INSTITUT CHOISEUL

Briefings Choiseul

Décembre 2025

Menaces hybrides et résilience stratégique : bâtir une souveraineté d'entreprise

CHOISEUL | Souveraineté

Les Briefings de l’Institut Choiseul

Conçus comme des synthèses de nos rencontres, les Briefings Choiseul sont des documents stratégiques courts et percutants. Ils sont assortis de recommandations opérationnelles et rapidement mobilisables sur des thématiques économiques d’avenir. En explorant des secteurs variés — défense, innovation, industrie, agroalimentaire, énergie, enjeux macroéconomiques ou de filière — l’Institut Choiseul croise les regards d’acteurs économiques prescripteurs et de praticiens. Ces points de vue nourrissent des analyses ancrées dans la réalité du terrain.

Chaque Briefing dresse un état des lieux clair, met en lumière les principaux enjeux et propose des pistes d’action concrètes. Leur objectif : interpeller et appeler à l’action les décideurs, parties prenantes et le grand public.

La 22ème Rencontre Souveraineté & Menaces Hybrides s’est tenue le 22 octobre 2025 autour d’acteurs de premier plan qui ont partagé leur témoignage, visions stratégiques et bonnes pratiques : Mme Fadila Leturcq, Directrice du Campus du Numérique Public, Mme Marjorie Bordes, CISO chez Capgemini, Frédéric Fauchère, Directeur de la Division Mobile de Samsung Electronics France, Patrick Guyonneau, Directeur de la Sécurité chez Orange, et Florent Kirschner, directeur du pôle souveraineté numérique au Secrétariat Général pour l’Investissement.

Sommaire

Introduction

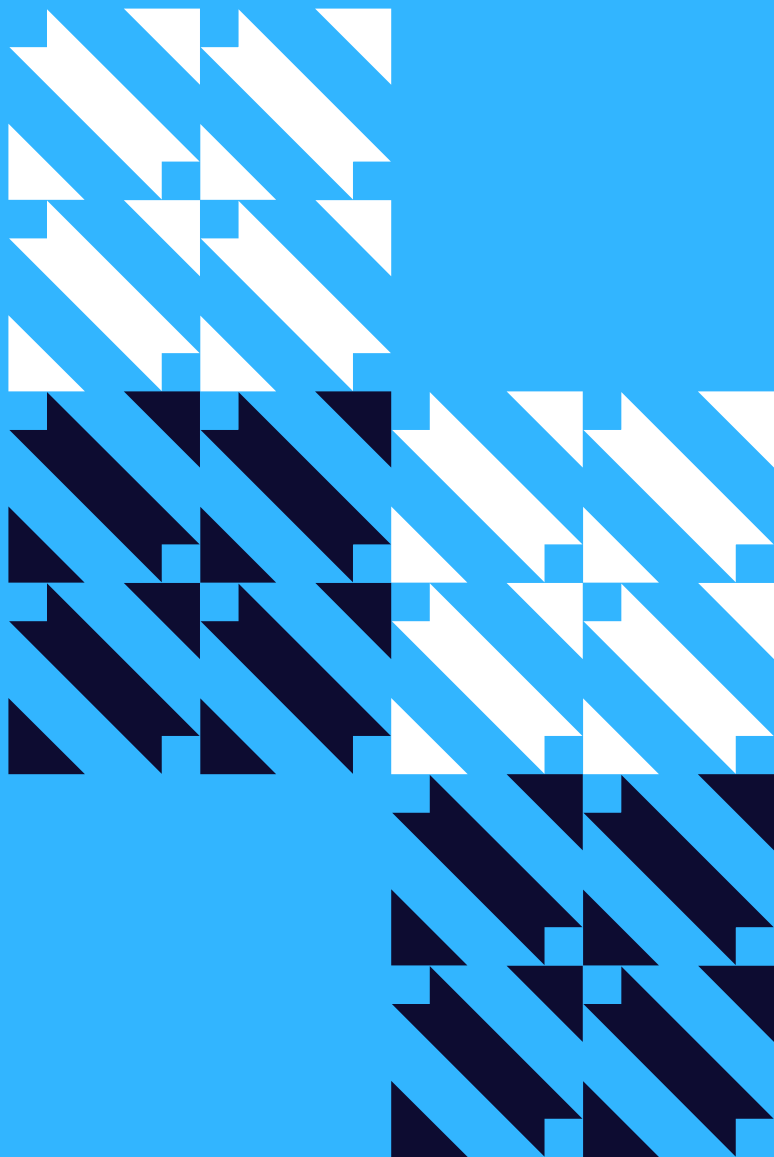
En septembre 2025, les autorités lituaniennes ont arrêté quinze personnes accusées d'être à l'origine des incendies à travers les réseaux de livraison DHL et DPD. Des colis piégés avec des engins explosifs ont été envoyés en Allemagne, en Pologne et au Royaume-Uni, provoquant des explosions dans plusieurs entrepôts, centres logistiques ou camions. Les inculpés sont suspectés d'avoir été au service des services de renseignement militaire russes. L'actualité des mois précédents illustre aussi les menaces croissantes qui pèsent sur les entreprises européennes. Le 7 mai 2025, la maison Dior a reconnu avoir été victime d'une cyberattaque au cours de laquelle des données de clients avaient été compromises plusieurs mois auparavant. Au Danemark, le 21 mai, des composants suspects ont été découverts dans des équipements importés par Green Power Denmark et destinés au réseau énergétique national. Le lendemain, la chaîne britannique Marks & Spencer a révélé une attaque informatique ayant causé plus de 300 millions de livres de pertes malgré des dispositifs de cybersécurité réputés solides.

Les menaces hybrides sont désormais omniprésentes et ne se limitent plus aux sphères étatiques. D'après Florent Kirschner, constitue une menace hybride « le recours par un acteur étranger d'une combinaison intégrée et volontairement ambiguë, des modes d'actions militaires et/ou non militaires, directs et indirects, légaux et illégaux, difficilement attribuables. » Elles ciblent un nombre croissant d'acteurs, en particulier les grandes entreprises. En combinant cyberattaques, espionnage économique, désinformation ou pressions réglementaires, elles exploitent les interdépendances technologiques et visent à affaiblir la compétitivité et la souveraineté.

Ces incidents traduisent une évolution majeure : dans un contexte géopolitique marqué par la fragmentation, les entreprises européennes sont devenues des cibles privilégiées d'acteurs étatiques comme non étatiques. La résilience stratégique ne relève donc plus du seul champ de la défense nationale, mais devient une responsabilité partagée entre États et entreprises.

Partie 1

Constats – Enjeux stratégiques



I Constats – Enjeux stratégiques

A) La souveraineté technologique : à l'intersection de la sécurité et de l'industrie

La Revue Nationale Stratégique publiée par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) en juillet 2025 évoque explicitement le risque d'une guerre majeure de haute intensité en Europe. En outre, les tensions géopolitiques ont une incidence bien au-delà des fronts de guerre. L'exposition aux menaces hybrides impose aux décisionnaires d'appeler à un effort simultané de défense, de résilience et d'industrialisation. Les entreprises sont ainsi en ligne de front, d'une guerre où les frontières entre menaces physiques et menaces cyber sont de plus en plus floues.

La revue mentionne un durcissement de la posture de la Chine ainsi qu'une mise à l'épreuve de la solidarité transatlantique et souligne les conséquences hybrides de la hausse des tensions. L'opposition croissante entre Chine et Etats-Unis se manifeste sur plusieurs champs simultanément : guerre commerciale avec la hausse des tarifs douaniers (+145% sur les importations venues de Chine en avril 2025), la course aux technologies de rupture (avec une mesure de rétorsion sur la vente de terres rares vers les Etats-Unis, éléments essentiels à la fabrication des semi-conducteurs) jusqu'à l'influence sur les institutions internationales ou encore l'influence sur les publics (avec la mise en place d'une filiale américaine de TikTok dont l'algorithme sera contrôlé par les autorités étatsuniennes).

La RNS pose comme objectif de résilience cyber, la maîtrise des technologies critiques et des capacités d'évaluation des produits et des services, qui passe par un soutien au niveau européen des d'acteurs industriels de premier rang mondial.

La majorité des infrastructures numériques et des services cloud européens reposent sur des solutions étrangères, en particulier américaines, ce qui concerne tant le stockage, les traitements de données que les outils de sécurité, avec peu d'alternatives locales suffisamment robustes. La dépendance inclut aussi le matériel critique (semi-conducteurs et composants électroniques), en grande partie produits en Asie, ainsi que l'accès à des matières premières stratégiques comme les terres rares, dont la Chine contrôle la majeure partie des ressources et de la chaîne d'approvisionnement. Cette dépendance s'est intensifiée alors que le nombre et la gravité des cyberattaques explosent : près d'une entreprise française sur deux a connu une attaque majeure en 2024-2025, les secteurs essentiels comme la santé, l'énergie, l'industrie et les collectivités étant particulièrement exposés. Au premier trimestre 2025, les campagnes de ransomware ont connu une croissance de 126% par rapport à 2024. Parmi elles, des groupes russophones comme CI0p ou Qilin, deux groupes qui calibrent leurs attaques en fonction des retours financiers espérés. De plus, la France est le deuxième pays au monde le plus touché par les fuites de données (1,8M de comptes compromis au S1 2025).

Face à l'amplification des menaces cyber et hybrides, il est crucial de sortir de la situation de dépendance des technologies extracommunautaires.

Garantir un accès souverain à ces technologies est essentiel, non pour viser une autarcie illusoire, mais pour réduire les leviers de pression extérieurs.

B) La protection de la compétitivité dans un contexte réglementaire renforcé

Le Cyber Resilience Act adopté fin 2024 adresse ces menaces sécuritaires qui touchent les réseaux informatiques et les appareils numériques. Cette réglementation (qui comprend le matériel mais aussi le logiciel) vise quatre objectifs :

- L'application stricte de la Security by Design and by Default. Les produits numériques devront être conçus avec des dispositifs de sécurité inclus dès leur phase de développement et activé par défaut.
- La responsabilisation des fabricants. Les producteurs devront répondre aux obligations de détection et correction des vulnérabilités des produits proposés.
- Harmonisation européenne. La portée de cette réglementation sera communautaire et permettra d'harmoniser les dispositions nationales au sein du marché unique. Elle assurera aussi l'alignement entre conformité des produits et niveau de cybersécurité pertinent.

- Le CRA assure une transparence vis-à-vis des consommateurs en permettant à ceux-ci d'être au courant des capacités de sécurité du produit qu'il achète.

Certains acteurs industriels sont toutefois déjà largement structurés autour de ces exigences, notamment en matière de sécurité-by-design, d'encryptage natif dans le hardware, de gestion continue des vulnérabilités ou encore de cycles de vie allongés des produits. Ces approches anticipent l'esprit du CRA : des technologies conçues dès l'origine pour réduire la surface d'attaque, limiter les risques de compromission et offrir aux organisations des garanties plus robustes sur l'intégrité de leurs terminaux. Elles démontrent qu'une convergence réelle entre innovation privée et exigences réglementaires européennes est non seulement possible, mais déjà engagée.

Cette nouvelle règlementation qui entrera en vigueur en septembre 2026 renforcera la robustesse et la résilience stratégique des entreprises. En imposant la sécurité dès la conception (« security by design ») et la gestion continue des vulnérabilités, le CRA oblige les fabricants à réduire les risques d'exploitation des failles, limitant ainsi les vecteurs d'attaques potentielles sur les entreprises utilisatrices. De plus, les entreprises qui utiliseront des produits numériques conformes au CRA auront, d'une part, une plus grande autonomie dans les choix technologiques qu'ils réaliseront. D'autre part, ils seront pleinement conscients des implications stratégiques et sécuritaires que représentent ces choix. Sur le long terme, les entreprises développeront une plus grande culture de la sécurité et de vigilance qui sera elle-même gage de fiabilité et facteur de compétitivité.

Le CRA oblige les producteurs et importateurs de produits numériques à prendre en compte les risques de sécurité dans la production et le cycle de vie, de manière à pouvoir apporter des conseils aux utilisateurs, en signaler les vulnérabilités et fournir des mises à jour pendant cinq ans. Toutes ces dispositions nécessiteront donc des investissements importants. Néanmoins, les coûts de mise en conformité seront compensés par les coûts de traitement des incidents de cybersécurité évités, l'harmonisation des normes et la compétitivité.

La capacité à concilier ces impératifs de sécurité avec l'agilité économique et l'innovation conditionnera la place de l'Europe dans la compétition mondiale. Cette exigence de contextualisation est au coeur de l'acceptabilité du changement.

C) Gouvernance et Sécurité : la nécessité d'un pilotage stratégique

La résilience ne doit plus être pensée comme un enjeu purement technique relevant du département informatique, mais comme un pilier de la stratégie globale. Les menaces hybrides qui visent les entreprises ne prennent pas uniquement la forme de cyberattaques. Bien que l'ENISA (Agence européenne pour la Cybersécurité) ait documenté plus de 4800 incidents entre juin 2024 et juin 2025 contre les entreprises européennes, celles-ci peuvent également se retrouver victimes de campagnes de désinformation, d'espionnage industriel ou d'attaques physiques. Face à cette diversité de formes des menaces hybrides, les entreprises ont pour impératif de définir une stratégie de protection et de proactivité. La sécurité hybride ne saurait se cloisonner aux départements techniques des entreprises. Les implications de ces risques et menaces imposent aux conseils d'administration de s'emparer de la question.

La construction d'une résilience face aux risques et menaces hybrides passe par le renforcement des capacités d'anticipation, de réponse, de veille, en somme d'une vigilance accrue. Ces piliers de la résilience présentés par Marjorie Bordes, CISO chez Capgemini, concernent l'ensemble des niveaux hiérarchiques d'une entreprise et doivent être saisis par les instances de direction et d'administration en premier lieu afin d'en assurer le pilotage stratégique.

L'anticipation des menaces hybrides passe par la mise en place d'une veille stratégique systématique. A partir de sources internes et externes, les entreprises doivent créer un système de remontée et de centralisation des signaux. Les signaux faibles permettent par la suite d'évaluer les risques et menaces, de pouvoir en anticiper les conséquences et adresser les failles. Néanmoins, la veille systématique ne saurait se limiter aux données numériques. L'ensemble de l'organisation doit être formée à l'identification de ces signaux faibles. L'implication de l'ensemble des collaborateurs permet à l'entreprise d'établir et d'entretenir une culture de la vigilance qui renforce sa résilience face aux différentes menaces.

Les capacités de défense et de réponse des entreprises relèvent d'abord de l'orientation stratégique de son conseil d'administration. C'est aux décideurs de définir les risques et menaces prioritaires pour développer les mesures de protection adaptées. En ce sens, l'entreprise doit connaître ses actifs critiques (systèmes, logiciels, données...), ses vulnérabilités, et mettre en place des plans de traitement des risques.

Les conseils d'administration doivent traiter la sécurité et la gestion des risques hybrides comme des priorités au même titre que les enjeux financiers ou

environnementaux. Dans un contexte où les attaques contre les chaînes logistiques, les données sensibles et la réputation des entreprises sont omniprésents et où ces menaces touchent autant les capacités de production des entreprises que leur réputation, il existe d'importants risques financiers. Le cas des attaques contre le réseau Orange en Roumanie en février 2025 illustre bien la complexité de ces menaces ; les attaques ont visé à la fois le matériel physique, les logiciels et des fuites de données, et la réputation de l'entreprise avec des relais dans les médias.

D) Les partenariats public-privé (PPP), facteur d'autonomie face aux menaces hybrides

Les menaces hybrides évoluent à un rythme que les cycles budgétaires et décisionnels publics peinent à suivre. Face à cette asymétrie temporelle et capacitaire, les partenariats public-privé (PPP) s'imposent comme des leviers stratégiques de résilience. Les entreprises, cibles privilégiées de ces menaces, détiennent des capacités technologiques et une agilité d'innovation valorisables. En associant le secteur privé à l'anticipation et à la réponse, les PPP permettent un partage des risques, une accélération du déploiement de solutions, et un renforcement mutuel des capacités. Cette complémentarité est particulièrement critique dans les secteurs stratégiques où les opérateurs d'importance vitale constituent la première ligne de défense.

Toutefois, l'efficacité des PPP dans la gestion des menaces hybrides est conditionnée par leur inscription dans un cadre de souveraineté numérique rigoureux. Les partenariats à long terme doivent garantir la conformité aux réglementations européennes (NIS2, Cyber Resilience Act) et permettre aux autorités publiques de conduire des audits réguliers des solutions développées. L'interopérabilité technologique entre systèmes publics et privés, le recours à des solutions certifiées, et l'établissement de mécanismes de gouvernance partagés sont essentiels pour prévenir les risques de dépendance excessive ou de conflits d'intérêts.

La résilience hybride repose in fine sur une compréhension commune des risques entre entreprises stratégiques et autorités publiques. Cela implique des protocoles de partage d'information sécurisés, des exercices conjoints de simulation de crise, et des mécanismes de décision collaboratifs en temps réel. Néanmoins, ces dispositifs doivent être encadrés par des garde-fous assurant la protection des données sensibles et la préservation des prérogatives régaliennes. Frédéric Fauchère, Directeur de la Division Mobile de Samsung Electronics France le souligne : « je n'ai jamais observé de situation de dépendance lorsque le partenariat est correctement tissé, fondé sur un socle de confiance, d'exigences communes et d'alignement avec les standards européens. »

En somme, les PPP ne constituent pas une externalisation de la sécurité nationale, mais une extension du périmètre de défense collective face à des adversaires qui ne distinguent pas secteurs public et privé dans leurs stratégies de déstabilisation.

E) La protection des secteurs stratégiques face aux ingérences étrangères

Les entreprises dans l'énergie, la défense, les télécommunications, les biotechnologies ou l'aéronautique sont directement ciblées par des stratégies d'influence ou d'acquisition. Philippe Susnjara, ancien général à la tête de la Direction du Renseignement de la Sécurité de la Défense (DRSD) a déclaré lorsqu'il était toujours en poste, dans un entretien à Franceinfo, que « les champs les plus visés aujourd'hui sont liés à l'aéronautique et au spatial, aux technologies de rupture, l'intelligence artificielle et le quantique » ainsi que les domaines liés aux grands fonds marins. L'avance de la France dans ces secteurs attise l'intérêt des rivaux. Il devient donc indispensable de protéger des tentatives d'ingérence étrangères ces secteurs qui constituent autant d'avantages stratégiques pour notre économie.

Le rapport d'information déposé en juillet à la commission des finances par Christophe Plassard, député de Charente-Maritime, dresse un panorama inquiétant des menaces sur la Base Industrielle et Technologique de Défense (BITD) : les menaces informatiques/cyber, réputationnelles et physiques ne constituent qu'une seule partie des menaces hybrides. Les menaces humaines, juridiques et économiques, moins visibles, constituent la partie la plus importante de celle-ci.

Les menaces humaines incluent l'espionnage, les indiscrétions internes des salariés, le chantage ou le recrutement ciblé de compétences. Par exemple, dans certains cas, le personnel d'une entreprise peut être invité à un faux entretien d'embauche organisés par des cabinets de conseil étrangers pour soutirer des informations à des cadres du secteur de la défense. Les attaques physiques, qui représentent 1 attaque sur 5, concernent les sabotages, cambriolages, la dégradation de matériel ou le survol de sites sensibles par drone.

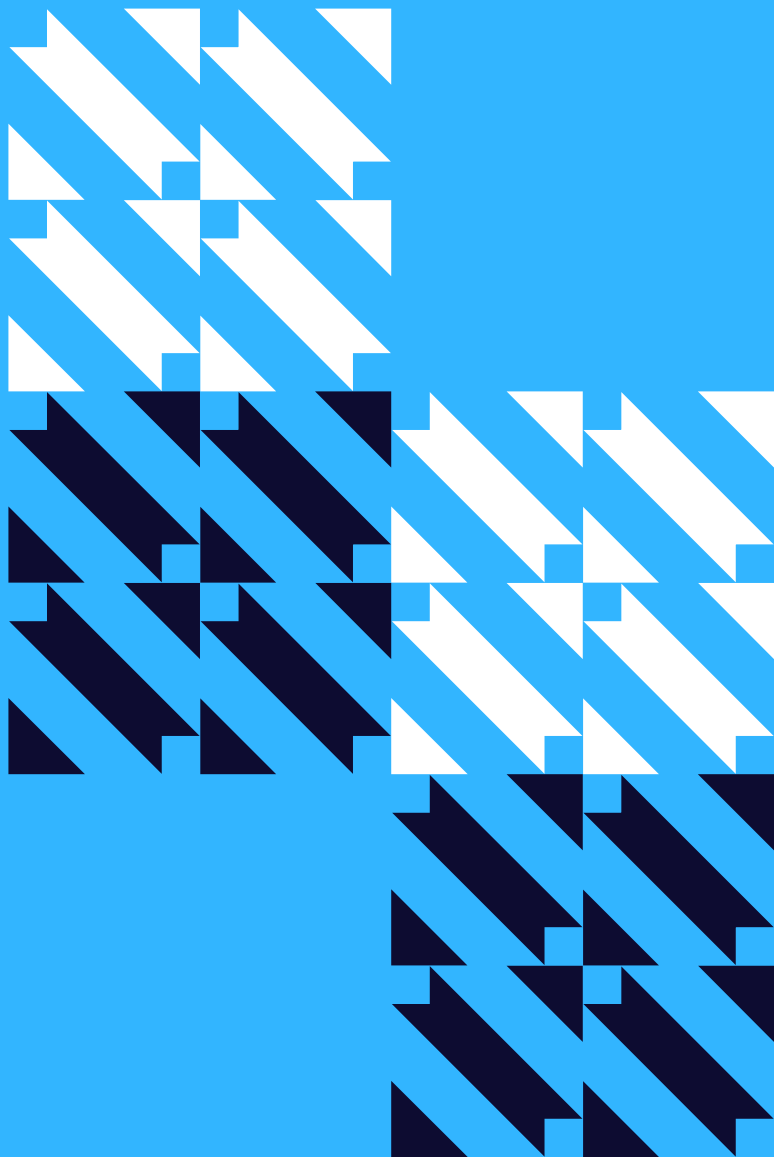
Les menaces économiques (ou capitalistiques) visent les entreprises financièrement fragiles par des prises de contrôle hostiles par investissement. Ces opérations menacent directement la souveraineté économique, et porte le risque de pertes de contrôle sur des technologies critiques, et des délocalisations au profit de concurrents directs. De plus, la menace économique peut être couplée à une menace juridique, appelée lawfare. Cette menace correspond à une instrumentalisation du droit par un pays tiers (en général par des normes à portée extraterritoriale) ce qui leur permet d'avoir accès à des données confidentielles.

Ces deux dernières menaces ont ceci de particulier qu'ils n'ont pas nécessairement leurs origines dans des pays inamicaux et adversaires. Comme rapporté par C. Plassard, « Les ingérences étrangères les plus graves proviennent naturellement de la Russie et de la Chine ainsi que d'autres pays dont l'industrie de défense est concurrente de la nôtre, mais certaines proviennent aussi de pays qui sont nos alliés sur le plan géostratégique, en tête desquels les États-Unis. » Le levier principal contre les menaces capitalistiques reste la loi de blocage du 26 juillet 1986 qui a été réactivée et qui interdit à toute personne de nationalité française de communiquer des renseignements de nature à porter atteinte à la souveraineté de la France à des autorités publiques étrangères.

L'État cherche à renforcer sa capacité de réponse aux menaces hybrides en impliquant l'ensemble des parties prenantes (entreprises, société civile…) qui sont visées mais aussi comme sources de solutions. Parce que la réponse doit être interministérielle, c'est le SGDSN qui coordonne les actions de réponse en s'appuyant sur l'ANSSI, Vigenum et le C4 (centre de coordination des crises cyber) et les autres acteurs de lutte contre les différents types d'attaques. L'arsenal juridique et institutionnel a été renforcé au cours des dernières années pour rehausser la capacité de réponse de la France et plus largement de l'Europe.

Partie 2

Défis – Menaces



II Défis – Menaces

A) Des menaces sophistiquées et persistantes

L'espionnage numérique, le sabotage discret, le vol de données, la désinformation et l'intoxication constituent un arsenal de menaces hybrides qui, par leur diversité et leur persistance, créent un bruit de fond permanent déstabilisant profondément les institutions et les entreprises. Cette pollution stratégique constante érode méthodiquement les fondations de nos sociétés.

La force de ces menaces réside dans leur adaptabilité exceptionnelle. Les acteurs hybrides renouvellent continuellement leurs vecteurs d'attaque, passant du cyberespace aux manipulations médiatiques, du sabotage économique aux pressions juridiques. Cette mutation perpétuelle complexifie la détection et contourne systématiquement les stratégies de défense traditionnelles. Contrairement aux menaces conventionnelles, elles frappent simultanément sur tous les fronts : infrastructures numériques, chaînes d'approvisionnement, opinion publique, secteur énergétique. Cette multiplicité crée une surcharge cognitive qui épuise les capacités de réponse des organisations.

L'intégration d'acteurs non étatiques, le recours à des réseaux criminels et l'exploitation des failles juridiques permettent des attaques insidieuses, souvent détectées trop tard. Ces opérations coordonnées visent un objectif central : affaiblir la cible sans déclencher de conflit ouvert, créant une incertitude permanente qui paralyse la prise de décision. Les entreprises, constamment sur la défensive, perdent leur capacité d'innovation. Les États voient leur souveraineté grignotée par des tactiques de lawfare et des acquisitions stratégiques orchestrées.

Les conséquences à long terme de ce harcèlement permanent sont importantes et doivent être adressées avec attention. Les employés doutent de la sécurité de leurs informations, les citoyens questionnent la légitimité de leurs institutions, les partenaires commerciaux hésitent à collaborer. Cette érosion de la confiance, difficilement quantifiable mais profondément destructrice, fragilise l'ensemble de l'écosystème économique et social.

L'altération de la perception collective amplifie cette déstabilisation. En investissant massivement la sphère informationnelle, les acteurs hybrides manipulent l'opinion, polarisent les sociétés et dressent les groupes les uns contre les autres. Cette fragmentation sociale augmente exponentiellement la vulnérabilité face à d'autres attaques, créant un cercle vicieux de défiance et d'affaiblissement.

Sur le plan économique, la cohésion se délite. Les investissements ralentissent face à l'incertitude chronique, les coûts de sécurité explosent, les collaborations internationales se raréfient. Les ressources consacrées à la défense contre ces menaces sont autant de moyens détournés de l'innovation et du développement. Pire encore, le vol systématique de savoir-faire et la capture progressive de secteurs stratégiques modifient durablement la balance des pouvoirs économiques mondiaux.

B) Prouver la capacité à se transformer et éviter le biais de confirmation

Les chaînes d'approvisionnement constituent aujourd'hui le maillon le plus vulnérable de notre architecture économique et sécuritaire. Leur complexité croissante et leur interdépendance mondiale en font des cibles privilégiées pour les acteurs hybrides, qui y voient une opportunité d'infiltration discrète et de déstabilisation profonde. L'explosion des cyberattaques ciblant les fournisseurs révèle l'ampleur de cette menace systémique.

Les ransomwares frappant des fournisseurs souvent invisibles mais critiques illustrent cette vulnérabilité. Un simple prestataire de logiciels de gestion peut devenir le vecteur d'une compromission massive, propageant l'infection à des centaines d'entreprises simultanément. Ces fournisseurs négligés, aux budgets de sécurité limités, représentent des portes dérobées idéales pour accéder à des organisations bien mieux protégées. L'effet domino qui en résulte paralyse des secteurs entiers en quelques heures.

Plus insidieux encore, l'insertion de composants compromis dans des équipements critiques constitue une bombe à retardement. L'affaire Green Power au Danemark a démontré comment des éléments corrompus peuvent infiltrer des infrastructures stratégiques, menaçant directement la sécurité nationale. Ces chevaux de Troie matériels, indétectables pendant des années, permettent l'espionnage, le sabotage ou la paralysie de systèmes essentiels dans les

secteurs de l'énergie, des télécommunications ou de la défense.

La dépendance économique stratégique amplifie cette fragilité. Le rachat systématique de fournisseurs clés par des acteurs étrangers, le contrôle de matières premières critiques ou l'établissement de monopoles sur des technologies essentielles créent des rapports de force asymétriques. Cette mainmise progressive érode la souveraineté économique et transforme les États en otages de leurs propres besoins industriels.

Si nous ne nous défendons pas, les conséquences seront catastrophiques. La perturbation coordonnée de la logistique, combinant cyberattaques et événements physiques, pourrait paralyser durablement la circulation de matières premières et de composants vitaux. Une nation privée de semi-conducteurs, de terres rares ou d'équipements de télécommunication se retrouve instantanément vulnérable, incapable de maintenir ses infrastructures critiques.

La manipulation économique via le contrôle des chaînes d'approvisionnement permet d'exercer une pression politique dévastatrice. Un fournisseur monopolistique peut dicter ses conditions, influencer les décisions souveraines ou simplement fermer le robinet au moment stratégique. Cette arme économique, invisible mais redoutable, transforme la dépendance commerciale en levier géopolitique.

L'objectif ultime de ces tactiques est clair : saper la résilience nationale en multipliant les points de défaillance. Chaque composant compromis, chaque dépendance créée, chaque fournisseur racheté constitue un maillon supplémentaire dans les chaînes qui entraveront demain notre liberté d'action. L'instabilité accrue facilite les crises orchestrées et les actes de sabotage dissimulés dans le tissu économique normal.

Face à cette menace existentielle, la reconquête de notre souveraineté industrielle et la sécurisation de nos approvisionnements ne sont plus des options, mais des impératifs de survie stratégique.

C) Les stratégies étrangères en coulisses

Les opérations de menace hybride qui déstabilisent l'Europe ne relèvent pas du hasard ou d'acteurs isolés. Elles sont méthodiquement coordonnées par des puissances étrangères qui ont érigé la guerre non conventionnelle en doctrine stratégique. La Russie et la Chine dominent ce paysage, déployant des stratégies sophistiquées visant à affaiblir l'Union européenne et ses États membres sans franchir le seuil d'un conflit armé ouvert.

L'opacité constitue le socle de ces opérations. En mêlant habilement actions licites et illicites, ces puissances rendent l'attribution formelle quasi impossible. Cyberattaques, campagnes de désinformation, sabotages d'infrastructures, pressions économiques et ingérences politiques forment un arsenal diffus qui maintient les cibles dans l'incertitude permanente. Cette ambiguïté délibérée paralyse les réponses occidentales, prisonnières de la nécessité de prouver l'implication directe avant d'agir.

La Russie déploie une stratégie particulièrement agressive depuis l'invasion de l'Ukraine. Ce conflit sert de laboratoire géant pour expérimenter et perfectionner ses tactiques hybrides. Sabotages d'infrastructures critiques, campagnes d'espionnage massif, infiltration des réseaux de soutien à Kiev, incursions dans l'espace aérien européen : Moscou multiplie les provocations calculées pour affaiblir simultanément l'Ukraine et les démocraties européennes qui la soutiennent. L'objectif est double : épuiser la détermination occidentale tout en testant les limites de la réponse collective.

La Chine privilégie une approche à plus long terme, mais tout aussi redoutable. Sa stratégie vise à établir une domination globale d'ici 2049, en s'appuyant sur l'acquisition méthodique d'acteurs stratégiques européens, le contrôle de secteurs technologiques clés et des campagnes d'influence sophistiquées. Dans les domaines critiques pour la compétitivité européenne – semi-conducteurs, intelligence artificielle, énergies renouvelables, télécommunications – Pékin déploie une stratégie de pénétration économique qui masque des objectifs géopolitiques. Les investissements chinois dans les ports, les réseaux 5G ou les entreprises technologiques créent des dépendances structurelles qui seront activées le moment venu.

Au-delà de l'Ukraine et des tensions autour de Taïwan, ces puissances étendent leur influence en Afrique, dans les Balkans et au Moyen-Orient, tissant une toile globale d'affaiblissement des structures occidentales. Cette expansion multidirectionnelle dilue les capacités de réponse et crée des fronts multiples d'instabilité.

Face à ces menaces coordonnées, l'Europe doit comprendre qu'elle affronte non pas des incidents isolés, mais une guerre stratégique de longue haleine, orchestrée par des États déterminés à remodeler l'ordre mondial à leur avantage.

D) Des formes hybrides de coercition économique et financière

Les formes hybrides de coercition économique et financière redéfinissent radicalement le paysage des risques pour les organisations françaises en 2025, en transforment la compétition économique en terrain d'affrontement stratégique où les frontières entre commerce et guerre d'influence s'effacent dangereusement.

Le facteur humain constitue désormais la première ligne de vulnérabilité. Selon la DRSD, 36% des atteintes dénoncées ciblent les personnels clés à travers des opérations de débauchage orchestré, de manipulation psychologique ou de recrutements fictifs. Cette captation systématique des talents vise directement le savoir-faire stratégique, affaiblissant durablement la capacité d'innovation et la compétitivité des entreprises françaises.

Le lawfare et les pressions réglementaires constituent des armes redoutablement efficaces. Les entreprises se retrouvent prises en étau entre des contraintes réglementaires légitimes mais croissantes – RGPD, normes européennes – et leur instrumentalisation malveillante. Procédures judiciaires abusives, interprétations hostiles de la législation, campagnes de dénigrement déguisées en alertes réglementaires : ces tactiques permettent d'affaiblir ou de discréditer les concurrents sans confrontation directe.

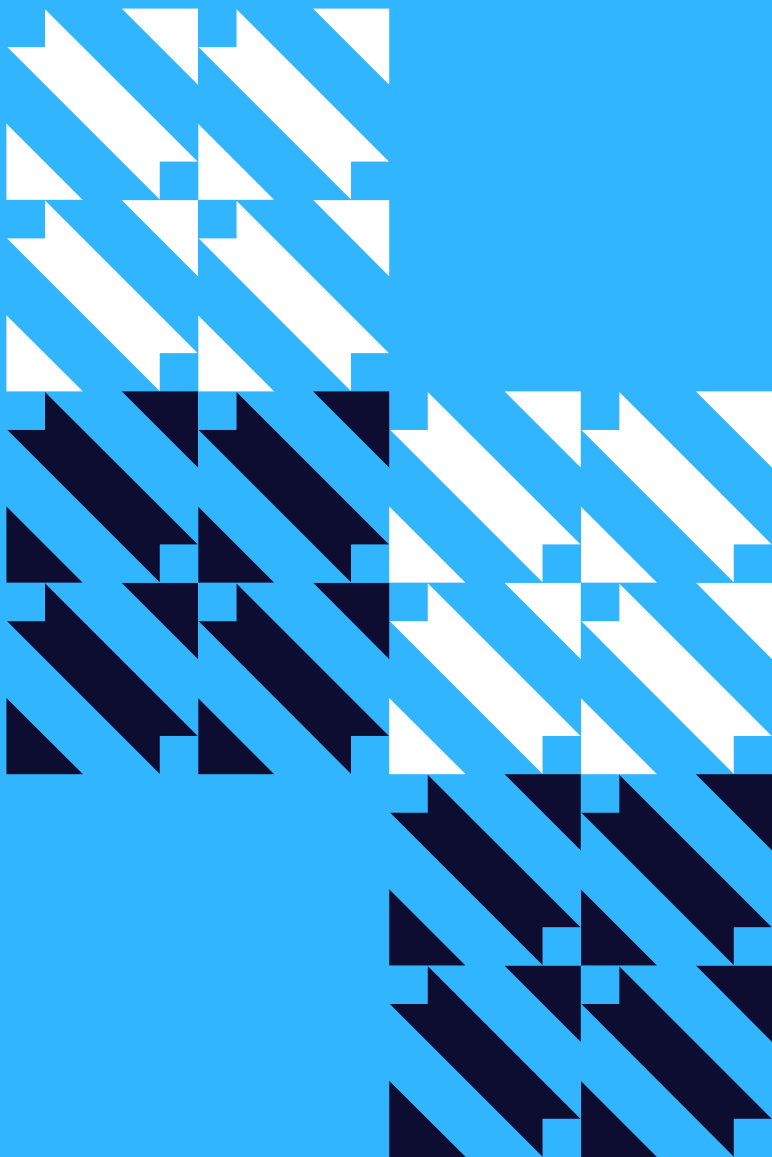
Les dépendances critiques dans les chaînes d'approvisionnement exposent les entreprises à des manipulations industrielles sophistiquées. L'introduction de composants compromis dans les logiciels ou le matériel crée des vulnérabilités stratégiques exploitables à distance et sur demande. Cette infiltration progressive transforme les outils de production en chevaux de Troie potentiels.

Les prises de participation et acquisitions hostiles complètent cet arsenal. Sous couvert d'investissements légitimes, des acteurs étrangers prennent le contrôle d'actifs stratégiques, accédant ainsi aux technologies sensibles, aux carnets de commandes et aux secrets industriels. Les manipulations médiatiques accompagnent souvent ces opérations, déstabilisant la gouvernance et facilitant les prises de contrôle.

L'impact sur la compétitivité est dévastateur. Les coûts de sécurisation explosent, mobilisant des ressources considérables au détriment de l'innovation. Les chaînes logistiques déstabilisées génèrent retards et surcoûts. La défiance des clients et partenaires qui en découle entraîne des pertes de parts de marché durables. Certaines entreprises renoncent purement et simplement à certains marchés sensibles, jugés trop risqués.

Partie 3

Propositions



III Propositions

A) Mobiliser les outils européens existants

L'UE a développé des outils de protection et de financement afin de contrer les menaces hybrides. En mars 2022, au lendemain de l'invasion de l'Ukraine, la boussole stratégique approuvée par le Conseil de l'UE incluait la mise en place d'une « boîte à outils hybrides [...] visant à détecter un large éventail de menaces hybrides et à y réagir » et à augmenter les investissements pour « réduire les dépendances technologiques ». En décembre, de la même année, l'adoption de la directive NIS 2 vient élargir le champ d'application des exigences en matière de cybersécurité et oblige les États membres à définir des stratégies nationales, à créer des équipes nationales de réponse aux incidents informatiques (CSIRTs) et instaure un réseau de gestion de crise cyber (EU-CyCLONe) pour coordonner les ripostes aux attaques majeures.

Le mécanisme SAFE présenté en septembre dans le cadre du plan Readiness 2030 prévoit 150 milliards d'euros de financement destinés aux Etats et acteurs de la BITDE sous formes de prêts à taux préférentiels. Les secteurs financés incluent en priorité les systèmes utiles contre les menaces hybrides : dans la « catégorie 1 » figurent la protection des infrastructures critiques et la cyberdéfense.

Néanmoins, ces financements doivent être orientés et accessibles pour les entreprises privées critiques qui constituent la première ligne de défense face aux menaces hybrides. En soutenant directement leur innovation, leur mise en conformité et leur intégration dans les chaînes industrielles européennes, l'UE renforcerait à la fois sa résilience stratégique et son autonomie technologique, transformant la défense commune en levier de souveraineté économique.

B) Mettre en place un fonds européen de résilience stratégique

Les petites et moyennes entreprises demeurent aujourd'hui parmi les cibles les plus exposées aux cyberattaques. Leur vulnérabilité s'explique à la fois par leurs ressources limitées en matière de cybersécurité et par leur rôle d'intermédiaires dans les chaînes de valeur. Reliées à de grands groupes ou à des services publics via des contrats ou des prestataires, elles constituent souvent la porte d'entrée idéale pour des attaques plus larges. En 2024, plusieurs incidents l'ont rappelé : des attaques contre des prestataires logistiques liés à Boulanger et Cultura ont entraîné la fuite des données personnelles de plusieurs millions de clients. Ce type d'événement illustre combien les maillons intermédiaires de l'économie européenne reste exposés aux menaces hybrides.

Les modes d'attaque les plus répandus demeurent le phishing et les ransomwares, souvent combinés à des campagnes d'ingénierie sociale. Le télétravail massif a accentué les failles de sécurité : connexions non sécurisées, ordinateurs personnels mal protégés, usage de réseaux Wi-Fi publics. Par ailleurs, la généralisation des objets connectés (caméras, capteurs, équipements domotiques) ouvre de nouvelles brèches pour les cybercriminels. Les PME, souvent peu préparées à cartographier et à protéger ces dispositifs, voient ainsi leur surface d'exposition s'accroître de façon exponentielle.

Face à ces risques, les besoins de renforcement sont multiples. Le modèle de « zero trust », reposant sur une vérification systématique des identités et des accès, doit devenir la norme, tout comme l'authentification multifactorielle. La sécurisation des messageries – principal vecteur de phishing – et la protection des données hébergées sur le cloud constituent également des priorités. Ces évolutions supposent des investissements importants : acquisition d'équipements conçus selon le principe du security by design, diversification des fournisseurs technologiques pour réduire les dépendances critiques, et déploiement de politiques internes de formation continue. En effet, la compétence humaine reste le premier rempart contre la désinformation, la négligence et les erreurs d'utilisation.

Or, de nombreuses PME ne disposent ni des moyens financiers ni des expertises techniques nécessaires pour mettre en oeuvre ces mesures. D'où la nécessité d'un fonds européen de résilience stratégique, spécifiquement destiné à renforcer la cybersécurité des acteurs privés critiques. Ce dispositif pourrait cofinancer les audits, les équipements, la formation et la mise à niveau des infrastructures numériques. En soutenant la montée en compétence des PME et en encourageant une culture commune de la sécurité, l'Union européenne renforcerait non seulement la protection de son tissu économique, mais aussi la cohérence globale de sa défense face aux menaces hybrides.

C) Création d'une agence européenne de défense économique

Les menaces économiques, souvent sous-estimées, constituent un risque majeur à la souveraineté européenne. L'UE s'est dotée progressivement d'outils visant à contrôler les investissements étrangers et les risques qu'ils représentent dans les secteurs stratégiques. Établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union, établi en octobre 2020, prévoit un mécanisme d'échange d'informations entre les Etats et la Commission dans le cadre d'investissements extra-européens. Néanmoins, les systèmes de filtrage peuvent encore être développés. Selon la Cour Européenne des Comptes, « les États ne sont pas tenus de communiquer à la Commission européenne leurs décisions en matière de filtrage, même si celle-ci a émis un avis ou que d'autres États membres ont fait part de leurs inquiétudes. » En l'occurrence, un rapport de la CCE démontre que seuls 17 membres ont notifié la Commission, les 12 autres ayant gardé le silence sur leurs dossiers. Le rapport de C. Plassard illustre le risque que présente ce manque de protection avec le cas de la start-up Vade. Celle-ci ayant longtemps refusé un rachat par l'américain Proofpoint a été finalement revendu à l'allemand Hornetsecurity. Or, cette même entreprise allemande a été revendue à Proofpoint un an plus tard.

Il est donc crucial de mettre en place une agence européenne de défense économique chargée de filtrer les investissements et d'harmoniser les règles en la matière. La Commission a déjà engagé une révision du règlement européen en 2024, qu'il faut concrétiser par une institutionnalisation de la défense économique.

D) Renforcer la diplomatie économique et cyber de l'Union européenne

La réponse aux menaces hybrides doit également passer par une série de politiques diplomatiques communes qui permettent à l'UE d'imposer des normes et protéger ses intérêts face aux tentatives d'ingérence étrangères. La sécurité économique est un concept encore émergent au sein de l'Union européenne, sans définition unique ni répartition claire des compétences entre l'UE et les États membres. L'UE, par ses instruments économiques, réglementaires et commerciaux (contrôles des exportations, NIS 2, filtrage des IDE), et doit les compléter par une augmentation de ses capacités de dissuasion. Celle-ci passe par une coopération entre UE et OTAN, avec notamment la création en 2017 du Centre Européen d'Excellence pour la Lutte Contre les Menaces Hybrides (Hybrid CoE) qui rassemble.

Une coordination accrue des exercices de planification de crise, du partage de renseignement et de la gestion des menaces hybrides permettrait d'éviter les doublons et de renforcer la cohérence euro-atlantique. Néanmoins, compte tenu des menaces américaines sur les entreprises françaises - illustré avec le cas de la start-up française Vade plus haut - l'UE doit maintenir sa propre autonomie dans la définition de sa stratégie et le renforcement de ses capacités.

Bibliographie

- Aubin, Paul. « Les menaces hybrides dans les espaces maritimes ». Institut National des Affaires Stratégiques. Consulté le 31 octobre 2025. https://inas-france.fr/les-menaces-hybrides-dans-les-espaces-maritimes/.
- Bassot, Etienne. « Dix questions essentielles à suivre en 2025 ». Janvier 2025. https://www.europarl.europa.eu/RegData/etudes/IDAN/2025/767186/EPRS_IDA(2025)767186_FR.pdf.
- Centre d'excellence européen pour la lutte contre les menaces hybrides (Hybrid CoE), https://www.hybridcoe.fi/
- « Contrer les menaces hybrides », Organisation du Traité de l'Atlantique Nord (OTAN), 7 mai 2024.
- Cyber Resilience Act, Commission européenne (texte et initiatives réglementaires).
- « Détection des signaux faibles : le bouclier stratégique - CriseHelp ». CriseHelp. Consulté le 31 octobre 2025. https://crisehelp.fr/detection-signaux-faibles-menaces-hybrides-anticipation/.
- Ellison Jonathon, « Cyber Security and Resilience Policy Statement to strengthen regulation of critical sectors », National Cyber Security Centre, 1er avril 2025.
- Fondation Robert Schuman, « Les menaces hybrides, nouveaux horizons de l'Europe de la sécurité intérieure », avril 2025.
- IFRI, « Menaces hybrides », septembre 2025.
- IRIS, « L'Union européenne face aux menaces hybrides et au défi de la résilience », janvier 2025.
- Klepper David, « Russian hackers target Western firms shipping aid to Ukraine », Associated Press, 22 mai 2025.
- « La Commission dévoile le Livre blanc sur la défense européenne et le plan ReArm Europe/Readiness 2030 », Commission européenne, 19 mars 2025.
- Maślanka Łukasz, Szymański Piotr, « The resilience of the European Union and NATO in an era of multiple crises », OSW Centre for Eastern Studies, 28 février 2025.
- Mafart, Jean. « Les menaces hybrides, nouveaux horizons de «l'Europe de la sécurité intérieure» ? » La Fondation Robert Schuman le centre de recherches et d'études sur l'Europe, 14 avril 2025. https://www.robert-schuman.eu/questions-d-europe/787-les-menaces-hybrides-nouveaux-horizons-de-l-europe-de-la-securite-interieure.
- « Menaces hybrides : alerte maximale sur les secteurs stratégiques français - L'Essor de la Sécurité ». L'Essor de la Sécurité, 5 mai 2025. https://lessordelasecurite.org/menaces-hybrides-alerte-maximale-sur-les-secteurs-strategiques-francais/.
- Ministère des Armées (France), « Revue nationale stratégique 2025 : onze objectifs pour une France prête face aux menaces », juillet 2025.
- Motet Laura, Leloup Damien, Reynaud Florian, « Dior victime d'un vol de données personnelles de clients », Le Monde, 13 mai 2025.
- « NIGHT HAWK 21 ~ NATO Special Operations Forces | Joint Forces News ». Joint Forces News. Consulté le 31 octobre 2025. https://www.joint-forces.com/special-forces/47560-night-hawk-21-nato-special-operations-forces. « Menaces hybrides : quand la menace devient invisible et globale ».
- Pyysalo Tapio, « Europe must quickly ramp up its resilience against hybrid threats », Helsinki Security Forum, 24 août 2024.
- Portail Intelligence Économique, « Le sabotage russe en Europe : une menace en plein essor », août 2025.
- Reuters, « Unexplained components found in Denmark's energy equipment imports, industry group says », 21 mai 2025.
- « Rising number of cyber attacks poses challenge for investors », Financial Times, 23 mai 2025.
- Sullivan, Rory. « Lituanie : un réseau soutenu par la Russie inculpé pour des explosions de colis DHL et DPD en Europe ». euronews, 18 septembre 2025. https://fr.euronews.com/2025/09/18/un-reseau-soutenu-par-la-russie-est-a-lorigine-de-lexplosion-de-colis-en-europe-selon-viln.
- Semkel. Consulté le 31 octobre 2025. https://semkel.com/menaces-hybrides-quand-la-menace-devient-invisible-et-globale/.Diploweb, «Les menaces hybrides : quels enjeux pour nos démocraties ?», 2025.
- TRM Labs, « EU and UK crackdown on Russian hybrid threat networks », mai 2025.
- Vigilant, Jean-Marc. « L'Union européenne face aux menaces hybrides et au défi de la puissance ». IRIS - Institut de relations internationales et stratégiques, janvier 2025. https://www.iris-france.org/wp-content/uploads/2025/01/ProgEurope_2025_01_menace-hybride_Vigilant_Note.pdf.

Institut Choiseul

L'Institut Choiseul est un think and do tank indépendant et non partisan. Il se dédie au décryptage des grands enjeux économiques et à la fédération de la jeune génération économique.

Pour alimenter le débat public et incarner les dynamiques économiques en cours, l'Institut Choiseul produit des Notes Stratégiques, des études ponctuelles et des classements de jeunes leaders. Pour fédérer et animer ses communautés, il déploie des évènements de haut-niveau mêlant networking convivial, témoignages d'experts et de praticiens et échanges sur des sujets de prospective, sur différents territoires et verticales économiques, en France, en Europe et en Afrique.

Au croisement de la communauté d'affaires et du cercle de réflexion, l'Institut Choiseul offre une plateforme aux décideurs économiques privés comme publics pour s'identifier mutuellement, se mettre en réseau, promouvoir leurs initiatives et réfléchir aux grandes tendances économiques de demain.

Les partenaires de Choiseul Souveraineté

L'Institut Choiseul est accompagné par un noyau dur de partenaires actuels, tous acteurs français et européens, qui prennent une part active à la discussion et à la formalisation de recommandations.

14, rue Gaillon
7502 Paris, France

EMAIL
contact@choiseul.info

www.choiseul.info

YOUTUBE
Institut Choiseul

TWITTER / X
@instchoiseul

LINKEDIN
Institut Choiseul

INSTITUT
CHOISEUL