

# Cybersécurité et Cyberdéfense : leviers de l'intelligence économique

|   |   |
|---|---|
| x | La transition numérique en<br>Afrique étroitement liée à<br>l'intelligence économique |
|---|---|

---

**La numérisation de la société africaine s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu continental. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'Etat, les acteurs économiques et les citoyens. La cybercriminalité, l'espionnage, la propagande, le sabotage ou l'exploitation excessive de données personnelles menacent la confiance et la sécurité dans le numérique et appellent une réponse collective.**

Le second pilier de l'intelligence économique est par définition la sécurité du patrimoine immatériel. Composante indispensable au développement. Le problème est que ce patrimoine est de plus en plus numérisé en Afrique comme partout dans le monde. A cela il faut rajouter le fait que la technologie est injectée à forte dose dans les entreprises pour améliorer la croissance et la compétitivité. Il y va de même pour les Etats.

Dans ce contexte, l'utilisation, l'accès et l'exploitation de la technologie est en forte croissance. Ce qui a pour implication d'exposer les données stratégiques. Il faut alors disposer de mécanismes efficaces pour protéger ce patrimoine. « La cybersécurité est la prévention des risques de sécurité et de sûreté liés à l'emploi des technologies de l'information. Elle est à ce titre un volet de « l'intelligence des risques » elle-même composante de l'intelligence économique. » Bernard Besson.

De nouveaux crimes, risques, infractions et menaces sont apparus dans le cyberspace africain : utilisations criminelles d'internet (cybercriminalité), espionnage politique, économique et industrielle, attaques contre les infrastructures critiques de la finance, des transports, de l'énergie et des communications à des fins de spéculation, de sabotage et de terrorisme.

Émanant de groupes étatiques ou non-étatiques, les cyberattaques n'ont aucune contrainte de distances, de frontières et même d'espaces ; peuvent être complètement anonymes ; ne nécessitent plus de coûts et de moyens importants et peuvent présenter de très faibles risques pour l'attaquant...[lire la suite]

---

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur  
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : **Cybersécurité et Cyberdéfense : leviers de l'intelligence économique. »**