aussi sur les **menaces étatiques** qui pèsent sur la France, surtout dans le contexte géopolitique actuel. En effet, des hackeurs en provenance de Russie ont déjà été à l'origine de cyberattaques lors de précédentes éditions des jeux-olympiques.



Les jeux olympiques, cibles de cyberattaques depuis seize ans. JO 2024. « La menace cyber va être multipliée par dix » : comment les organisateurs s'y préparent (ouest-france.fr)

Cisco a mis en place la stratégie *zero trust* qui repose sur le principe de ne faire confiance à aucun utilisateur ou appareil, même s'ils se trouvent à l'intérieur du réseau. Pour ce faire, Cisco met en place un contrôle d'accès réseau qui vérifie l'identité et les autorisations des utilisateurs chaque fois qu'ils tentent d'accéder aux applications des JO.

Cette approche permet de segmenter les droits d'accès en fonction des accréditations et des usages spécifiques de chaque utilisateur, assurant ainsi que seules les personnes légitimes ont accès aux applications pour lesquelles elles sont autorisées. En utilisant des systèmes d'analyse et de détection alimentés par l'intelligence artificielle, Cisco peut détecter les comportements suspects, circonscrire les attaques et garantir la sécurité du réseau.

Perspectives et Défis

Toutes ces mesures et protections ont évidemment un coût, qui avait été sous-évalué au départ. Effectivement, sur les 400 millions d'euros de rallonge budgétaire votés l'an dernier, 10 millions concernaient la cybersécurité. Au total ce sont 17 millions d'euros qui sont consacrés à la défense cyber.

La Cour des comptes, quant à elle, exprime des préoccupations quant à la sécurité informatique des Jeux Olympiques de Paris 2024. Bien qu'elle reconnaisse les efforts accrus en matière de sécurité, elle soulève des inquiétudes concernant le système informatique déployé, notant qu'il doit encore être amélioré et sécurisé pour faire face aux menaces de cybercriminalité. De plus, elle émet des réserves quant à la confidentialité des données, notamment celles qui pourraient être confiées à des prestataires comme le groupe chinois Alibaba.

Les JO 2024 apparaissent dès lors comme un défi majeur de sécurité reposant entre les mains françaises, une occasion de démontrer l'efficacité cyber de l'hexagone, et d'en repousser les limites.

SOURCES

- “Cybersécurité : les JO de Paris 2024 sortent le grand jeu”, *Goron*, 19/10/21, Cybersécurité : les JO de Paris 2024 sortent le grand jeu - RNM+S (goron.fr)
- “Cybersécurité : comment les Jeux Olympiques de Paris 2024 se préparent”, Mathieu Pollet, *l’Usine Digitale*, 21/10/22, Cybersécurité : comment les Jeux Olympiques de Paris 2024 se préparent (usine-digitale.fr)
- “Des plans de sécurisation de voirie des JO Paris 2024 dérobés (MAJ)”, Dominique Filippone, *le Monde Informatique*, 28/02/24, Des plans de sécurisation de voirie des JO Paris 2024 dérobés (MAJ) (lemondeinformatique.fr)
- “JO 2024. « La menace cyber va être multipliée par dix » : comment les organisateurs s’y préparent”, Marion Dubois, *Ouest-France*, 17/12/2023, JO 2024. « La menace cyber va être multipliée par dix » : comment les organisateurs s’y préparent (ouest-france.fr)
- “Cybersécurité des JO de Paris 2024 : un défi collectif”, Fabrice Deblock, *INCYBER News*, 25/10/23, Cybersécurité des JO de Paris 2024 : un défi collectif (incyber.org)
- “Cyberattaques pendant les JO 2024 : pourquoi les experts paniquent ?”, Elina S., *le big data*, 25/01/24, Les JO 2024 sous la menace des cyberattaques (lebigdata.fr)
- “Cybersécurité des JO de Paris 2024 : « Il y a une vraie mobilisation, et nous sommes dans les temps »”, Martin Untersinger, *Le Monde*, 06/07/23, Cybersécurité des JO de Paris 2024 : « Il y a une vraie mobilisation, et nous sommes dans les temps » (lemonde.fr)
- “Paris 2024 : le chantier colossal de la cybersécurité pour découvrir d'éventuelles failles permettant à "un hacker de s'infiltrer"”, Emma Sarango, *France Info*, 25/04/2023, Paris 2024 : le chantier colossal de la cybersécurité pour découvrir d'éventuelles failles permettant à "un hacker de s'infiltrer" (francetvinfo.fr)
- “Jeux olympiques et paralympiques de Paris 2024 : l'ANSSI dans les starting-blocks”, ANSSI, 17/04/23, Jeux olympiques et paralympiques de Paris 2024 : l'ANSSI dans les starting-blocks | ANSSI (cyber.gouv.fr)
- “Cybersécurité : quelle stratégie pour les JO de Paris 2024 ?”, Maxence Fabrion, Less Numériques, 26/10/22, Cybersécurité : quelle stratégie pour les JO de Paris 2024 ? - Les Numériques (lesnumeriques.com)

SUIVEZ DEF'INSEEC SUR

DEFINSEEC.COM DEFINSEEC@GMAIL.COM 07 83 51 70 94