

NOTRE SÉCURITÉ A UN PRIX, MAIS ELLE OFFRE AUSSI DES OPPORTUNITÉS

Il convient de considérer la sécurité dans son sens le plus large. Notre sécurité physique, bien sûr, mais aussi la continuité de nos activités, la sécurité de l'emploi, la prospérité... Le monde incertain d'aujourd'hui est sous pression. Comment pouvons-nous nous protéger de manière adéquate contre les risques prévus et inattendus ? Voilà de quoi alimenter une table ronde avec deux ministres compétents, Theo Francken et Bernard Quintin, et le CEO de la FEB, Pieter Timmermans.



Bernard Quintin
Ministre fédéral de la Sécurité
et de l'Intérieur



Theo Francken
Ministre fédéral de la Défense
et du Commerce extérieur



Pieter Timmermans
CEO de la FEB

En collaboration avec l'École Royale Militaire, la FEB a enquêté sur la perception qu'ont les entreprises belges des risques de rupture et sur leur capacité à y faire face (lire l'article « L'imprévisibilité comme seule certitude », p. 06). Les résultats de l'enquête dressent un tableau clair : les risques numériques dominent le paysage belge des menaces. Dans tous les secteurs et dans toutes les entreprises, quelle que soit leur taille, les cyberattaques et les défaillances techniques des systèmes sont considérées comme les plus grandes menaces pour la continuité des activités. Suivies par les tensions commerciales et géopolitiques.

RISQUES & MENACES

Les résultats de l'enquête correspondent-ils à ce que vous considérez comme les plus grands risques pour notre pays et, par extension, pour nos entreprises ?

Bernard Quintin (BQ) : « Le Centre de crise national (NCCN) réalise régulièrement une analyse nationale des risques, la Belgian National Risk Assessment. Pour l'édition 2023-2026, plus d'une centaine de risques ont été étudiés, couvrant des phénomènes naturels, des incidents liés à l'activité humaine et des risques technico-économiques. L'analyse ne se limite pas à la probabilité : elle considère aussi l'impact humain, social, financier et environnemental. Vingt-neuf risques clés ont été identifiés, parmi lesquels la désinformation, les cyberattaques, les pannes d'électricité ou les interruptions de services essentiels comme les infrastructures numériques et l'aviation. Les inondations et les vagues de chaleur constituent également des risques naturels importants. »

Theo Francken (TF) : « 2025 a été une année noire, en raison de l'incertitude liée aux droits de douane américains. À cet égard, je suis plus optimiste pour 2026. L'accord conclu entre l'UE et les États-Unis en Écosse à la fin du mois de juillet n'était certes pas parfait, mais il présente l'avantage de clarifier la situation. Il nous appartient maintenant de continuer à faire pression de manière décisive sur l'UE et les États-Unis pour qu'ils accordent des droits de douane moins élevés à un plus grand nombre de secteurs. Ce qui ne veut pas dire qu'aucun autre risque de perturbation ne se profile à l'horizon. Une action militaire de la Chine contre Taïwan n'est pas non plus à exclure. Si Pékin décide de passer à l'action armée, nous subirons le pire choc économique depuis la crise pétrolière de 1973. Taïwan produit environ 90 % des puces les plus avancées. Celles-ci sont indispensables à l'économie d'aujourd'hui. Il est impossible de les obtenir rapidement ailleurs. Aujourd'hui, les producteurs alternatifs ont déjà de longs délais de livraison. Pour atténuer ce risque, l'Europe met aujourd'hui les bouchées doubles. Mais cela demeure une course contre la montre. Si la Chine jette l'éponge en 2026, la production industrielle en Europe sera gravement perturbée, ce qui entraînera de l'inflation et une grave récession. Par rapport à ce risque économique, tous les autres sont en fait insignifiants. En effet, ces autres risques entraîneraient tout au plus des désagréments à très court terme. »

En ce qui concerne la Chine, quelle est la gravité du risque de boycott des exportations de matières premières critiques vers l'Europe ?

TF : « Elle est plus que réelle. Les exportations de minéraux critiques chinois vers l'Europe font déjà l'objet de restrictions. En période de conflit, ces restrictions se transformeront immédiatement en boycott. Nous nous dirigerions alors vers une paralysie industrielle. Il est donc urgent que l'Europe reprenne pied en Afrique dans le domaine de l'exploitation minière et du raffinage. Cela nécessite une politique africaine réaliste plutôt que moralisatrice. Ce changement est en cours, mais il doit être mis en œuvre beaucoup plus rapidement et plus concrètement. Il n'y a plus de temps à perdre à ce niveau. »

Notre pays doit-il vraiment redouter des scénarios comme celui que nous avons connu récemment avec la panne d'électricité au Portugal et en Espagne ?

TF : « La panne d'électricité en Espagne a montré que lorsqu'un seul maillon faible du réseau se rompt,

« L'EXPERTISE TECHNIQUE DES ENTREPRISES SERA MOBILISÉE POUR CONSTRUIRE DES SOLUTIONS OPÉRATIONNELLES ET PRATIQUES »

Bernard Quintin
Ministre fédéral de la Sécurité et de l'Intérieur





**« CEUX QUI
PENSENT NE PAS
ÊTRE UNE CIBLE
INTÉRESSANTE
POUR UNE
CYBERATTAQUE
LE SONT
JUSTEMENT
SOUVENT »**

Pieter Timmermans
CEO de la FEB

de grandes parties du pays peuvent être paralysées. En Espagne, la panne semble résulter d'une tension trop élevée sur le réseau. Mais cela peut également se produire suite à des cyberattaques ciblées. Le 23 décembre 2015, la Russie a coupé le réseau électrique dans certaines parties de l'Ukraine pendant six heures. Nous nous protégeons de mieux en mieux contre ce risque, mais nous ne pouvons jamais l'exclure totalement. »

Pieter Timmermans (PT) : « Les graves pannes d'électricité survenues en Espagne et au Portugal montrent à quel point l'approvisionnement en énergie peut s'interrompre rapidement, avec des conséquences dramatiques. Heureusement, la Belgique a jusqu'à présent réussi à éviter de tels incidents, le réseau de notre pays se trouvant dans une situation moins précaire que celui de la péninsule ibérique. Maintes fois, des experts ont cependant lancé des mises en garde contre une dépendance excessive à l'égard des importations d'énergie, tout en insistant sur la nécessité de renouveler nos infrastructures pour rendre notre approvisionnement plus robuste. Avec la digitalisation et l'électrification croissantes de notre société, nous devons considérer l'énergie comme un fondement de notre autonomie stratégique. Outre les sources classiques, nous devons par conséquent envisager toutes les options disponibles, telles que le nucléaire, les biocarburants et l'hydrogène. »

Un pays peut-il se « défendre » contre des cyberattaques ciblées, par exemple ?

TF : « Très certainement, et c'est d'ailleurs ce que nous faisons. Nous avons transformé notre Cyber Command en une force à part entière : la Force Cyber. Nous investissons massivement dans les spécialistes et le matériel IT. La coopération avec nos alliés au sein de l'OTAN est excellente. Nous apprenons constamment les uns des autres. À cet égard, nous disposons d'un avantage de taille par rapport à la Russie. Les militaires de notre Force Cyber s'entraînent régulièrement au sein de l'OTAN. Lors d'exercices de simulation, ils se défendent contre les attaques les plus sévères possibles. Dans ce cadre, ils exploitent pleinement l'IA. La Force

Cyber de la Défense est compétente non seulement pour protéger les réseaux, mais aussi pour remédier aux attaques. Les systèmes et réseaux infectés peuvent être nettoyés et redémarrés très rapidement. Je tiens cependant à souligner que la résilience en ligne requiert une approche de l'ensemble de la société. Entreprises, institutions et pouvoirs publics : tout le monde doit veiller à se protéger efficacement. »

BQ : « Je ne peux que me rallier à ce point de vue. Comme pour une entreprise, un pays est plus efficace lorsqu'il combine anticipation efficace et capacité de réaction rapide. La résilience repose essentiellement donc sur ces deux piliers : prévenir les incidents et être prêt à absorber les chocs lorsqu'ils surviennent malgré tout. La loi NIS 2¹ et la future loi CER² instaurent une approche globale des risques, couvrant toutes les menaces pouvant toucher nos infrastructures et services. En parallèle, nous demandons aux entités critiques d'intégrer ces risques de manière complète, tandis que l'État renforce sa capacité de préparation et de réponse via la planification d'urgence, la gestion de crise et le développement du plan national de résilience. L'objectif est de rendre le pays plus robuste et réactif, à l'image des entreprises qui innovent dans la gestion des risques pour garantir la continuité de leurs activités. »

PT : « La cybersécurité est une priorité pour toutes les entreprises. Pas seulement pour les grandes entreprises et les entreprises essentielles qui tombent dans le champ d'application de la loi NIS 2. Pourtant, de nombreuses entreprises pensent encore à tort qu'elles sont 'trop insignifiantes' ou 'trop bien protégées' pour être ciblées. Une méprise dangereuse. En effet, les pirates informatiques ne font pas de différence et choisissent leurs cibles en fonction de leurs faiblesses. Ceux qui pensent ne pas être une cible intéressante le sont justement souvent. Et les dommages directs sont considérables. L'impact indirect est souvent bien plus important encore : perte de productivité, atteinte à la réputation, conséquences juridiques, fuite de données et perte de clients. Dans certains cas, c'est même la continuité de l'activité qui est menacée. Bref, les

1 Cette loi du 26 avril 2024 transpose la directive NIS2 (UE 2022/2555), qui remplace la précédente directive européenne sur la cybersécurité et vise à renforcer la résilience numérique et économique de l'Union européenne en améliorant la cybersécurité des secteurs essentiels.

2 Cette loi transposera la directive européenne CER (directive UE 2022/2557) qui fait partie de la stratégie plus large de l'UE visant à renforcer la sécurité et la résilience d'entités critiques et de leurs infrastructures contre diverses menaces, telles que les catastrophes naturelles, les attaques terroristes, les menaces cybernétiques/technologiques et les pandémies.

cyberattaques constituent aujourd'hui un risque structurel pour les entreprises. Elles affectent non seulement les systèmes IT, mais aussi la santé financière, l'influence stratégique et la confiance des clients et des partenaires. »

PRÉPARATION & PRÉVENTION

Sous l'effet de glissements géopolitiques, nous constatons également une fragmentation du commerce mondial : le commerce se fait de plus en plus entre des pays géopolitiquement alignés plutôt qu'entre des blocs rivaux. Les entreprises peuvent-elles s'adapter à cette nouvelle donne ?

TF : « Oui, elles le peuvent, de deux manières. Depuis la chute du mur, nos entreprises sont parties du principe que l'économie mondiale s'intégrerait progressivement, ce qui se traduirait par des droits de douane de plus en plus bas et des transports de plus en plus efficaces et de moins en moins coûteux. Cela a conduit à un 'comportement insouciant' dans le chef de certaines entreprises. Certaines se sont fiées aveuglément à un seul fournisseur d'un autre continent pour des pièces cruciales. D'autres n'ont plus constitué de stocks en se fiant de manière presque maniaque aux livraisons juste à temps. Ce même optimisme s'est également traduit par une insouciance financière. Depuis la pandémie de coronavirus, nous nous sommes à nouveau rendu compte que l'avenir est imprévisible. Une nouvelle crise mondiale pourrait effectivement se produire. Un bon chef d'entreprise agit comme un bon père de famille : il garde des réserves financières suffisantes et dispose d'un carnet de fournisseurs alternatifs, si possible en Europe même. »

PT : « Le commerce international est essentiel pour une économie ouverte. Nos exportations représentent plus de 85% du PIB belge. En outre, à l'horizon 2030, plus de 85 % de la croissance économique mondiale sera générée en dehors de l'UE. Nos entreprises doivent conquérir les (nouveaux) marchés de croissance. Or cela est loin d'être simple : les entreprises sont confrontées à des tensions géopolitiques, mais aussi à la concurrence techno-industrielle (capitalisme d'État en Chine, politique protectionniste aux États-Unis, etc.). En outre, l'UE a initié différentes mesures unilatérales pour promouvoir la durabilité (CBAM, rapportage ESG...). Tout cela rend le commerce international plus complexe, plus risqué et plus difficile à gérer. Il revient à l'Europe et à la Belgique de faciliter l'accès aux marchés tiers afin que nos entreprises puissent conclure de nouveaux partenariats, diversifier leurs échanges commerciaux et devenir moins dépendantes de partenaires moins fiables. »

Comment un gouvernement/pays peut-il se préparer à des risques d'une ampleur globale et (inter) nationale ?

BQ : « Depuis une dizaine d'années, l'OTAN et l'Union européenne renforcent la résilience des États membres. La Belgique a structuré son action autour de trois plans nationaux coordonnés : défense, résilience et

'enablement'. Ce dispositif définit les mécanismes de décision et les initiatives nécessaires pour assurer la continuité de l'État, même face à des menaces multiples et simultanées. La future loi CER confiera au NCCN la responsabilité d'élaborer une stratégie globale de résilience pour les entités critiques, essentielles au fonctionnement de notre économie et de notre société. L'expertise technique des entreprises sera mobilisée pour construire des solutions opérationnelles et pratiques, ce qui peut également offrir des opportunités économiques. Parallèlement, un travail de sensibilisation sera mené auprès du grand public pour préparer chacun à faire face à divers risques, des inondations aux coupures d'électricité, renforçant ainsi la préparation collective et la continuité économique et sociétale. »

Vous faites référence au Belgian National Resilience Plan (BNR-P). Qu'est-ce que la politique attend des entreprises dans la mise en œuvre de ce plan ?

BQ : « Le Plan touche les secteurs stratégiques, par exemple : énergie, alimentation, eau potable, télécommunications et transports. Aujourd'hui, beaucoup de ces secteurs sont partiellement privatisés ou sous-traités, ce qui fait de la résilience des entreprises un élément clé pour la sécurité nationale. Les pouvoirs publics travailleront donc en concertation avec elles pour intégrer leurs contraintes opérationnelles et garantir la continuité de leurs activités. La loi CER étend également le champ des infrastructures critiques et prévoit pour les entités concernées de réaliser une 'analyse tous risques' et de mettre en place un propre plan de résilience. Cela comprendra, entre autres, l'adaptation au changement climatique, la sécurisation des chaînes d'approvisionnement et la continuité opérationnelle.

Les entreprises organiseront des exercices, renforceront leurs mesures de protection et atténueront certaines dépendances extérieures. Leur expertise technique contribuera directement à l'élaboration de solutions efficaces pour répondre à ces enjeux. Ces actions ne génèrent pas toujours un retour immédiat, mais elles sont essentielles pour la pérennité de nos entreprises et de notre économie. »

PT : « Inversement, les entreprises ont besoin d'un dialogue ouvert, d'informations claires et de conseils de la part des autorités. C'est essentiel pour garantir que les politiques tiennent mieux compte de l'ensemble des chaînes de valeur, tant en Belgique qu'à l'échelle internationale. Celles-ci sont encore trop souvent

« UNE ACTION MILITAIRE DE LA CHINE CONTRE TAÏWAN REPRÉSENTERAIT POUR NOUS LE PIRE CHOC ÉCONOMIQUE DEPUIS LA CRISE PÉTROLIÈRE DE 1973 »

Theo Francken
Ministre fédéral de la Défense
et du Commerce extérieur





»

**« L'EXPERTISE
TECHNIQUE DES
ENTREPRISES
SERA MOBILISÉE
POUR CONSTRUIRE
DES SOLUTIONS
OPÉRATIONNELLES
ET PRATIQUES »**

Bernard Quintin

Ministre fédéral de la Sécurité
et de l'Intérieur

sous-estimées. En outre, les entreprises ont besoin d'un soutien ciblé, de lignes directrices et d'une sécurité juridique pour se préparer correctement aux situations de crise, en se concentrant à la fois sur la prévention et la continuité des activités. Enfin, il est important que les autorités gardent sous contrôle le discours sur les risques actuels et potentiels. Cela peut se faire en sensibilisant les entreprises de manière proactive et en leur fournissant des informations précises et transparentes. »

BQ : « Il est en effet essentiel de créer des structures de concertation entre pouvoirs publics et entreprises pour partager connaissances, bonnes pratiques et priorités. Cela permet d'intégrer l'expertise technique, opérationnelle et financière des entreprises dans la construction et la réalisation des solutions de résilience et de défense. Des mécanismes seront mis en place pour faciliter la circulation d'informations sur les menaces et incidents, tandis que le cadre législatif sera évalué pour offrir plus de flexibilité et permettre aux entreprises d'y investir progressivement et efficacement. Cette collaboration garantit que les entreprises puissent renforcer leur résilience tout en contribuant activement à l'efficacité et à la cohérence des solutions nationales. Nos entreprises seront soutenues pour améliorer leur préparation et leur résilience. »

OPPORTUNITÉS & SOUTIEN

Mettre en place des structures de concertation et offrir de la flexibilité sont une chose... mais faut-il encore plus ?

TF : « La mission commerciale belge sur la côte ouest des États-Unis à la fin de l'année 2025 fut une expérience enrichissante, mais aussi très interpellante. Là-bas, vous observez beaucoup plus de dynamisme, d'optimisme et d'innovation que chez nous. En outre, vous pouvez voir de vos propres yeux comment les entreprises américaines s'approprient nos ingénieurs les plus talentueux. La fuite de nos cerveaux vers l'Amérique est énorme. Tout cela peut être ramené à deux facteurs. Nous avons une administration publique beaucoup trop plantureuse, entraînant une taxation beaucoup trop

élevée. Et nous avons trop d'État. Les chefs d'entreprise aspirent à une plus grande marge de manœuvre et à plus de liberté. Et je leur donne raison. »

PT : « Avant tout, les entreprises ont besoin de sécurité juridique. L'imposition de mesures top-down sans concertation préalable - par exemple, des restrictions à l'exportation, l'expropriation ou la réaffectation de lignes de production, ou des licences d'exploitation obligatoires trop strictes - a un effet contre-productif. Il est en outre essentiel de prévoir un cadre réglementaire adéquat, qui réponde vraiment aux besoins des entreprises. Pensons notamment à l'organisation de réservistes, à la nécessité de précontrats (par exemple dans le cadre des marchés publics entre les autorités et les fournisseurs privés potentiels) et aux licences obligatoires, la prudence étant de mise. Dans tous les cas, il est important que les charges administratives n'augmentent pas davantage. »

Donc, à condition d'adopter la bonne approche, les crises ne sont pas uniquement synonymes de désastre, mais offrent également des opportunités d'affaires ?

TF : « Jusqu'à récemment, l'industrie de la défense n'était pas soutenue par le gouvernement fédéral. Credendo, par exemple, n'était pas autorisé à y garantir des investissements. Cela a complètement changé. Aujourd'hui, les opportunités d'affaires et d'innovation dans le domaine de la défense peuvent être saisies. Notre plan pour l'infrastructure représente à lui seul sept milliards EUR pour la prochaine décennie. Et puis il y a les investissements régionaux qui nous permettent de remplir notre mission de plaque tournante des transports au sein de l'OTAN. Une grande partie de ces fonds peut bénéficier à notre propre industrie de la construction. Notre réarmement implique d'autres facteurs. La qualité est le paramètre décisif pour être sélectionné dans les appels d'offres. Mais si vous pouvez offrir cette qualité et que vous pouvez le faire à grande échelle, la défense peut être un partenaire commercial solide pour votre entreprise. Et n'oublions pas non plus le gigantesque marché étranger pour les entreprises belges actives dans le domaine de la défense et des biens à double usage. »

**« NOTRE PAYS POSSÈDE
UNE ADMINISTRATION
PUBLIQUE BEAUCOUP
TROP PLANTUREUSE,
ENTRAÎNANT UNE
TAXATION BEAUCOUP
TROP ÉLEVÉE »**

Theo Francken

Ministre fédéral de la Défense
et du Commerce extérieur



PT : « Le monde a changé. Notre sécurité a un prix, mais elle offre aussi des opportunités. Si nous en payons le prix intelligemment, c'est non seulement notre protection que nous achetons, mais aussi des opportunités dans de nombreux secteurs. Cela signifie un retour sur investissement pour nos entreprises et donc de la croissance économique, de la prospérité et de l'emploi. Autour du noyau d'entreprises développant des applications militaires, un écosystème plus large d'entreprises se développe. En effet, de nombreuses technologies de sécurité ont des applications civiles en plus de leurs applications militaires. Ce que nous développons aujourd'hui pour renforcer notre sécurité pourrait demain faire progresser les soins de santé, rendre la logistique plus intelligente ou accélérer la transition énergétique. »

Peut-on concilier « entreprise durable » et une économie qui repose sur un complexe militaro-industriel en pleine expansion ?

TF : « Pendant des années, les milieux financiers, académiques, politiques et économiques de Belgique et d'Europe ont boudé le secteur de la défense. Pour ce secteur, aucun projet de recherche ne pouvait être mené, aucune action n'a été achetée et aucun prêt n'a été accordé. C'était totalement 'contraire à l'éthique' selon des critères ESG élaborés par des bureaucrates en dehors de la réalité, que le monde de la finance suivait servilement. Par conséquent, le secteur a connu une traversée du désert en Belgique. Seuls les plus forts ont survécu à cette éprouvante traversée. Je qualifierais cela d'autogratisation moralisatrice. Du genre naïf, de surcroît. Et cela les a fait bien rire en Russie et en Chine. Or il n'y a rien de contraire à l'éthique dans le fait d'investir dans des entreprises de défense. Bien au contraire. Acheter des actions des entreprises de défense belges et européennes, c'est investir dans notre démocratie, notre liberté et notre sécurité. Il est temps que le monde financier s'en rende compte. En raison de ces critères ESG désastreux, l'Europe se retrouve aujourd'hui avec une base industrielle de défense trop petite et trop fragile. Pendant ce temps, des fortunes de capitaux d'investissement européens ont été dilapidées pendant des années dans des châteaux verts non

rentables, tels que les projets en matière d'hydrogène en Namibie et à Oman. Qu'on m'explique ce qu'il y avait de durable là-dedans ? »

Pour conclure, j'aimerais entendre un message positif et plein d'espoir pour la Belgique entrepreneuriale ?

BQ : « Le monde évolue rapidement et les menaces se complexifient. C'est un défi pour nos entreprises, mais aussi une opportunité sans précédent. Nous travaillerons main dans la main avec elles et soutiendrons toutes les initiatives qui renforcent la continuité et la sécurité des activités. Nous mobiliserons leur expertise pour concevoir des solutions efficaces et adaptées. Ensemble, pouvoirs publics et entreprises, nous construirons un environnement sûr et robuste, capable de protéger nos citoyens et d'assurer la stabilité et la pérennité de notre économie. »

TF : « L'Europe et l'Occident en général font souvent preuve d'un certain fatalisme. Ainsi, nous ne serions plus à même de nous mesurer à la puissance industrielle de la Chine. Néanmoins, je suis optimiste quant à la capacité de nos économies à résister aux turbulences du 21^e siècle. Nous possédons deux caractéristiques que la Chine ne possède pas : la créativité des esprits libres dans des sociétés libres et notre capacité à coopérer au-delà des frontières et des continents. Dans le domaine de l'innovation, cela nous permettra d'avoir toujours une longueur d'avance. En termes d'accès à d'autres marchés, cela confère également à nos entreprises un avantage décisif. »

PT : « L'incertitude ne doit pas être une menace. La résilience peut être planifiée. Les risques peuvent être gérés. Avec sa campagne BE PREPARED, la FEB aide les entreprises à identifier les risques, à anticiper stratégiquement les menaces, à renforcer leur résilience et à les mettre en contact avec l'expertise adéquate, et même à échanger des opportunités. Il ne s'agit pas seulement de protéger nos entreprises. Il s'agit de renforcer l'épine dorsale de notre économie, de préserver l'emploi, l'innovation et la prospérité. » 

**« L'INCERTITUDE
NE DOIT PAS ÊTRE
UNE MENACE. LA
RÉSILIENCE PEUT
ÊTRE PLANIFIÉE »**

Pieter Timmermans

CEO de la FEB