

Intelligence de la guerre. Renseignement, cyberdéfense, influence



Lundi 24 février
18h00 - 20h00

Par webinaire Zoom



Les guerres d'Ukraine Cybersécurité, Renseignement, Intelligence, économique



Bernard BESSON

Directeur scientifique
du
Comité intelligence économique
des ingénieurs et scientifiques
de France (IESF)

Organisateurs



Pr Ahmed Mehaoua



Béatrice Laurent



Gérard Peliks

Le conflit Ukrainien et la cybersécurité



La cyberguerre et la cybersécurité sont aujourd'hui au centre de toutes les batailles. A la lutte informatique offensive et défensive s'ajoute la lutte informatique d'influence.

L'interception du signal, le brouillage des fréquences, les drones volant en essaims, ou pilotés par fibre optique dont l'IA désigne les cibles, les missiles hypervéloces et très précis des forces balistiques russes, le renseignement humain et électronique, ajoutés aux mercenaires du cyberspace, mafias, proxies ou armée régulière, menacent les souverainetés des Etats.

Entre la dissuasion nucléaire et la dissuasion conventionnelle, la cyberguerre peut devenir cataclysmique. La dissuasion informatique est tout aussi terrifiante.

Au Lundi de la Cybersécurité de février, l'intervenant nous parlera de cette tragédie et en dressera le bilan.

Je donne la plume à l'intervenant Bernard BESSON

La cybersécurité est au cœur du champ de bataille, au cœur des systèmes financiers de la guerre économique. Elle soutient les actions du renseignement humain et électronique. Tous les belligérants cherchent à renforcer leur souveraineté numérique face à l'adversaire.

Les hommes et les femmes de la cybersécurité dont le statut mérite une considération accrue, sont sollicités nuit et jour sur les conséquences militaires, sociales et psychologiques de cette guerre. Comme tout conflit celle-ci innove.

Le 24 février 2025 sera le troisième anniversaire d'un affrontement effroyable qui peut briser l'Union européenne car les choses tournent mal. Le Lundi de la Cybersécurité sera l'occasion d'un bilan. Pourquoi ce conflit ? Quels en sont les véritables ressorts, les aspects cachés ou négligés de cette tragédie ?



Je reprends la plume

Qui est Bernard BESSON ?



Bernard Besson, dirigeant chez Bernard Besson Consulting, ancien chef de cabinet aux RG puis à la DST au moment de la chute de l'URSS a été l'adjoint de M Alain Juillet, Haut responsable à l'intelligence économique.

Il est aujourd'hui directeur scientifique du Comité Intelligence Economique et stratégique des Ingénieurs et scientifiques de France (IESF). Il est l'auteur de plusieurs ouvrages, essais et fictions ayant trait à l'intelligence économique **et** de thrillers sur les risques et les enjeux géopolitiques de notre époque.

Sur le premier affrontement balistique entre la Russie et les Etats-Unis il est l'auteur d'une tétralogie sur les événements de l'époque. : **1961 1962 1963 1964** Ceux-ci ressemblent à ceux d'aujourd'hui. Le lecteur intéressé pourra se plonger dans les arcanes du renseignement de l'époque suivant les aventures d'Otto Heinner et de Sabine Racinet, une femme exceptionnelle, un couple d'espions hors pair inspiré de la réalité car *la fiction est un mensonge qui dit la vérité*.

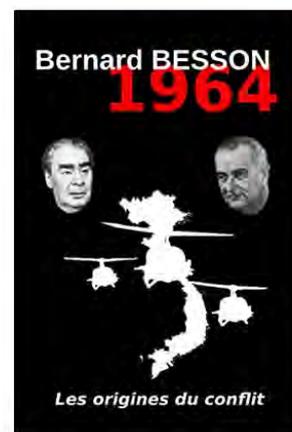
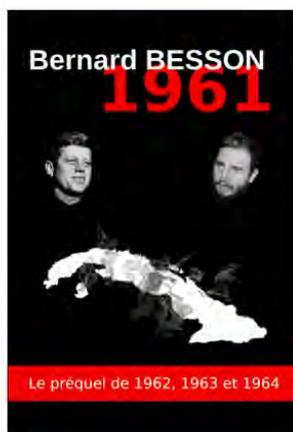


Pour plus de renseignements, voir en : https://fr.wikipedia.org/wiki/Bernard_Besson

Tétralogie de la guerre froide: Politique et Renseignement

Odile Jacob- Amazon Kindle

Bernard Besson Directeur scientifique du Comité intelligence économique des ingénieurs et scientifiques de France (IESF)



Demande d'inscription pour le Lundi de la cybersécurité du mois de février 2025

Lundi 24 février, par visio-conférence Zoom à partir de 18 h 00.



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien vers la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à Béatrice Laurent :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@arcsi.fr).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 24 février, dès 18 h 00**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00**.

Quelques minutes avec Myriam Quéméner

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Cette séquence du Lundi de février sera animée par **Myriam QUEMENER**,



Myriam Quéméner est magistrate, docteure en droit, et experte en matière de lutte contre la cybercriminalité pour le Conseil de l'Europe, la chancellerie et l'École nationale de la Magistrature. Elle participe à de nombreux travaux interministériels et parlementaires.

Elle est l'auteur de plusieurs ouvrages sur la cybercriminalité et la cybersécurité, dont *Hacker « éthique » et cybersécurité* - 26 novembre 2024.

Myriam Quéméner fera un focus sur les nouvelles législations et un commentaire sur l'organisation de la justice (projet de parquet éco fi etc...)



Les hackers sont souvent perçus comme de redoutables pirates informatiques.

Mais au-delà des délinquants, se cachent les hackers « éthiques » qui détectent les failles des logiciels et des sites web.

Ce livre est co-écrit avec Amélie Köcke (EY).

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez tous les détails, slides, parfois aussi les enregistrements et des comptes rendus, écrits par Clarisse Véron, cette année élève du master2 « Cybersécurité et e-Santé » de l'université Paris Cité, sur le web de l'ARCSI en https://www.arcsi.fr/evt_passes.php.

Par exemple, pour le Lundi de la Cybersécurité du mois de décembre 2024 :

La lettre d'invitation est [disponible ici](#).

Les slides de la présentation de Thomas ARGHERIA sont [disponibles ici](#).

Les slides de la présentation du CyberCercle sont [disponibles ici](#).

Le compte-rendu est [disponible ici](#).

La rediffusion est [disponible ici](#).

Mais attention, il n'est pas garanti qu'il y aura ces documents pour chacun de nos futurs lundis. Donc il est conseillé d'être connectés pour les suivre par Zoom.

Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?
Prompt posé à Gemini (l'IA Générative de Google) :

Quelle est la place de la cyberguerre dans le conflit ukrainien ?

La cyberguerre joue un rôle de plus en plus important et complexe dans le conflit ukrainien. Elle est devenue une composante essentielle des opérations militaires, aux côtés des actions sur le terrain.

Pourquoi la cyberguerre est-elle si importante dans ce conflit ?

- **Une guerre hybride** : Le conflit en Ukraine est souvent qualifié de "guerre hybride", mêlant actions militaires conventionnelles et actions dans le cyberspace. La cyberguerre permet de mener des attaques à distance, de perturber les communications, de désinformer et de saper le moral des populations.
- **Un champ de bataille parallèle** : Le cyberspace est devenu un véritable champ de bataille où se confrontent les forces armées russes et ukrainiennes, ainsi que des acteurs non étatiques.
- **Des enjeux stratégiques** : La maîtrise du cyberspace permet d'obtenir un avantage stratégique significatif. En attaquant les infrastructures critiques, en perturbant les communications ou en diffusant de la propagande, les acteurs peuvent influencer le cours du conflit.

Quelles sont les principales formes de cyberattaques observées ?

- **Les attaques par déni de service (DDoS)** : Ces attaques visent à rendre inaccessibles des sites web ou des services en ligne en saturant les serveurs de requêtes.
- **Les attaques par rançongiciels** : Les attaquants chiffrent les données des victimes et exigent une rançon pour les déchiffrer.
- **La désinformation et la propagande** : La diffusion de fausses informations sur les réseaux sociaux est utilisée pour manipuler l'opinion publique et semer la confusion.
- **Les cyber espionnage** : Les acteurs étatiques et non étatiques cherchent à voler des informations sensibles pour obtenir un avantage stratégique.

Quelles sont les conséquences de ces cyberattaques ?

- **Des perturbations des services essentiels** : Les cyberattaques peuvent paralyser des infrastructures critiques comme les réseaux électriques, les hôpitaux ou les transports.
- **Des pertes financières importantes** : Les entreprises et les organisations peuvent subir des pertes financières considérables en raison des cyberattaques.
- **Une érosion de la confiance** : La multiplication des cyberattaques érode la confiance des citoyens dans les institutions et les technologies numériques.
- **Une escalade du conflit** : Les cyberattaques peuvent conduire à une escalade du conflit et à des représailles.

Quels sont les enjeux pour l'avenir ?

- **Une course à l'armement cybernétique** : La cyberguerre est en constante évolution, et les États investissent massivement dans le développement de nouvelles capacités offensives et défensives.
- **La nécessité d'une coopération internationale** : La cybercriminalité ne connaît pas de frontières, et la coopération internationale est essentielle pour lutter contre les menaces communes.
- **Le renforcement de la résilience numérique** : Les organisations et les États doivent renforcer leur résilience numérique pour mieux faire face aux cyberattaques.

En conclusion, la cyberguerre est devenue un élément incontournable des conflits modernes. Le conflit en Ukraine illustre parfaitement l'importance de cette nouvelle dimension de la guerre. Pour faire face à ces défis, il est nécessaire de développer de nouvelles stratégies et de renforcer la coopération internationale.

Bon, intéressant, mais qu'en pensent Bernard BESSON et Myriam QUEMENER ? Ils nous en diront plus le 24 février et répondront à nos questions, et nous en discuterons..

Gérard Peliks