

Guerre économique et souveraineté numérique

Par Christian Harbulot (Directeur de l'Ecole de Guerre Economique)

Réunion Courante du 15/05/2026



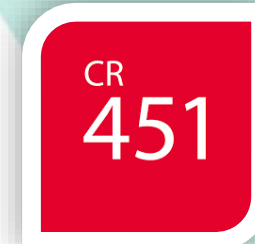
Présentation EGE



ECOLE

***Formations du Bachelor à l'Exe MBA
Formations Online et Certifiantes, BtoB***

*Renseignement, intelligence économique,
influence, risques numériques, analyse
stratégique et guerre de l'information,
management de la cybersécurité*



Centre de Recherche appliquée

www.cr451.fr

Séminaires thématiques

Rapports

Podcasts

Documentaires

Webinaires

Journées d'étude

Guerre économique, guerre de l'information

Définition donnée par le CR451 de l'EGE

La guerre économique est une confrontation entre parties pour capter, contrôler, accaparer des richesses, accroître sa puissance par l'économie.

Rappel à ce propos : l'économiste et historien américain Edward Luttwak déclarait de manière prophétique dans les années 1990 :

« L'économie mondiale, au terme d'un long processus d'unification ou de globalisation favorisé par la pax americana, est en train de se fragmenter à nouveau en blocs économiques concurrents. »

Edward Luttwak, Le Rêve américain en danger, Paris, Odile Jacob, 1995.

Les trois formes de guerre économique

Économie de guerre

Mise sous tutelle d'une partie des entreprises par l'État, dans le cadre d'une planification autoritaire, afin de garantir aux armées les moyens d'une guerre militaire en cours.

Guerre économique du temps de guerre

Opérations offensives visant à parasiter les circuits d'approvisionnement adverses et à affaiblir les capacités de survie de la population ennemie.

Guerre économique du temps de paix

Confrontation pour capter, contrôler, accaparer des richesses et accroître sa puissance ; elle génère un mode de domination qui évite, parce qu'il s'en passe, l'usage de la puissance militaire.

Les champs de confrontation

Champs économiques directs

Concurrence, douane, capital, monnaie, finance, industrie, assurance, notation

Champs institutionnels et régulateurs

Norme, droit, contentieux, diplomatie coercitive, ESG, contentieux climatique

Champs informationnels et cognitifs

Information, cognitif, cyber, renseignement, algorithmique, données

Champs des ressources et flux physiques

Énergie, alimentaire, matières premières critiques, logistique, câbles, spatial, sanitaire

Champs humains et sociétaux

Migratoire, talents, académique, culturel et linguistique, démographique

Champs infrastructurels profonds

Paiements, infrastructures numériques, semi-conducteurs, télécommunications

Enseignements à tirer du colloque

« Guerre économique du temps de paix » (26 octobre 2024)

Le professeur Greg Kennedy (Economic Conflict & Competition Research Group du King's College de Londres) souligne l'importance stratégique du domaine maritime dans la guerre économique actuelle. (Blocus du détroit d'Ormuz... 2026)

Selon lui, le contrôle des voies maritimes constitue un impératif absolu pour la préservation de l'ordre international libéral. ***Il argumente que depuis 250 ans, l'hégémonie économique occidentale repose en grande partie sur sa capacité à assurer une libre circulation des marchandises par les voies maritimes internationales, assurant ainsi prospérité, crédit et stabilité financière.***

Le professeur Kennedy appelle à abandonner l'inertie actuelle au profit d'une stratégie proactive et intégrée, impliquant corporatisme, régulation économique, contrôle des chaînes d'approvisionnement critiques et renforcement du domaine maritime. **Ce changement stratégique s'impose comme une nécessité absolue pour faire face aux nouvelles réalités de la guerre économique contemporaine.**

La mutation des problématiques sécuritaires

L'analyse d'Yves Tiberghien, University of British Columbia (Professor of Political Science) :

Dans ce contexte, **le concept de sécurité économique est hybride.**

Il s'agit de **sécuriser les nœuds clés, les chaînes d'approvisionnement économiques stratégiques et les technologies à double usage potentiel, tout en continuant à fonctionner dans une économie mondialisée et profondément interconnectée.**

Il s'agit d'une **intervention sélectionnée de l'État et d'un débranchement partiel (« clôture ») du marché mondial.**

Il nécessite un dialogue entre experts en sécurité et experts en économie politique et c'est un travail permanent.

La **fragilisation de la dynamique classique de conquêtes de marché** face aux politiques d'accroissement de puissance par l'économie.

L'**importance croissante de la question de la dépendance**.

La **montée en puissance des politiques de sécurité économique** dans les économies clés.

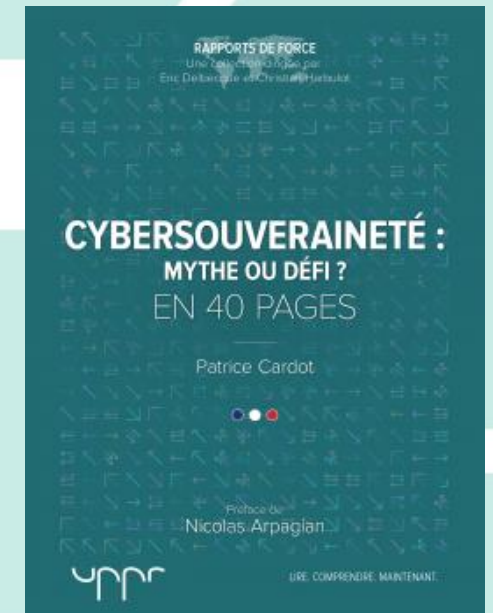
La **limite des mesures de sécurité économique face à la mise en œuvre de politiques offensives d'expansion économique** sur le court/moyen et long terme.

Les **démarches déstabilisatrices des régimes autoritaires** (exemple du chantage sur le commerce mondial à partir du blocage du détroit d'Ormuz) .

Les notions de dépendance technologique, de capture des compétences et d'encerclement cognitif par l'intelligence artificielle sont au cœur de cette guerre économique dans le numérique.

Selon Patrice Cardot, la **dépendance** aux géants du numérique repose sur des mécanismes qui se renforcent mutuellement. Le **verrouillage technologique** (standards fermés, API propriétaires) alimente le **verrouillage cognitif** (habitudes des utilisateurs, formation des équipes), qui lui-même renforce le **verrouillage économique** (coûts de sortie prohibitifs, économies d'échelle écrasantes).

Casser un seul maillon ne suffit pas : il faut une approche systémique, car **ces verrouillages forment un système auto-entretenu où chaque dépendance en crée une autre.**



La dynamique de conquête dans le numérique

Les géants du numérique (GAFAM, BATX) ont une dynamique de conquête fondée sur la création d'une dépendance durable.

Technologiquement, ils contrôlent les infrastructures, les systèmes d'exploitation et les gammes flexibles de composants logiciels.

Économiquement, leurs milliards de profits et leurs économies d'échelle écrasent toute concurrence frontale.

Juridiquement, ils contournent systématiquement les régulations via des montages complexes.

Cognitivement, leur écosystème verrouille les compétences et les habitudes.

Géopolitiquement, leur alliance avec les États-Unis ou avec la Chine leur confère une influence mondiale.

La tentative de réaction européenne

ements à tirer



Les États européens sont en position de faiblesse structurelle, et toute tentative de souveraineté se heurte à cette asymétrie et à la volonté active des GAFAM, mais aussi à terme des BATX, de la maintenir.

Jusqu'à présent, l'Union européenne ne disposait pas d'un référentiel unique permettant d'évaluer le niveau de souveraineté d'une offre cloud.

Présenté le 3 juin 2026, le Cloud and AI Development Act, (CAIDA), vise à être intégré dans le "paquet" sur la souveraineté numérique dont l'objectif est de réduire les dépendances du continent européen aux fournisseurs étrangers de technologies stratégiques, telles que le cloud, l'IA ou encore les semi-conducteurs.

Mais comme le note la presse spécialisée*, « ***l'objectif semble moins d'écarter les grands fournisseurs de services cloud et de cloud computing américains que de mieux encadrer leur présence*** : Google, Amazon et Microsoft pourraient continuer à servir une large partie du marché européen, y compris public, sous certaines conditions ».

* Alice Vitard, Journaliste à L'Usine Digitale

Les menaces générées par l'Intelligence Artificielle

Selon Guy Philippe Goldstein*, **la menace la plus immédiate ne vient pas d'un adversaire extérieur : elle vient de l'intérieur, par l'usage non gouverné de l'outil.**

Aux Etats-Unis, cette menace est nommée la “shadow AI” : plus de $\frac{3}{4}$ des salariés recourent à leurs propres outils d'IA sans en prévenir leur entreprise . Les incidents liés à cette pratique représentent désormais 20 % de l'ensemble des violations, avec un surcoût moyen de 700 000 dollars par rapport aux violations classiques .

Si mal contrôlé, jusqu'à 10 % des données d'une entreprise, y compris les plus sensibles, pourraient être accessibles à tous les employés . Et l'absence de contrôle ne touche pas seulement la confidentialité. Elle affecte la fiabilité même des systèmes. En programmation, presque 85 % des développeurs utilisent déjà l'IA pour coder . Or 45 % du code ainsi généré contient des failles de sécurité — x1,7 à x2,7 fois plus de vulnérabilités selon leurs spécificités que pour du code humain.

* Article « La cybersécurité à l'âge de l'IA : vers la grande accélération », in *Manuel 4 de l'intelligence économique*, PUF, à paraître le 3 septembre 2026.

Pour aller plus loin sur la guerre de l'information



Chaine You Tube du CR451 de l'EGE

Première partie :

<https://www.youtube.com/watch?v=F5MjPsGZ88A>

Pour aborder la culture du combat informationnel



<https://www.youtube.com/watch?v=mD82sTLKiwy>

Deux hommes, deux mondes que tout opposait. L'un avait appris à subvertir l'ordre établi, l'autre à le servir. Aujourd'hui, ils mènent le même combat.

Christian Harbulot, fondateur de l'École de guerre économique, et le général **Jean-Claude Gallet** se sont rencontrés là où nul ne les attendait : sur le front d'une guerre qui ne se déclare plus, mais qui se livre sans relâche dans le champ économique et informationnel.

De la **culture militante de l'action clandestine** à la **culture militaire du renseignement et du commandement**, cet entretien raconte la convergence de deux trajectoires, et la fusion de deux cultures antagoniques.

Le choix de la défense des intérêts de la France dans une période où elle est fragilisée est la condition de cette alliance hors du commun. Guerre de l'information, guerre cognitive, guerre économique : sur ces terrains sans front ni uniforme, la France demeure exposée faute d'une capacité d'action structurée. C'est pourquoi la complémentarité de ces deux hommes dessine **une nouvelle forme de culture du combat informationnel** dans la guerre économique.