Wir fertigen das vorliegende Gesetz aus und ordnen an, dass es mit dem Staatssiegel versehen und durch das *Belgische Staatsblatt* veröffentlicht wird.

Gegeben zu Brüssel, den 25. Mai 2024

PHILIPPE

Von Königs wegen:

Die Ministerin des Innern, der Institutionellen Reformen und der Demokratischen Erneuerung,
A. VERLINDEN

Die Staatssekretärin für Asyl und Migration
N. DE MOOR

Mit dem Staatssiegel versehen:

Der Minister der Justiz
P. VAN TIGCHELT

FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER

[C − 2026/003089]

14 APRIL 2026. — Koninklijk besluit tot vaststelling van het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons voor het Belgisch grondgebied, de territoriale zee en de exclusieve economische zone

VERSLAG AAN DE KONING

Sire,

Het ontwerp van koninklijk besluit dat U wordt voorgelegd, heeft tot doel het kader voor het beheer van cybercrises te herzien om het aan te passen aan de huidige praktijken en om te waarborgen dat het plan in overeenstemming is met de bepalingen van de NIS2-richtlijn, zoals omgezet in het Belgisch recht door de NIS2-wet. Het huidige plan zal door dit ontwerp worden vervangen.

Het beheer van cybercrises wordt momenteel geregeld door het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons, dat op 28 april 2017 door de ministerraad is goedgekeurd.

Sindsdien zijn de praktijk en het juridische kader rond cyberveiligheid in België geëvolueerd. Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/114, is aangenomen. Deze richtlijn verplicht de lidstaten om autoriteiten voor het beheer van cybercrises aan te wijzen, te zorgen voor samenhang met het algemene nationale kader voor crisisbeheer en een nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons op te stellen.

Deze richtlijn werd in Belgisch recht omgezet via de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS2 wet). Om de samenhang van het beheer van cybercrises met bestaande kader voor het beheer van cybercrises in België te waarborgen, is bepaald dat het nationale plan voor cyberbeveiligingsincidenten en cybercrisisrespons formeel door U moet worden goedgekeurd bij een besluit vastgelegd na overleg in de Ministerraad.

Dit plan werd voorgelegd aan het Coördinatiecomité Inlichtingen en Veiligheid, daarna aan het Strategisch Comité voor Inlichtingen en Veiligheid, dat het op 16 oktober 2025 goedkeurde.

Dit nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons heeft tot doel een structuur te bieden om te reageren op cyberbeveiligingsincidenten en/of cyberdreigingen die een coördinatie vergen op nationaal niveau.

Het beschrijft de taken die de verschillende instanties en diensten, elk binnen de grenzen van hun wettelijke en reglementaire bevoegdheden, moeten uitvoeren in het kader van het algemene proces voor de behandeling van cyberbeveiligingsincidenten en -crises. Op die manier kunnen de betrokken partners op een gecoördineerde manier samenwerken om de vitale sectoren van ons land te beschermen tegen cyberincidenten en/of cyberdreigingen. Dit plan coördineert de aanpak van de betrokken partners, die het op hun beurt operationeel kunnen maken voor hun eigen taken.

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE

[C − 2026/003089]

14 AVRIL 2026. — Arrêté royal portant fixation du plan national de réaction aux crises cyber et incidents de cybersécurité pour le territoire belge, la mer territoriale et la zone économique exclusive

RAPPORT AU ROI

Sire,

Le projet d'arrêté royal qui Vous est soumis vise à réviser le cadre de la gestion de crise cyber afin de refléter les pratiques actuelles et afin d'assurer la conformité du plan avec les dispositions de la directive NIS2, telle que transposée en droit belge par la loi NIS2. Le plan actuellement en vigueur, sera remplacé par ce projet.

La gestion de crise cyber est actuellement encadrée par le plan national de réaction aux crises cyber et incidents de cybersécurité, approuvé par le Conseil des Ministres le 28 avril 2017.

Depuis, la pratique et le cadre juridique entourant la cybersécurité en Belgique ont évolué. La directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n°910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/114 a été adoptée. Celle-ci impose aux Etats Membres de désigner les autorités de gestion de crises cyber, d'assurer la cohérence avec le cadre national général de gestion de crise, et d'adopter un plan national de réaction aux crises et incidents de cybersécurité majeurs.

Cette directive a été transposée en droit belge au travers de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (loi NIS2). Afin d'assurer la cohérence de la gestion de crise cyber avec le cadre de gestion de crise existant en Belgique, il y est prévu que le plan national de réaction aux crises cyber et incidents de cybersécurité soit formellement adopté par Vous, par un arrêté délibéré en Conseil des ministres.

Ce plan a été soumis au Comité de coordination du renseignement et de la sécurité, puis au Comité stratégique du renseignement et de la sécurité, qui l'a approuvé le 16 octobre 2025.

Le plan national de réaction aux crises cyber et incidents de cybersécurité vise à fournir une structure pour répondre aux incidents de cybersécurité et/ou aux cybermenaces qui nécessitent une coordination au niveau national.

Il décrit les missions que les différents organismes et services, chacun dans les limites de ses compétences légales et réglementaires, doivent accomplir, le cas échéant, dans le cadre du processus global de traitement des incidents et des crises de cybersécurité. Les partenaires concernés peuvent de cette manière travailler ensemble de manière coordonnée pour protéger les secteurs vitaux de notre pays contre les incidents de cybersécurité et/ou les cybermenaces. Ce plan coordonne l'approche des partenaires impliqués, qui peuvent à leur tour le rendre opérationnel pour leurs propres tâches.

Wat het beheer van een nationale cybercrisis betreft, wordt de structuur van het algemene nationale noodplan zoveel mogelijk overgenomen in het huidige nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons. Vanwege het specifieke karakter van cyberrisico's worden echter bepaalde aanvullende elementen benadrukt. Het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons dus een specifiek nationaal plan, met name met een bijzondere structuur voor het geval van een federale fase.

Om veiligheidsredenen is de inhoud van het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons niet toegankelijk voor het publiek. Het zal echter worden meegedeeld aan alle partijen die worden vermeld in artikel 3 van het ontwerp van koninklijk besluit dat u wordt voorgelegd.

ARTIKELSGEWIJZE BESPREKING

Artikel 1

Dit artikel verklaart de definities bedoeld in artikel 9 van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid van toepassing.

Dit project maakt namelijk onlosmakelijk deel uit van het wettelijk kader dat is vastgelegd in deze wet, die de bovengenoemde richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 omzet. Het is bijgevolg absoluut noodzakelijk dat de begrippen die in het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons worden gebruikt, consistent zijn met de begrippen die in de bovengenoemde wet van 26 april 2024 worden gebruikt.

Artikel 2

Dit artikel legt het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons vast en verduidelijkt het territoriaal toepassingsgebied.

Overeenkomstig artikel 29, § 1 van de NIS2-wet, bevat dit plan ten minste de volgende elementen:

1° de doelstellingen van de nationale paraatheidsmaatregelen en -activiteiten;

2° de taken en verantwoordelijkheden van de cybercrisisbeheerautoriteiten;

3° de cybercrisisbeheerprocedures, met inbegrip van de integratie ervan in het algemene nationale crisisbeheerkader en in de informatie-uitwisselingskanalen;

4° de nationale paraatheidsmaatregelen, met inbegrip van oefeningen en opleidingsactiviteiten;

5° de relevante publieke en private belanghebbenden en betrokken infrastructuur;

6° de nationale procedures en regelingen tussen de betrokken nationale autoriteiten en instanties om de effectieve deelname van België aan het gecoördineerde beheer van cybercrises en cyberbeveiligingsincidenten op het niveau van de Europese Unie en de ondersteuning daarvan te waarborgen.

Het plan is onderverdeeld in verschillende niveaus. Voor elk niveau bepaalt het plan: de rollen en verantwoordelijkheden van de verschillende actoren, de registratie- en evaluatiemechanismen; het delen van informatie; de op te richten cellen; de communicatieketen; de afsluiting, de evaluatie en de rapportage.

Het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons is van toepassing op cyberbeveiligingsincidenten en/of cyberdreigingen op het Belgische grondgebied, in de Belgische ambassades in het buitenland, de diplomatieke en economische vertegenwoordiging van de deelgebieden, in de territoriale zee of de exclusieve economische zone, indien er mogelijke gevolgen zijn voor het Belgisch grondgebied of de Belgische bevolking, of er minstens gevolgen zijn voor Belgische organisaties.

Artikelen 3 en 4

Artikel 3 lijst de partijen op die zich moeten houden aan het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons. Dit artikel dient samen gelezen te worden met artikel 4.

In het verlengde van de wettelijke verplichtingen tot samenwerking op nationaal niveau waarin de NIS2-wet voorziet, bepaalt artikel 4 van het ontwerp van koninklijk beluit uitdrukkelijk dat onverminderd het geheim van het opsporingsonderzoek en het gerechtelijk onderzoek, respectievelijk bedoeld in de artikelen 28*quinquies* en 57 van het Wetboek van Strafvordering, of andere wettelijke bepalingen die informatie-uitwisseling beperken, de partijen (bedoeld in artikel 3) werken samen in het kader van het in artikel 2 bedoelde nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons en wisselen ze onderling op adequate wijze informatie uit over uit over cyberbeveiligingsincidenten en/of cyberdreigingen.

En ce qui concerne la gestion d'une crise cyber nationale, la structure du plan d'urgence national général est reprise dans toute la mesure du possible dans le présent plan national de réaction aux crises cyber et incidents de cybersécurité. Toutefois, en raison de la spécificité du risque cyber, certains éléments supplémentaires sont mis en exergue. Le plan national de réaction aux crises cyber et incidents de cybersécurité constitue donc un plan national spécifique, comportant notamment une structure particulière en cas de phase fédérale.

Pour des raisons de sécurité, le contenu du plan national de réaction aux crises cyber et incidents de cybersécurité n'est pas accessible au public. Il sera cependant notifié à toutes les parties visées à l'article 3 du projet d'arrêté royal qui Vous est soumis.

COMMENTAIRE DES ARTICLES

Article 1er

Cet article rend applicable les définitions visées à l'article 8 de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

En effet, ce projet fait partie intégrante du cadre juridique fixé par cette loi qui transpose la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 précitée. Il est donc impératif de maintenir une cohérence entre les notions utilisées dans le cadre du plan national de réaction aux crises cyber et incidents de cybersécurité et les notions utilisées par la loi du 26 avril 2024 précitée.

Article 2

Cet article fixe le plan national de réaction aux crises cyber et incidents de cybersécurité et précise son champ d'application territorial.

Conformément à l'article 29, § 1er de la loi NIS2, ce plan contient au moins les éléments suivants :

1° les objectifs des mesures et activités nationales de préparation ;

2° les tâches et responsabilités des autorités de gestion des crises cyber ;

3° les procédures de gestion des crises cyber, y compris leur intégration dans le cadre national général de gestion des crises et les canaux d'échange d'informations ;

4° les mesures de préparation nationales, y compris des exercices et des activités de formation ;

5° les parties prenantes et les infrastructures des secteurs public et privé concernées ;

6° les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs de la Belgique à la gestion coordonnée des crises cyber et incidents de cybersécurité au niveau de l'Union européenne.

Le plan se divise en plusieurs niveaux. Pour chaque niveau, le plan détermine : les rôles et les responsabilités des différents acteurs ; les mécanismes d'enregistrement et d'évaluation ; le partage d'information ; les cellules à mettre en place ; la chaîne de communication ; la clôture, l'évaluation ; et le rapportage.

Le plan national de réaction aux crises cyber et incidents de cybersécurité s'applique aux incidents de cybersécurité et/ou aux cybermenaces sur le territoire belge, dans les ambassades belges à l'étranger, les représentations diplomatiques et économiques dans les entités fédérées, dans les eaux territoriales ou la zone économique exclusive, ayant un impact potentiel sur le territoire ou la population belge, ou affectant au moins des organisations belges.

Articles 3 et 4

L'article 3 liste les parties soumises au plan national de réaction aux crises cyber et incidents de cybersécurité. Il doit être lu en combinaison avec l'article 4.

Dans le prolongement des obligations légales de coopération au niveau national prévues par la loi NIS2, l'article 4 du projet d'arrêté royal prévoit explicitement que, sans préjudice du secret de l'information et de l'instruction visés respectivement aux articles 28*quinquies* et 57 du Code d'Instruction Criminelle ou d'autres dispositions légales limitant le partage des informations, les parties visées par le plan (reprises à l'article 3) collaborent mutuellement dans le cadre du plan national de réaction aux crises cyber et incidents de cybersécurité visé à l'article 2 et s'échangent adéquatement entre elles les informations relatives aux incidents de cybersécurité et/ou aux cybermenaces.

Er moet namelijk voor worden gezorgd dat de betrokken overheidsinstanties toezien op de naleving van de procedures, taken en verantwoordelijkheden die in het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons zijn vastgelegd.

Om het obligatoire karakter voor de in artikel 3 bedoelde partijen te benadrukken, wordt deze verplichting formeel herhaald in artikel 4.

Gezien het ontbreken van een regelgevend karakter ten aanzien van alle Belgen, de geheimhoudingsverplichtingen voorzien in artikel 26, § 3 van de NIS2-wet, de belangen beschermd door artikel 6, § 1, 1° en 4° van de wet van 11 april 1994 betreffende de openbaarheid van bestuur en artikel 113 van het koninklijk besluit van 20 december 2024 (gevoelig niet-geclassificeerd), is het de bedoeling om het koninklijk besluit in het *Belgisch Staatsblad* te publiceren, maar zonder de bijlage die de gedetailleerde inhoud van het plan bevat. Het aangenomen koninklijk besluit en het in de bijlage opgenomen plan zullen niettemin worden meegedeeld aan de verschillende betrokken administraties, die zijn opgenomen in artikel 3 van het koninklijk besluit.

Artikel 5

Dit artikel verduidelijkt dat het nieuwe nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons, het plan dat werd vastgesteld door de Ministerraad van 28 april 2017 vervangt. Er wordt geen melding gemaakt van een intrekking, aangezien het vorige plan niet bij koninklijk besluit werd goedgekeurd.

Artikel 6

Dit artikel belast de bevoegde ministers met de uitvoering van dit besluit en behoeft geen verder commentaar.

Dit is, Sire, de draagwijdte van het besluit dat U wordt voorgelegd,

Wij hebben de eer te zijn,

Sire,
van Uwe Majesteit,
de zeer eerbiedige
en zeer getrouwe dienaars,

De Eerste Minister,
B. DE WEVER

De Minister van Veiligheid en Binnenlandse Zaken,
B. QUINTIN

---

14 APRIL 2026. — Koninklijk besluit tot vaststelling van het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons voor het Belgisch grondgebied, de territoriale zee en de exclusieve economische zone

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de Grondwet, de artikelen 37 en 108;

Gelet op de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, artikel 29, § 1;

Gelet op de wet van 15 mei 2007 betreffende de civiele veiligheid, artikel 9, § 2;

Gelet op de vrijstelling van de regelgevings-impactanalyse bedoeld in artikel 8, § 2, 1°, van de wet van 15 december 2013 houdende diverse bepalingen inzake administratieve vereenvoudiging;

Gelet op het advies van de Inspecteur van Financiën geaccrediteerd bij de Federale Overheidsdienst Binnenlandse zaken, gegeven op 25 november 2025;

Gelet op het advies van de Inspecteur van Financiën geaccrediteerd bij de Federale Overheidsdienst Kanselarij van de Eerste Minister, gegeven op 2 december 2025;

Gelet op de akkoordbevinding van de Minister van Begroting van 12 december 2025;

Overwegende het nationaal cybernoodplan dat werd goedgekeurd door de Ministerraad van 28 april 2017;

Overwegende dat wij in de huidige nationale en internationale context geconfronteerd worden met cyberbeveiligingsincidenten en cyberdreigingen; dat het daarom noodzakelijk is om onverwijld te beschikken over een adequaat noodplan dat in overeenstemming is met de ontwikkelingen op dit gebied en met de Europese en internationale richtlijnen;

Il convient, en effet, de s'assurer que les autorités publiques concernées veillent bien au respect des procédures, tâches et responsabilités définies dans le plan national de réaction aux crises cyber et incidents de cybersécurité.

Afin d'en assurer le caractère obligatoire pour les parties visées à l'article 3, cette obligation est formellement reprise à l'article 4.

Compte tenu de l'absence de caractère réglementaire à l'égard de tous les belges, des obligations de confidentialité prévues à l'article 26, § 3 de la loi NIS2, des intérêts protégés par l'article 6, § 1er, 1° et 4° de la loi du 11 avril 1994 relative à la publicité de l'administration et de l'article 113 de l'arrêté royal du 20 décembre 2024 (caractère sensible non classifié), il est prévu de publier au *Moniteur belge* l'arrêté royal, mais sans son annexe laquelle contient le contenu détaillé du plan. L'arrêté royal adopté et le plan repris en annexe seront néanmoins notifiés aux différentes administrations intéressées, reprises à l'article 3 de l'arrêté royal.

Article 5

Cet article précise que le nouveau plan national de réaction aux crises cyber et incidents de cybersécurité remplace le plan approuvé par le Conseil des Ministres le 28 avril 2017. Il n'est pas fait mention d'une abrogation car le plan précédent n'avait pas été adopté par un arrêté royal.

Article 6

Cet article charge les Ministres compétents de l'exécution du présent arrêté et ne nécessite pas d'autre commentaire.

Telle est, Sire, la portée de l'arrêté qui Vous est soumis,

Nous avons l'honneur d'être,

Sire,
de Votre Majesté,
les très respectueux
et très fidèles serviteurs,

Le Premier Ministre,
B. DE WEVER

Le Ministre de la Sécurité et de l'Intérieur,
B. QUINTIN

---

14 AVRIL 2026. — Arrêté royal portant fixation du plan national de réaction aux crises cyber et incidents de cybersécurité pour le territoire belge, la mer territoriale et la zone économique exclusive

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

Vu la Constitution, les articles 37 et 108;

Vu la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'article 29, § 1er;

Vu la loi du 15 mai 2007 relative à la sécurité civile, l'article 9, § 2;

Vu la dispense d'analyse d'impact de la réglementation, visée à l'article 8, § 2, 1°, de la loi du 15 décembre 2013 portant des dispositions diverses concernant la simplification administrative;

Vu l'avis de l'Inspecteur des Finances accrédité auprès du Service public fédéral Intérieur, donné le 25 novembre 2025;

Vu l'avis de l'Inspecteur des Finances accrédité auprès du Service public fédéral Chancellerie du Premier Ministre, donné le 2 décembre 2025;

Vu l'accord du Ministre du Budget du 12 décembre 2025;

Considérant le plan national d'urgence cyber approuvé par le Conseil des Ministres le 28 avril 2017;

Considérant que, dans le contexte national et international actuel, nous sommes confrontés à des incidents de cybersécurité et des cybermenaces; qu'il est donc nécessaire de disposer sans délai d'un plan d'urgence adéquat, conforme aux évolutions en la matière et aux directives européennes et internationales;

Overwegende dat, hoewel de territoriale zee en de exclusieve economische zone geen deel uitmaken van het nationaal grondgebied, en de Belgische Staat geen volledige soevereiniteit over deze maritieme zones heeft zoals hij die over zijn grondgebied heeft, het passend en noodzakelijk is dat dit noodplan hierop van toepassing is; dat dit geen nieuwe bevoegdheden voor België impliceert met betrekking tot de territoriale zee en de exclusieve economische zone, maar aansluit bij de bevoegdheden waarover België reeds beschikt voor deze gebieden en toelaat om deze adequaat te kunnen uitoefenen;

Overwegende dat dit noodplan in werking treedt zodra één van de daarin omschreven niveaus wordt bereikt;

Overwegende dat de betrokken actoren zich, zodra dit plan bestaat, bewust moeten zijn van hun rol en moeten toezien op de operationalisering ervan in hun interne procedures;

Op de voordracht van de Eerste Minister en van de Minister van Veiligheid en Binnenlandse Zaken, en op het advies van de in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij:

Artikel 1. Voor de toepassing van dit besluit gelden de definities als bedoeld in artikel 8 van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Art. 2. Het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons wordt vastgesteld in de bij dit besluit gevoegde bijlage.

Het plan bedoeld in het eerste lid is van toepassing op cyberbeveiligingsincidenten en/of cyberdreigingen op het Belgisch grondgebied, in de territoriale zee of de exclusieve economische zone overeenkomstig de artikelen 4 en 5 van de wet van 22 april 1999 betreffende de exclusieve economische zone van België in de Noordzee, alsook in de Belgische ambassades in het buitenland en de diplomatieke en economische vertegenwoordigingen van de deelgebieden, indien er mogelijke gevolgen zijn voor het Belgisch grondgebied of de Belgische bevolking, of er minstens gevolgen zijn voor Belgische organisaties.

Art. 3. De partijen die zich aan het in artikel 2 bedoelde plan moeten houden, zijn de volgende:

- de nationale cyberbeveiligingsautoriteit;
- het NCCN;
- het Coördinatieorgaan voor de dreigingsanalyse, opgericht bij de wet van 10 juli 2006 betreffende de analyse van de dreiging;
- de FOD Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking;
- de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (VSSE en ADIV, met inbegrip van het Cyber Command);
- de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;
- Het Openbaar Ministerie en de gerechtelijke overheden;
- de sectorale overheden;
- het Belgisch Instituut voor postdiensten en telecommunicatie;
- de gegevensbeschermingsautoriteiten;
- de Cyber Response Teams.

Art. 4. Onverminderd het geheim van het opsporingsonderzoek en het gerechtelijk onderzoek, respectievelijk bedoeld in de artikelen 28*quinquies* en 57 van het Wetboek van Strafvordering, of andere wettelijke bepalingen die informatie-uitwisseling beperken, werken de in artikel 3 bedoelde partijen samen in het kader van de uitvoering van het in artikel 2 bedoelde nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons en wisselen op adequate wijze onderling informatie uit over cyberbeveiligingsincidenten en/of cyberdreigingen.

Considérant que, bien que la mer territoriale et la zone économique exclusive ne fassent pas partie du territoire national et que l'Etat belge ne dispose pas d'une souveraineté pleine et entière sur ces zones maritimes similaire à celle exercée sur son territoire, il est approprié et nécessaire que ce plan d'urgence y soit d'application; que cela n'implique aucune nouvelle compétence de la Belgique en ce qui concerne la mer territoriale et la zone économique exclusive, mais est conforme aux compétences dont dispose déjà la Belgique dans ces zones et permet l'exercice adéquat de ces compétences;

Considérant que ledit plan d'urgence est activé dès qu'un des niveaux tels qu'y définis est atteint;

Considérant que pour ce faire, les acteurs concernés doivent, dès l'existence dudit plan, être conscients de leur rôle et veiller à l'opérationnalisation de celui-ci dans leurs procédures internes;

Sur la proposition du Premier Ministre et du Ministre de la Sécurité et de l'Intérieur, et de l'avis des Ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

Article 1er. Pour l'application du présent arrêté, les définitions visées à l'article 8 de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique sont d'application.

Art. 2. Le plan national de réaction aux crises cyber et incidents de cybersécurité est fixé en annexe du présent arrêté.

Le plan visé à l'alinéa 1er s'applique aux incidents de cybersécurité et/ou aux cybermenaces sur le territoire belge, dans la mer territoriale ou dans la zone économique exclusive conformément aux articles 4 et 5 de la loi du 22 avril 1999 concernant la zone économique exclusive de la Belgique en mer du Nord, ainsi que dans les ambassades belges à l'étranger et les représentations diplomatiques et économiques des entités fédérées, lorsqu'il y a un impact potentiel sur le territoire ou la population belges, ou que des organisations belges sont à tout le moins affectées.

Art. 3. Les parties soumises au respect du plan visé à l'article 2 sont les suivantes :

- l'autorité nationale de cybersécurité;
- le NCCN;
- l'Organe de coordination pour l'analyse de la menace, institué par la loi du 10 juillet 2006 relative à l'analyse de la menace;
- le SPF Affaires étrangères, Commerce extérieur et Coopération au Développement;
- les services de renseignement et de sécurité visés par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (VSSE et SGRS, en ce compris le Cyber Command);
- les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux ;
- le Ministère public et les autorités judiciaires;
- les autorités sectorielles;
- l'Institut belge des services postaux et des télécommunications;
- les autorités de protection des données;
- les Cyber Response Teams.

Art. 4. Sans préjudice du secret de l'information et de l'instruction visés respectivement aux articles 28*quinquies* et 57 du Code d'Instruction Criminelle ou d'autres dispositions légales limitant le partage des informations, les parties visées à l'article 3 collaborent mutuellement dans le cadre de l'exécution du plan national de réaction aux crises cyber et incidents de cybersécurité visé à l'article 2 et notamment s'échangent adéquatement entre elles les informations relatives aux incidents de cybersécurité et/ou aux cybermenaces.

Art. 5. Het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons in bijlage vervangt het nationaal cybernoodplan dat werd vastgesteld door de Ministerraad van 28 april 2017.

Art. 6. De Eerste Minister en de Minister bevoegd voor Binnenlandse Zaken en Veiligheid zijn, ieder wat hem betreft, belast met de uitvoering van dit besluit.

Gegeven te Brussel, 14 april 2026.

FILIP

Van Koningswege:

De Eerste Minister,
B. DE WEVER

De Minister van Binnenlandse Zaken,
B. QUINTIN

Bijlage. Nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons voor het Belgisch grondgebied, de territoriale zee en de exclusieve economische zone
(niet gepubliceerd)

Gezien om gevoegd te worden bij ons besluit van 14 april 2026 tot vaststelling van het nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons voor het Belgisch grondgebied, de territoriale zee en de exclusieve economische zone

Gegeven te Brussel, 14 april 2026.

FILIP

Van Koningswege:

De Eerste Minister,
B. DE WEVER

De Minister van Binnenlandse Zaken,
B. QUINTIN

Art. 5. Le plan national de réaction aux crises cyber et incidents de cybersécurité en annexe remplace le plan d'urgence national cyber fixé en Conseil des Ministres le 28 avril 2017.

Art. 6. Le Premier Ministre et le Ministre qui a l'Intérieur et la Sécurité dans ses attributions sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

Donné à Bruxelles, le 14 avril 2026.

PHILIPPE

Par le Roi :

Le Premier Ministre,
B. DE WEVER

Le Ministre de l'Intérieur,
B. QUINTIN

Annexe. Plan national de réaction aux crises cyber et incidents de cybersécurité pour le territoire belge, la mer territoriale et la zone économique exclusive
(non publié)

Vu pour être annexé à notre arrêté royal du 14 avril 2026 portant fixation du plan national de réaction aux crises cyber et incidents de cybersécurité pour le territoire belge, la mer territoriale et la zone économique exclusive

Donné à Bruxelles, le 14 avril 2026.

PHILIPPE

Par le Roi :

Le Premier Ministre,
B. DE WEVER

Le Ministre de l'Intérieur,
B. QUINTIN

FEDERALE OVERHEIDSDIENST WERKGELEGENHEID, ARBEID EN SOCIAAL OVERLEG

[C − 2025/007622]

11 JANUARI 2026. — Koninklijk besluit waarbij algemeen verbindend wordt verklaard de collectieve arbeidsovereenkomst van 1 september 2025, gesloten in het Paritair Comité voor het verzekeringswezen, tot wijziging van de collectieve arbeidsovereenkomst van 30 juni 2022 tot vaststelling van de statuten van FOPAS, het "Fonds voor de bevordering van de werkgelegenheid en de opleiding in de verzekeringssector" (1)

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de wet van 5 december 1968 betreffende de collectieve arbeidsovereenkomsten en de paritaire comités, inzonderheid op artikel 28;

Gelet op het verzoek van het Paritair Comité voor het verzekeringswezen;

Op de voordracht van de Minister van Werk,

Hebben Wij besloten en besluiten Wij:

Artikel 1. Algemeen verbindend wordt verklaard de als bijlage overgenomen collectieve arbeidsovereenkomst van 1 september 2025, gesloten in het Paritair Comité voor het verzekeringswezen, tot wijziging van de collectieve arbeidsovereenkomst van 30 juni 2022 tot vaststelling van de statuten van FOPAS, het "Fonds voor de bevordering van de werkgelegenheid en de opleiding in de verzekeringssector".

SERVICE PUBLIC FEDERAL EMPLOI, TRAVAIL ET CONCERTATION SOCIALE

[C − 2025/007622]

11 JANVIER 2026. — Arrêté royal rendant obligatoire la convention collective de travail du 1er septembre 2025, conclue au sein de la Commission paritaire des entreprises d'assurances, modifiant la convention collective de travail du 30 juin 2022 déterminant les statuts du FOPAS, le "Fonds pour la promotion de l'emploi et la formation dans le secteur de l'assurance" (1)

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

Vu la loi du 5 décembre 1968 sur les conventions collectives de travail et les commissions paritaires, notamment l'article 28;

Vu la demande de la Commission paritaire des entreprises d'assurances;

Sur la proposition du Ministre de l'Emploi,

Nous avons arrêté et arrêtons :

Article 1er. Est rendue obligatoire la convention collective de travail du 1er septembre 2025, reprise en annexe, conclue au sein de la Commission paritaire des entreprises d'assurances, modifiant la convention collective de travail du 30 juin 2022 déterminant les statuts du FOPAS, le "Fonds pour la promotion de l'emploi et la formation dans le secteur de l'assurance".