ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité »
Lundi 24 Février 2025

Intelligence économique des guerres d'Ukraine
Cybersécurité et renseignement

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 2 Cybersécurité et E-santé

SOMMAIRE

Introduction

Le **Lundi de la Cybersécurité** du 24 février 2025 s'est inscrit dans un contexte géopolitique particulièrement sensible, marquant le troisième anniversaire du conflit en Ukraine. Organisée par l'Université Paris Cité, cette session a rassemblé des experts en intelligence économique, en cybersécurité et en droit du numérique afin d'examiner les conséquences stratégiques et réglementaires de la guerre économique et numérique actuelle.

Deux experts reconnus sont intervenus pour apporter leurs analyses et éclairages sur ces problématiques :

- **Bernard Besson** : Ancien chef de cabinet aux Renseignements Généraux (RG) puis à la Direction de la Surveillance du Territoire (DST), il a ensuite occupé le poste d'adjoint du Haut Responsable à l'Intelligence Économique, **Alain Juillet**. Il est aujourd'hui **directeur scientifique du Comité Intelligence Économique et Stratégique des Ingénieurs et Scientifiques de France (IESF)** et auteur de plusieurs ouvrages et MOOC sur l'intelligence économique. Son intervention s'est concentrée sur **l'impact de la cybersécurité dans les conflits modernes**, notamment dans la guerre en Ukraine, et les enjeux de **souveraineté numérique et de guerre économique**.

- **Myriam Quéméner** : Magistrate et docteure en droit, elle est une spécialiste reconnue du **droit du numérique et de la cybercriminalité**. Son intervention a porté sur **les évolutions réglementaires en cybersécurité**, avec un accent particulier sur les nouvelles directives européennes comme **NIS 2, DORA et l'IA Act**, qui renforcent les obligations des entreprises et les protections des citoyens face aux cybermenaces.

La conférence a débuté par l'intervention de **Bernard Besson**, qui a dressé un tableau des nouvelles dynamiques de la guerre économique et des défis posés par la cybersécurité dans les conflits contemporains.

I. L'intelligence économique et conflits modernes

Lors de son intervention, **Monsieur Bernard Besson** a mis en évidence le rôle central de l'intelligence économique dans les conflits contemporains. Selon lui, la guerre ne se limite plus aux champs de bataille traditionnels, mais s'étend désormais aux sphères numériques et économiques, où les nations et les entreprises s'affrontent pour protéger leurs intérêts stratégiques. Il a insisté sur le fait que la **cybersécurité et le renseignement économique sont devenus des armes essentielles** dans la guerre économique qui se joue à l'échelle mondiale.

Monsieur Besson a souligné que **l'intelligence économique repose sur la collecte, l'analyse et l'exploitation d'informations stratégiques** permettant d'anticiper les menaces et de saisir des opportunités. Il a rappelé que, dans un conflit comme celui de l'Ukraine, **les États et les entreprises doivent surveiller et protéger leurs infrastructures critiques**, car celles-ci deviennent des cibles privilégiées des adversaires.

Il a expliqué que la guerre moderne se joue autant dans les coulisses du pouvoir que sur le terrain. Ainsi, **le renseignement économique est utilisé pour influencer les décisions stratégiques, affaiblir des concurrents et manipuler les marchés financiers**. Il a notamment évoqué l'utilisation de la désinformation et du cyberespionnage comme des **méthodes privilégiées pour déstabiliser les économies ennemies**.

Selon Monsieur Besson, la guerre économique ne se limite pas aux sanctions et aux embargos ; elle passe aussi par **le sabotage numérique, le cyberespionnage et la manipulation des marchés financiers**. Il a mentionné plusieurs exemples de cyberattaques ayant eu un impact majeur, notamment **les attaques contre les infrastructures énergétiques ukrainiennes**, qui ont démontré la capacité d'un État à plonger une nation dans le chaos sans tir de missile.

Il a insisté sur le fait que **les grandes puissances économiques ne se contentent plus de se concurrencer par l'innovation et le commerce** ; elles utilisent également des moyens offensifs en cybersécurité pour affaiblir leurs adversaires. Les attaques contre les entreprises, les banques et les réseaux de télécommunication font partie d'une stratégie globale où **le contrôle de l'information est aussi important que la possession de ressources matérielles**.

Monsieur Besson a particulièrement mis en avant **l'importance de la guerre de l'information dans les conflits modernes**. Il a affirmé que **la désinformation est devenue une arme aussi puissante que les cyberattaques**, car elle permet d'influencer l'opinion publique, de semer le doute et de diviser les sociétés.

Il a évoqué **les campagnes de désinformation orchestrées via les réseaux sociaux**, notamment en Russie et en Chine, qui visent à affaiblir les démocraties occidentales en manipulant l'information et en accentuant la polarisation des débats. Il a également rappelé que **les États comme les entreprises doivent désormais intégrer la lutte contre la désinformation dans leur stratégie de cybersécurité**, car une attaque sur la réputation ou la confiance peut être tout aussi dévastatrice qu'une attaque technique.
Enfin, Monsieur Besson a insisté sur la nécessité pour l'Europe et la France de **renforcer leur souveraineté numérique**. Il a mis en garde contre **la dépendance excessive aux infrastructures technologiques étrangères**, notamment aux grandes plateformes américaines et chinoises.

Il a évoqué plusieurs pistes pour **réduire cette vulnérabilité**, notamment le développement de **clouds souverains, de systèmes de chiffrement nationaux et d'une autonomie stratégique dans le domaine des télécommunications et de l'intelligence artificielle**.
Il a conclu en rappelant que **la cybersécurité et l'intelligence économique sont désormais indissociables des enjeux de puissance et de souveraineté**.

Selon lui, **les États qui ne prendront pas conscience de cette nouvelle réalité risquent de perdre leur influence sur la scène internationale**, non pas à cause de leur faiblesse militaire, mais à cause de leur vulnérabilité numérique et économique.

II. La souveraineté numérique, un enjeu majeur du XXIe siècle

Lors de son intervention, **Monsieur Bernard Besson** a souligné que la souveraineté numérique est devenue un **enjeu stratégique crucial** pour les nations et les entreprises du XXIe siècle. Il a expliqué que dans un monde où les **données, les infrastructures numériques et l'intelligence artificielle** jouent un rôle central, les États qui ne maîtrisent pas leur écosystème numérique risquent de **perdre leur autonomie et leur influence géopolitique**.

Monsieur Besson a mis en évidence **l'émergence de blocs numériques opposés**, où la **cyberpuissance se mesure désormais à la capacité d'un État à protéger et contrôler son infrastructure numérique**. Il a rappelé que les grandes puissances, comme les **États-Unis, la Chine et la Russie**, ont compris très tôt l'importance de la **maîtrise des réseaux, des algorithmes et des infrastructures cloud** pour **consolider leur domination économique et stratégique**.

Il a expliqué que l'Europe, bien que dotée d'un **fort potentiel technologique**, reste largement dépendante des **géants américains du numérique (GAFAM)** et des infrastructures chinoises émergentes. Cette situation pose un problème majeur :

- **Dépendance aux plateformes étrangères** : la majorité des données sensibles européennes transitent par des serveurs américains ou chinois.
- **Surveillance et contrôle des flux numériques** : les États-Unis et la Chine ont mis en place des dispositifs de surveillance leur permettant d'exploiter les informations économiques et stratégiques des autres nations.
- **Risque de sanctions technologiques** : comme le montre le cas de la guerre commerciale entre les États-Unis et la Chine, **la privation d'accès à des technologies clés** (semi-conducteurs, 5G, cloud) peut paralyser un État ou une industrie.

Monsieur Besson a alerté sur le fait que **cette nouvelle guerre des blocs numériques ne se joue pas uniquement entre États, mais aussi entre entreprises multinationales**. Il a cité l'exemple des grandes firmes technologiques qui, par leur puissance financière et leur contrôle des infrastructures, influencent directement les décisions politiques des États.

Pour **assurer leur souveraineté**, Monsieur Besson a insisté sur la nécessité pour les États de **reprendre le contrôle de leurs infrastructures numériques**. Il a notamment évoqué plusieurs secteurs stratégiques :

- **Le cloud computing et les data centers** : l'hébergement des données critiques doit être sécurisé et localisé sur le territoire national pour éviter tout risque de surveillance étrangère. Il a mentionné l'initiative de **cloud souverain européen (Gaia-X)** comme une réponse à cette problématique.
- **Les réseaux de communication (5G, fibre optique, satellites)** : les tensions autour du déploiement de la 5G montrent que **le choix des fournisseurs technologiques impacte directement la souveraineté d'un pays**.
- **La cybersécurité des infrastructures vitales** : les hôpitaux, les banques, les transports et les réseaux énergétiques sont des cibles privilégiées des cyberattaques. Monsieur Besson a rappelé que **le sabotage numérique peut avoir des conséquences aussi graves qu'une attaque militaire**.

Il a cité l'exemple de l'attaque contre **Colonial Pipeline aux États-Unis**, où un ransomware a provoqué une **pénurie de carburant sur la côte Est**, illustrant ainsi la vulnérabilité des infrastructures critiques face aux cybermenaces.

Monsieur Besson a insisté sur **l'urgence pour l'Europe de renforcer son indépendance numérique**. Il a reconnu que l'Union européenne a pris conscience de ces enjeux en **développant un cadre**

réglementaire plus strict, notamment avec la directive **NIS 2** et le règlement **DORA**, qui imposent des mesures de cybersécurité renforcées aux entreprises et aux institutions.

Cependant, il a souligné plusieurs défis majeurs :

- **Le retard technologique** : l'Europe ne possède pas encore d'alternatives solides aux GAFAM et aux grandes entreprises chinoises dans des domaines clés comme l'intelligence artificielle et les semi-conducteurs.
- **Le manque d'investissement dans l'innovation** : les start-ups européennes peinent à rivaliser avec les géants américains et asiatiques, faute de financements suffisants.
- **L'absence d'une vision stratégique unifiée** : les pays européens ont des approches différentes en matière de cybersécurité et d'intelligence économique, ce qui nuit à la construction d'un véritable pôle de puissance numérique.

Monsieur Besson a averti que **si l'Europe ne développe pas rapidement ses propres infrastructures numériques souveraines, elle continuera à être dépendante des puissances étrangères**, avec le risque de se voir imposer des règles qu'elle ne maîtrise pas.

Pour conclure, Monsieur Besson a proposé plusieurs pistes pour **renforcer la souveraineté numérique des États et des entreprises** :

- **Développer un écosystème numérique souverain** : encourager l'émergence de **champions européens du numérique**, capables de concurrencer les GAFAM.
- **Favoriser l'adoption de solutions de cybersécurité locales** : utiliser des technologies développées en Europe plutôt que des solutions étrangères.
- **Créer une agence européenne de cybersécurité** avec des **capacités offensives et défensives** pour protéger les infrastructures stratégiques contre les cyberattaques.
- **Renforcer la formation en cybersécurité et en intelligence économique** : sensibiliser les décideurs et les entreprises aux enjeux de la souveraineté numérique.

Il a conclu en affirmant que **l'avenir des nations ne dépendra plus seulement de leur puissance militaire ou économique, mais aussi de leur capacité à contrôler et sécuriser leur environnement numérique**. Selon lui, **les États qui échoueront à assurer leur souveraineté numérique deviendront des acteurs secondaires dans le nouvel ordre mondial**.

III. Technologies et guerre moderne : Drones, IA et cyberattaques

Lors de son intervention, **Monsieur Bernard Besson** a souligné que la guerre moderne ne se limite plus aux confrontations physiques traditionnelles. Il a insisté sur le fait que **les nouvelles technologies, notamment les drones, l'intelligence artificielle et les cyberattaques, sont devenues des armes redoutables** qui redéfinissent les conflits contemporains. Il a évoqué l'évolution rapide de ces outils et les risques qu'ils posent, non seulement pour les États mais aussi pour les entreprises et les citoyens.

Monsieur Besson a expliqué que **les drones sont devenus des éléments centraux dans les stratégies militaires modernes**. Il a rappelé que ces appareils autonomes, initialement utilisés pour la surveillance, sont désormais capables de mener des attaques de haute précision et de **remplacer des soldats sur le champ de bataille**.

Il a pris l'exemple de la guerre en Ukraine, où les drones ont joué un rôle déterminant en permettant :

- **L'attaque de cibles stratégiques** : certaines frappes ciblées ont réussi à **détruire des infrastructures militaires et logistiques** sans engager de troupes au sol.
- **La surveillance en temps réel** : les drones fournissent des images détaillées des positions ennemies, **rendant les opérations militaires plus précises et plus efficaces**.
- **Leur accessibilité à des groupes non étatiques** : certains drones commerciaux, modifiés et armés, sont désormais utilisés par des groupes terroristes ou des milices, ce qui accentue les risques d'instabilité mondiale.

Monsieur Besson a averti que **la miniaturisation et l'autonomie croissante des drones posent un défi majeur**. Il a notamment évoqué la **possibilité de "nuées de drones"**, une technique où plusieurs drones agissent en coordination pour saturer les défenses ennemies. Selon lui, **ces nouvelles tactiques annoncent une transformation profonde des guerres futures**, où les combats seront **moins humains mais plus automatisés**.

Monsieur Besson a insisté sur **l'essor de l'intelligence artificielle dans les stratégies de défense**. Il a expliqué que **l'IA permet d'accélérer la prise de décision sur le champ de bataille**, en analysant des volumes massifs de données en temps réel et en proposant des scénarios d'action.

Il a cité plusieurs domaines où l'IA joue un rôle clé :

- **La reconnaissance faciale et l'identification des cibles** : certains systèmes militaires sont capables de repérer des ennemis à distance avec une précision inédite.
- **L'automatisation des drones et des véhicules militaires** : de nombreux pays investissent dans des armes autonomes qui **peuvent agir sans intervention humaine**.
- **La cyberdéfense proactive** : l'IA est utilisée pour **détecter et neutraliser** des cyberattaques avant qu'elles ne causent des dommages.

Toutefois, Monsieur Besson a mis en garde contre **les dérives potentielles de ces technologies**. Il a notamment évoqué :

- **Les risques éthiques liés aux armes autonomes** : la question de savoir **qui est responsable en cas d'erreur fatale** reste un débat crucial.
- **La possibilité de manipuler l'IA pour des campagnes de désinformation massives** : certaines IA peuvent générer de **fausses vidéos et des deepfakes**, créant ainsi **des crises diplomatiques artificielles**.
- **La dépendance croissante aux algorithmes** : si des États ou des armées deviennent trop dépendants de l'IA, ils pourraient être **vulnérables à des attaques ciblées visant ces systèmes**.

Monsieur Besson a conclu en affirmant que **l'IA sera un acteur incontournable des guerres futures**, mais que **sans encadrement strict, elle pourrait également devenir un facteur de chaos**.

Monsieur Besson a insisté sur le fait que **les cyberattaques sont aujourd'hui l'un des moyens les plus efficaces pour affaiblir un adversaire**. Il a rappelé que **les conflits modernes ne se gagnent plus uniquement sur les champs de bataille**, mais aussi dans le cyberespace, où des attaques informatiques peuvent **paralyser des pays entiers** sans qu'aucun missile ne soit tiré.

Il a illustré cette réalité avec plusieurs exemples :

- **Les attaques contre les infrastructures énergétiques** : il a cité le cas des cyberattaques russes sur le réseau électrique ukrainien, qui ont plongé plusieurs villes dans le noir.
- **Le cyberespionnage industriel et militaire** : de nombreux États utilisent des attaques informatiques pour **voler des secrets technologiques et militaires** à leurs adversaires.
- **Les ransomwares ciblant des administrations et des entreprises stratégiques** : certains groupes de hackers, parfois liés à des États, utilisent des **logiciels malveillants pour bloquer des infrastructures clés** et demander des rançons.

Il a également mis en avant le **rôle croissant des groupes cybercriminels privés**, qui peuvent être **utilisés comme des mercenaires numériques par des gouvernements** souhaitant éviter d'être directement impliqués. Ces groupes utilisent des méthodes avancées comme :

- **Le phishing ciblé** pour infiltrer des réseaux sensibles.
- **Les attaques de type supply chain**, où ils compromettent un fournisseur pour atteindre leur véritable cible.
- **L'utilisation de failles 0-day** pour exploiter des vulnérabilités inconnues avant qu'elles ne soient corrigées.

Monsieur Besson a conclu cette partie en affirmant que **la guerre cybernétique est devenue aussi stratégique que les conflits militaires classiques**. Il a mis en garde contre **l'illusion d'invulnérabilité numérique**, rappelant que **même les États les plus avancés technologiquement restent vulnérables** à des attaques sophistiquées.

IV. Le cadre juridique et les nouvelles régulations européennes en cybersécurité *(Intervention de Myriam Quéméner)*

Lors de son intervention, Madame Myriam Quéméner, magistrate et experte en droit du numérique, a présenté les évolutions récentes du cadre réglementaire européen en matière de cybersécurité. Elle a souligné que face à l'augmentation des cyberattaques et à la dépendance croissante aux infrastructures numériques, l'Union européenne a renforcé ses exigences en matière de protection et de résilience des systèmes informatiques.

Madame Quéméner a rappelé que plusieurs textes législatifs récents visent à mieux protéger les États, les entreprises et les citoyens contre les cybermenaces :

- Directive NIS 2 *(Network and Information Security)* : remplaçant la directive NIS 1, elle étend ses obligations de cybersécurité à un plus grand nombre d'acteurs, incluant désormais des PME et des administrations publiques.

- Règlement DORA *(Digital Operational Resilience Act)* : spécifique au secteur financier, il impose aux banques et aux assurances de renforcer leur capacité de résilience face aux attaques cybernétiques.

- Directive REC *(Résilience des Entités Critiques)* : vise à protéger les infrastructures critiques européennes contre les cybermenaces et les perturbations.

- Règlement MICA *(Markets in Crypto-Assets)* : encadre les cryptoactifs et impose une régulation stricte aux prestataires de services financiers liés aux cryptomonnaies.

- IA Act *(Règlement sur l'Intelligence Artificielle)* : établit un cadre de gouvernance des systèmes d'intelligence artificielle pour éviter les abus, notamment en matière de cybersécurité et de surveillance.

Ces nouvelles régulations imposent aux entreprises et aux organisations publiques des mesures plus strictes :

- Obligation de cybersécurité renforcée : mise en place de politiques de protection des systèmes informatiques et de gestion des incidents.

- Signalement obligatoire des cyberattaques : obligation de déclaration des incidents de cybersécurité sous 24 heures.

- Sanctions accrues en cas de non-conformité : amendes significatives pour les entités ne respectant pas les nouvelles exigences.

Madame Quéméner a également souligné que ces réglementations visent à protéger les consommateurs face aux cybermenaces. Parmi les principales avancées :

- Meilleure protection des données personnelles et financières.

- Renforcement de la lutte contre la fraude en ligne.

- Obligation pour les plateformes numériques de lutter contre la désinformation et les deepfakes.

V. Questions / Réponses

1. Question : Vladimir Poutine est-il véritablement une menace ?

Réponse de Bernard Besson :
Il reconnaît que Vladimir Poutine a violé le droit international en envahissant l'Ukraine, mais insiste sur le contexte historique et sociologique du conflit. Il rappelle que des populations russophones en Ukraine se sentaient persécutées et que la Russie est intervenue en réponse à ces tensions. Il souligne également que les conflits géopolitiques sont souvent motivés par des intérêts stratégiques complexes et non par une simple volonté d'agression soudaine.

2. Question : Pourquoi comparer la crise ukrainienne à la crise des missiles de Cuba ?

Réponse de Bernard Besson :
Il admet que la situation en Ukraine n'incluait pas encore de missiles américains, contrairement à Cuba en 1962, mais souligne que la possibilité que l'Ukraine installe des missiles à proximité de Moscou était perçue comme une menace par la Russie. Poutine a choisi d'intervenir avant que cette éventualité ne se concrétise.

3. Question : L'Union européenne a-t-elle failli dans la gestion du conflit ?

Réponse de Bernard Besson :
Il critique le rôle de l'UE dans le conflit, expliquant que l'Europe aurait dû être capable de trouver une solution diplomatique, notamment en respectant et en faisant appliquer les accords de Minsk. Selon lui, le manque de leadership et de capacité d'action de l'UE l'a rendue spectatrice d'un conflit qui se déroule sur son propre sol.

4. Question : L'envoi de troupes françaises en Ukraine est-il une option viable ?

Réponse de Bernard Besson :
Il met en garde contre les risques d'un engagement militaire direct en Ukraine, qui pourrait entraîner la France dans un affrontement direct avec la Russie. Il souligne également l'incohérence de la situation, où des milliers de jeunes Ukrainiens en âge de se battre restent en Europe, alors que l'armée ukrainienne souffre d'un vieillissement de ses troupes.

5. Question : Quel est l'impact des drones et des nouvelles technologies dans le conflit ?

Réponse de Bernard Besson :
Il insiste sur le rôle crucial des drones dans la guerre moderne et souligne les conséquences humanitaires désastreuses, notamment le nombre croissant d'amputés à cause des explosions. Il évoque également l'impact psychologique des bombardements incessants, comparant les traumatismes subis aux souffrances des soldats de la Première Guerre mondiale.

6. Question : Quelle est la place de la corruption dans l'économie ukrainienne ?

Réponse de Bernard Besson :
Il mentionne les inquiétudes concernant la corruption en Ukraine, expliquant que la moitié de l'aide financière envoyée au pays aurait été détournée. Il ajoute que les États-Unis exigent des garanties en échange de leur soutien, notamment sous forme de concessions sur les terres rares ukrainiennes.

7. Question : L'Europe est-elle en déclin face à la Russie et la Chine ?

Réponse de Bernard Besson :
Il estime que l'Europe est en recul sur le plan technologique et démographique, tandis que la Russie et la Chine forment et produisent davantage d'ingénieurs. Il critique également le manque de flexibilité et d'innovation de l'UE, qui freine son développement par une réglementation trop lourde.

8. Question : La cybersécurité européenne est-elle suffisante pour faire face aux menaces ?

Réponse de Bernard Besson :
Il affirme que l'Europe est trop défensive et manque d'une approche offensive en matière de cybersécurité. Il regrette que l'UE se concentre davantage sur la réglementation que sur le développement technologique, ce qui la rend vulnérable face aux États-Unis et à la Chine.

9. Question : Peut-on espérer une reprise de la souveraineté numérique en Europe ?

Réponse de Bernard Besson :
Il estime que cela nécessiterait une volonté politique forte, comparable à celle qui a permis la construction de la force nucléaire française sous De Gaulle. Selon lui, sans une politique ambitieuse et un engagement dans l'innovation, l'Europe restera technologiquement dépendante des grandes puissances étrangères.

10. Question : Comment l'intelligence artificielle peut-elle être utilisée dans les conflits modernes ?

Réponse de Bernard Besson :
Il explique que l'IA est omniprésente dans la guerre en Ukraine, notamment pour l'analyse des données et la planification stratégique. Il plaide pour une utilisation offensive de l'IA dans la cybersécurité et recommande de confronter plusieurs modèles d'IA (américains, européens, chinois) pour obtenir des analyses variées et éviter les biais cognitifs.