ANALYSE
DETAILLEE

EUROPEAN CYBERSECURITY ACT

ALLIANCE POUR LA CONFIANCE NUMERIQUE
WWW.CONFIANCE-NUMERIQUE.FR

Le *Cybersecurity Act*

Le 13 septembre 2017, Jean-Claude Juncker annonce dans son discours annuel sur l'état de l'Union que la protection des Européens à l'ère du numérique est une des grandes priorités de l'Union européenne. Il rappelle que 4000 attaques par rançongiciel ont été enregistrées en 2016. L'Union doit se doter de nouveaux outils pour lutter contre les cyberattaques, explique-t-il, notamment une Agence européenne de cybersécurité.

Le même jour, la Commission européenne publie son « *cybersecurity package* », un ensemble d'initiatives destinées à renforcer la résilience, dissuasion et défense de l'Union face aux cyberattaques. Parmi ces mesures, la proposition de règlement relatif à l'ENISA et à la certification des technologies de l'information et des communications en matière de cybersécurité (*Cybersecurity Act* - COM(2017) 477). Le règlement donne à l'ENISA un mandat permanent et renforce ses compétences en matière de prévention, conseil et coopération. Le *Cybersecurity Act* comporte également un deuxième volet qui vise à créer un cadre européen de certification de cybersécurité, au cœur duquel l'ENISA joue un rôle clé.

Au printemps 2019, le règlement est finalement adopté par le Parlement européen et par le Conseil de l'UE. Il devrait entrer en vigueur à la mi-2019.

Le *Cybersecurity Act* contient des dispositions qui auront un impact majeur dans le domaine de la cybersécurité en Europe, avec notamment la création de schémas européens de certification de cybersécurité. Ces schémas pourraient contribuer à la consolidation du marché unique en remédiant aux actuels problèmes de fragmentation des schémas de certification en Europe.

Le *Cybersecurity Act* en un coup d'œil

- Mandat permanent pour l'ENISA et compétences élargies, notamment en matière de certification de cybersécurité ;
- L'ENISA est en charge d'élaborer des schémas européens de certification de cybersécurité, sur proposition de la Commission ;
- Trois niveaux d'assurance assortis d'exigences différentes : élémentaire, substantiel, élevé ;
- Possibilité d'auto-évaluation de conformité pour le niveau d'assurance basique ;
- Triple rôle des autorités nationales de contrôle de certification :
    - Accréditation des organismes d'évaluation de la conformité ;
    - Contrôle de la conformité des certificats ou déclaration de conformité émis avec les exigences du schéma et du règlement ;
    - Délivrance de certificats pour le niveau d'assurance élevé, voire, dans certains cas, de moindres niveaux ;
- Certification volontaire mais la Commission établira, au plus tard en 2023, une liste des produits, services et processus couverts par un schéma de certification existant qui devraient être couverts par un schéma obligatoire ;
- Création d'un *Stakeholder Cybersecurity Certification Group,* composé de parties prenantes, pour conseiller l'ENISA en matière de certification.

La position de l'ACN sur le *Cybersecurity Act*

L'ACN a accueilli très favorablement ce texte, dont elle partage l'ambition de réduire la fragmentation du marché par le biais d'un cadre européen harmonisé de certification de cybersécurité. Néanmoins, la proposition initiale de la Commission européenne comportait de nombreuses incertitudes. L'ACN a rapidement émis une position sur ces points et a été très active tout au long du processus législatif. L'association a notamment porté plus de 20 amendements à la connaissance des eurodéputés des commissions ITRE, IMCO et LIBE.

Un système multi-niveaux adapté aux besoins du marché

L'ACN s'est prononcée en faveur d'un cadre de certification multi-niveaux adapté aux besoins du marché. Cela signifie concrètement que les domaines particulièrement sensibles doivent être soumis à un schéma de certification qui permette de garantir un niveau maximal de protection. Les produits, services et processus certifiés à ce plus haut niveau doivent ainsi être contrôlés par le biais de tests réalisés par des experts. En revanche, dans des domaines moins exposés ou moins critiques, un niveau de certification élémentaire ou substantiel, avec des exigences moindres, est suffisant et correspond mieux aux besoins du marché. Cela permet de limiter les coûts et les délais de certification pour les produits certifiés à un niveau élémentaire ou substantiel.

Dans la version finale du texte, un système multi-niveaux est effectivement mis en place avec trois niveaux d'assurance : élémentaire, substantiel et élevé (article 52). A chaque niveau d'assurance correspondent des exigences différentes en termes d'évaluation des produits, services et processus. Le niveau d'assurance basique est assorti de faibles exigences et peut même faire l'objet d'une auto-évaluation de conformité. A l'inverse, la certification d'un produit, service ou processus au niveau d'assurance élevé requiert une procédure plus exigeante et rigoureuse, qui évalue la résistance à des attaquants expérimentés.

La nécessité de conserver les acquis en termes de certification

L'association a également eu à cœur de souligner la nécessité de conserver les acquis stratégiques en termes de certification, construits depuis plus de deux décennies par l'ensemble des acteurs publics et privés de la cybersécurité. L'ACN souhaitait ainsi que les exigences du SOG-IS MRA soient intégralement reprises dans les futurs schémas de certification pour le niveau d'assurance élevé, afin d'étendre ces exigences à l'ensemble des pays européens. Une telle harmonisation serait bénéfique tant pour le dynamisme du marché intérieur que pour accroitre le niveau de cybersécurité en Europe.

Dans la version finale du texte, le SOG-IS MRA n'est pas explicitement mentionné mais le règlement établit l'obligation d'utiliser une procédure d'évaluation rigoureuse pour le niveau d'assurance élevé, avec notamment l'utilisation du *penetration testing* (article 52).

Un rôle central pour les autorités nationales de contrôle de certification

L'ACN a défendu un rôle plus prépondérant pour les autorités nationales de contrôle de certification, qui disposent de l'expertise en matière de certification de cybersécurité. L'association souhaitait ainsi que le *European Cybersecurity Certification Group* (ECCG), au sein duquel ces autorités sont représentées, ait un rôle plus important dans l'élaboration des schémas européens de certification. Selon l'ACN, le ECCG devrait ainsi avoir un pouvoir de codécision pour initier et pour valider les nouveaux schémas de certification.

Dans la version finale du texte, le ECCG se voit conférer un pouvoir d'initiative (article 48). Dans les cas dûment justifiés, il peut demander à l'ENISA de préparer un schéma de certification qui n'était pas prévu dans le programme de travail.

L'introduction d'un système de *peer review* entre autorités nationales

L'association a souligné l'importance d'avoir une approche harmonisée de la certification entre les différentes autorités nationales de contrôle. C'est la raison pour laquelle, l'introduction d'un système de *peer review* dans le texte était indispensable.

Dans la version finale du texte, un article entier (article 59) a été introduit pour établir une obligation de *peer review* entre autorités nationales de contrôle de certification. Le *peer review* concerne notamment les procédures de délivrance des certificats de cybersécurité.

L'indispensable dialogue avec les acteurs privés

L'ACN considère qu'en matière de certification le dialogue entre les représentants des entreprises de la confiance numérique et l'ENISA est essentiel. L'association a donc salué la place importante accordée à la consultation des acteurs privés dans la proposition de règlement. Néanmoins, afin d'avoir un dialogue équilibré, l'ACN a souligné qu'il était nécessaire que la participation aux instances consultatives ou aux groupes de travail soit soumise à un contrôle rigoureux.

Dans la version finale du texte, deux groupes de parties prenantes sont établis, au lieu d'un seul dans la version initiale de la proposition. Il y a, premièrement, le *ENISA Advisory Group*, qui conseille l'ENISA sur la conduite de ses activités, à l'exception des missions relatives à la certification (article 21). Un second groupe de parties prenantes, le *Stakeholder Cybersecurity Certification Group* a été introduit dans cette dernière mouture du texte (article 22). Celui-ci conseille la Commission et l'ENISA sur les points stratégiques relatifs à la certification de cybersécurité.

Principales dispositions

de la version finale du *Cybersecurity Act*

ENISA

Mandat et objectifs de l'ENISA

Le mandat actuel de l'ENISA prend fin en 2020 mais le *Cybersecurity Act* dote l'Agence d'un mandat permanent, qui en assure donc la pérennité (article 68).

Le règlement stipule que l'ENISA a pour objectif d'accroître le niveau commun de cybersécurité au sein de l'Union, notamment en soutenant activement les actions des Etats membres, institutions, organes et organismes de l'Union. En outre, l'ENISA doit contribuer à réduire la fragmentation du marché intérieur (article 3). L'ENISA se voit ainsi confier l'élaboration de schémas européens de certification de cybersécurité, tel qu'ils sont détaillés dans le Titre III du règlement, dans l'objectif notamment de réduire cette fragmentation.

Missions de l'ENISA

- **Elaboration et mise en œuvre du droit de l'Union (article 5)**

  L'ENISA :

  - prépare des avis indépendants et des travaux préparatoires concernant l'élaboration et la révision de la politique et du droit de l'Union dans le domaine de la cybersécurité. Elle fait de même pour les politiques sectorielles ayant un lien avec la cybersécurité ;
  - aide les Etats membres à mettre en œuvre de manière cohérence le politique et le droit de l'Union, notamment la Directive 2016/1148 (NIS) ;
  - facilite l'échange de bonnes pratiques entre les autorités compétentes.

- **Renforcement des capacités (article 6)**

  L'ENISA :

  - fournit aux Etats membres et aux institutions de l'Union les connaissances et l'expertise nécessaires pour améliorer la prévention, la détection et l'analyse des problèmes et incidents de cybersécurité, de même que la capacité à y réagir ;
  - soutient le renforcement des capacités des CERT nationales et de l'UE, notamment en favorisant le dialogue et l'échange d'information ;
  - organise au moins deux fois par an des exercices de cybersécurité à l'échelle de l'Union ;
  - assiste les Etats membres dans l'échange de bonnes pratiques, notamment en ce qui concerne l'identification des opérateurs de services essentiels.

- **Coopération opérationnelle au niveau de l'Union (article 7)**

  L'ENISA :

  - coopère sur le plan opérationnel et créé des synergies avec les institutions, organes et organismes de l'Union, y compris la CERT-UE, les services traitant de la cybercriminalité et les autorités de contrôle responsables de la protection de la vie privée et des données à caractère personnel, en vue de traiter des questions d'intérêt commun ;
  - assure le secrétariat du réseau des CSIRT ;
  - contribue à la coopération sur le plan opérationnel au sein du réseau des CSIRT par le soutien qu'elle apporte aux États membres ;
  - organise des exercices de cybersécurité réguliers à l'échelle de l'Union, et aide, à leur demande, les États membres et les institutions, organes et organismes de l'UE à organiser de tels exercices. Un exercice complet de grande ampleur doit être organisé tous les deux ans ;
  - contribue à des exercices de cybersécurité sectoriels ;
  - prépare, à intervalle régulier et en collaboration avec les Etats membres, un rapport de situation technique sur les incidents et menaces de cybersécurité dans l'UE ;
  - contribue à l'élaboration d'une réaction concertée au niveau de l'UE et au niveau national en cas d'incidents ou de crises transfrontières de cybersécurité majeurs.

- **Marché, certification de cybersécurité et normalisation (article 8)**

  L'ENISA :

  - soutient et promeut l'élaboration et la mise en œuvre de la politique de l'Union en matière de certification de cybersécurité des produits et services TIC, telle que décrite au titre III du règlement ;
  - facilite l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits, services et processus TIC ;
  - formule, en collaboration avec les États membres et l'industrie, des avis et des lignes directrices concernant les domaines techniques liés aux exigences de sécurité qui s'imposent aux opérateurs de services essentiels et aux fournisseurs de service numérique, et concernant les normes existantes, y compris les normes nationales des États membres, en application de l'article 19, paragraphe 2, de la directive (UE) 2016/1148 (NIS) ;
  - effectue et diffuse, à intervalle régulier, des analyses des principales tendances du marché de la cybersécurité, tant du côté de la demande que du côté de l'offre, en vue de stimuler le marché de la cybersécurité dans l'Union.

- **Connaissances et information (article 9)**

  L'ENISA :

  - analyse les technologies émergentes et fournit des évaluations thématiques sur les incidences escomptées des innovations technologiques en matière de cybersécurité du point de vue sociétal, juridique, économique et réglementaire ;
  - produit des analyses stratégiques à long terme des menaces et des incidents de cybersécurité ;
  - fournit, en coopération avec des experts des États membres and les parties prenantes, des avis, des orientations et des bonnes pratiques en matière de sécurité des réseaux et des systèmes d'information ;
  - regroupe, organise et met à la disposition du public, par l'intermédiaire d'un portail spécialisé, des informations sur la cybersécurité ;
  - collecte et analyse des informations du domaine public sur les incidents significatifs, et rédige des rapports en vue de fournir des orientations aux entreprises et aux particuliers dans toute l'Union.

- **Sensibilisation et éducation (article 10)**

  L'ENISA :

  - sensibilise le public sur les risques liés à la cybersécurité et fournit, à l'intention des particuliers et des organisations, des orientations sur les bonnes pratiques à adopter par les utilisateurs ;
  - organise à intervalle régulier, en coopération avec les États membres et les institutions, organes et organismes de l'Union, des campagnes d'information afin de relever le niveau de la cybersécurité, d'accroître sa visibilité dans l'Union et de stimuler le débat public ;
  - assiste les Etats membres dans leurs efforts pour accroitre la sensibilisation à la cybersécurité et promouvoir l'éduction en matière de cybersécurité ;
  - facilite une coordination plus étroite et l'échange de bonnes pratiques entre les Etats membres sur l'éducation et la sensibilisation en matière de cybersécurité.

- **Recherche et innovation (article 11)**

  L'ENISA :

  - conseille l'Union et les États membres sur les besoins et les priorités en matière de recherche dans le domaine de la cybersécurité ;
  - participe, lorsque la Commission lui a délégué les pouvoirs correspondants, à la phase de mise en œuvre des programmes de financement de la recherche et de l'innovation, ou est bénéficiaire de ces programmes ;
  - contribue dans le domaine de la cybersécurité à l'agenda stratégique en matière de recherche et innovation au niveau de l'Union.

- **Coopération internationale (article 12)**

  L'ENISA contribue aux efforts de l'Union pour coopérer avec les pays tiers et les organisations internationales, de même qu'avec les cadres pertinents de coopération internationales en :

  - s'impliquant, le cas échéant, en tant qu'observateur dans l'organisation d'exercices internationaux ;
  - facilitant, à la demande de la Commission, l'échange de bonnes pratiques ;
  - mettant son expertise à la disposition de la Commission si elle en fait la demande ;
  - fournissant des recommandations et de l'aide à la Commission sur les points liés aux accords de reconnaissance mutuelle des certificats de cybersécurité avec les pays tiers, en collaboration avec le Groupe de certification des Etats membres établi à l'article 53.

Gouvernance de l'ENISA (article 13)

Organe	Composition/Nomination	Missions	Durée du mandat des membres
Conseil d'administration (art. 14-18)	-Un représentant de chaque Etat membre -Deux représentants nommés par la Commission	-définir l'orientation générale du fonctionnement de l'Agence - adopter, en tenant compte de l'avis de la Commission, le document unique de programmation de l'Agence -adopter le budget annuel de l'Agence -adopter les règles relatives au fonctionnement interne de l'Agence -nommer le directeur exécutif et, le cas échéant, prolonger son mandat ou le démettre de ses fonctions	4 ans renouvelables
Conseil exécutif (art. 19)	Cinq membres nommés parmi les membres du conseil d'administration, dont son président et un représentant de la Commission.	-préparer les décisions qui doivent être adoptées par le conseil d'administration -assurer, avec le conseil d'administration, le suivi approprié des conclusions et des recommandations découlant des enquêtes de l'OLAF ainsi que des divers rapports d'audit interne ou externe et des évaluations -assister et conseiller le directeur exécutif dans la mise en œuvre des décisions du conseil d'administration relatives aux questions administratives et budgétaires	4 ans renouvelables
Directeur exécutif (art. 20 et art. 36)	Nommé par le conseil d'administration à partir d'une liste de candidats proposée par la Commission. Le directeur exécutif ne peut être démis de ses fonctions que par le conseil d'administration, sur proposition de la Commission.	-assurer l'administration courante de l'Agence -mettre en œuvre les décisions adoptées par le conseil d'administration -préparer le projet de document unique de programmation et le mettre en œuvre, une fois adopté -établir et maintenir le contact avec le secteur des entreprises et les organisations de consommateurs afin d'assurer un dialogue régulier avec les parties prenantes concernées -échanger régulièrement avec les institutions, organes et organismes de l'Union concernant leurs activités dans le domaine de la cybersécurité afin de garantir une cohérence dans l'élaboration et la mise en œuvre des politiques européennes -si besoin, créer des groupes de travail ad hoc composés d'experts, y	5 ans renouvelables une fois

		compris des experts des autorités compétentes des États membres. Le conseil d'administration en est préalablement informé.	
ENISA Advisory Group (art. 21)	Le groupe est créé par le conseil d'administration, sur proposition du directeur exécutif. Il est composé d'experts reconnus représentant les parties prenantes concernées, comme les entreprises du secteur des TIC, les fournisseurs de réseaux de communications électroniques ou de services accessibles au public, les PME, les opérateurs d'importance vitale, les organisations de consommateurs, les experts universitaires en matière de cybersécurité et les représentants des autorités compétentes notifiées au titre de la Directive 2016/0288, les organisations européennes en matière de standardisation, ainsi que les autorités chargées du respect de la loi et de la protection des données. Le groupe est présidé par le directeur exécutif ou par une personne désignée par ce dernier. Les membres du conseil d'administration ne peuvent être membres de ce groupe.	-conseiller l'Agence sur la conduite de ses activités, à l'exception de la mise en œuvre du titre III (certification) du règlement -conseiller le directeur exécutif lors de l'élaboration d'une proposition de programme de travail pour l'Agence -conseiller le directeur exécutif sur la communication avec les parties prenantes concernées pour toutes les questions liées au programme de travail	2 ans et demi
Réseau des officiers	Le Réseau des officiers nationaux de liaison est établi par le conseil d'administration,	-faciliter l'échange d'information entre l'ENISA et les Etats membres -soutenir l'ENISA dans la diffusion de ses activités, conclusions et	Non précisé dans le règlement

nationaux de liaison (art. 23)	sur proposition du directeur exécutif. Le Réseau est composé de représentants des Etats membres. Chaque Etat membre nomme un représentant.	recommandations -faciliter la coopération entre l'ENISA et les experts nationaux dans le cadre de la mise en œuvre du programme de travail	

Le *Stakeholder Cybersecurity Certification Group* (article 22)

Le *Stakeholder Cybersecurity Certification Group* n'apparait pas dans la proposition initiale de la Commission. Il s'agit d'une nouveauté introduite par le Parlement européen lors de la procédure législative.

Ce groupe est composé de membres sélectionnés parmi des experts reconnus qui représentent les parties prenantes concernées. La Commission européenne en choisit les membres, sur proposition de l'ENISA, par le biais d'un appel à candidature transparent et ouvert.

Le *Stakeholder Cybersecurity Certification Group* :

-conseille la Commission sur les points stratégiques relatifs au cadre européen de certification de cybersécurité ;

-sur demande, conseille l'ENISA sur des problèmes généraux et stratégiques concernant les missions de l'Agence relatives au marché, à la certification de cybersécurité et à la standardisation ;

-assiste la Commission dans la préparation du programme de travail multi annuel de l'Union ;

-émet une opinion sur ce programme ;

-en cas d'urgence, fournit des recommandations à la Commission et au ECCG sur la nécessité de schémas de certification additionnels qui ne sont pas prévus dans le programme de travail.

Ce groupe est co-présidé par la Commission et l'ENISA.

CERTIFICATION

Le titre III du *Cybersecurity Act* établit un cadre européen de certification de cybersécurité. Ce cadre vise à améliorer le fonctionnement du marché intérieur en élevant le niveau de cybersécurité au sein de l'Union et en offrant une approche harmonisée des schémas de certification. Il définit un mécanisme pour établir des schémas européens de certification et pour attester que les produits, services et processus TIC qui ont été certifiés conformément à ces schémas satisfont à des exigences de sécurité spécifiées.

Le *Cybersecurity Act* détaille les objectifs de sécurité des schémas européens de certification de cybersécurité (article 51), de même que les éléments d'un schéma européen de certification (article 54).

Les autorités nationales de contrôle de certification (article 58)

Chaque Etat membre désigne une ou plusieurs autorités nationales de contrôle de certification sur son territoire, ou, conformément à un accord mutuel, sur le territoire d'un autre Etat membre (article 58). Ces autorités ont un rôle clé dans l'accréditation des organismes d'évaluation de la conformité (article 60) mais également dans la délivrance des certificats, tout particulièrement pour le niveau d'assurance élevé (article 56(6)). Ces deux points seront développés ultérieurement.

En outre, les autorités nationales s'assurent, sur leur territoire respectif, que les produits, processus et services TIC certifiés satisfont effectivement les exigences associées aux certificats délivrés. Elles sont aussi en charge de veiller à ce que les fabricants ou fournisseurs qui effectuent une auto-évaluation de conformité respectent effectivement les obligations mentionnées dans le règlement. Les autorités nationales sont tenues de coopérer entre elles pour s'échanger les informations relatives aux potentielles non-conformité de processus, produits ou services avec les exigences du règlement ou du schéma.

La version finale du règlement instaure en son article 59 un mécanisme de *peer review* entre autorités nationales de certification. L'objectif est d'assurer que les certificats et déclarations de conformité correspondent effectivement aux mêmes exigences d'un Etat membre à l'autre. Le *peer review* vise notamment à garantir que les autorités nationales ont mis en place une stricte séparation des rôles et responsabilités entre leurs activités de délivrance de certificat et leurs activités de supervision.

Le European Cybersecurity Certification Group - ECCG (article 62)

Les autorités nationales de contrôle de certification prennent part au *European Cybersecurity Certification Group* (ECCG) ou Groupe européen de certification de cybersécurité. D'autres autorités nationales pertinentes peuvent également faire partie du ECCG.

Le Groupe a notamment pour mission :

- de conseiller et d'assister la Commission dans ses efforts pour assurer une mise en œuvre et une application cohérentes des dispositions du règlement, notamment en ce qui concerne le programme de travail pluriannuel ;

- d'assister, de conseiller et de coopérer avec l'ENISA en ce qui concerne l'élaboration d'un schéma candidat ;
- d'adopter un avis sur un schéma candidat ;
- de demander à l'ENISA d'élaborer un schéma européen de certification de cybersécurité candidat conformément à l'article 48(2) du règlement ;
- d'adopter des avis adressés à la Commission concernant l'actualisation et le réexamen de schémas européens de certification de cybersécurité existants ;
- de faciliter la coopération entre les autorités nationales de contrôle de la certification par le renforcement des capacités et l'échange d'informations ;
- de faciliter l'alignement des schémas européens de cybersécurité avec les normes reconnues à l'international, notamment en examinant les schémas européens existants et, le cas échéant, en recommandant à l'ENISA de discuter avec les organisations internationales de standardisation pertinentes pour répondre à des insuffisances ou des lacunes dans les standards reconnus à l'international.

La Commission préside le Groupe et en assure le secrétariat, avec l'aide de l'ENISA. Les parties prenantes intéressées peuvent être invitées à prendre part aux réunions du Groupe et à participer à son travail.

Elaboration d'un schéma européen de certification

- **Programme de travail (article 47)**

La Commission publie un programme de travail pluriannuel pour la certification européenne de cybersécurité, qui identifie les priorités stratégiques pour les futurs schémas européens de certification de cybersécurité. Le programme inclut notamment une liste des produits, services et processus ITC ou des catégories qui pourraient bénéficier d'une inclusion dans le champ d'application d'un schéma européen de certification de cybersécurité. Lors de l'élaboration de son programme, la Commission prend en compte les opinions du ECCG et du *Stakeholder Certification Group*.

Le premier programme sera publié au plus tard un an après l'entrée en vigueur du règlement. Il doit être mis à jour autant de fois que nécessaire, au moins tous les trois ans.

- **Initiative (article 48)**

Les schémas européens de certification de cybersécurité sont préparés par l'ENISA, à la demande de la Commission (dans la plupart des cas) ou du ECCG.

La Commission peut demander à l'Agence de préparer un schéma européen de certification de cybersécurité candidat ou de revoir un schéma existant sur la base du programme de travail. Dans les cas dûment justifiés, la Commission peut également demander à l'ENISA de préparer un schéma candidat ou de revoir un schéma existant alors que cela n'est pas prévu par le programme de travail (article 48).

Le ECCG dispose aussi d'un pouvoir d'initiative mais plus limité. Il peut, dans les cas dûment justifiés, demander à l'Agence de préparer un schéma candidat ou de revoir un schéma existant alors que cela n'est pas prévu par le programme de travail (article 48).

Il faut tout de même noter une différence entre l'initiative de la Commission et l'initiative du ECCG. Dans le cas où la Commission émet une demande de préparation de schéma, l'ENISA est dans l'obligation d'élaborer un tel schéma. En revanche, lorsqu'il s'agit d'une requête du ECCG, le conseil d'administration de l'ENISA peut rejeter la demande, l'Agence doit alors justifier son refus (article 49).

- **Préparation des schémas (article 49)**

Lors de l'élaboration des schémas candidats, l'ENISA consulte toutes les parties prenantes concernées par le biais d'un processus de consultation formel, ouvert, transparent et inclusif. Pour chaque schéma candidat, l'Agence établit un groupe de travail ad hoc conformément à l'article 20(4) du règlement. Ce groupe de travail fournit à l'Agence son expertise et des recommandations.

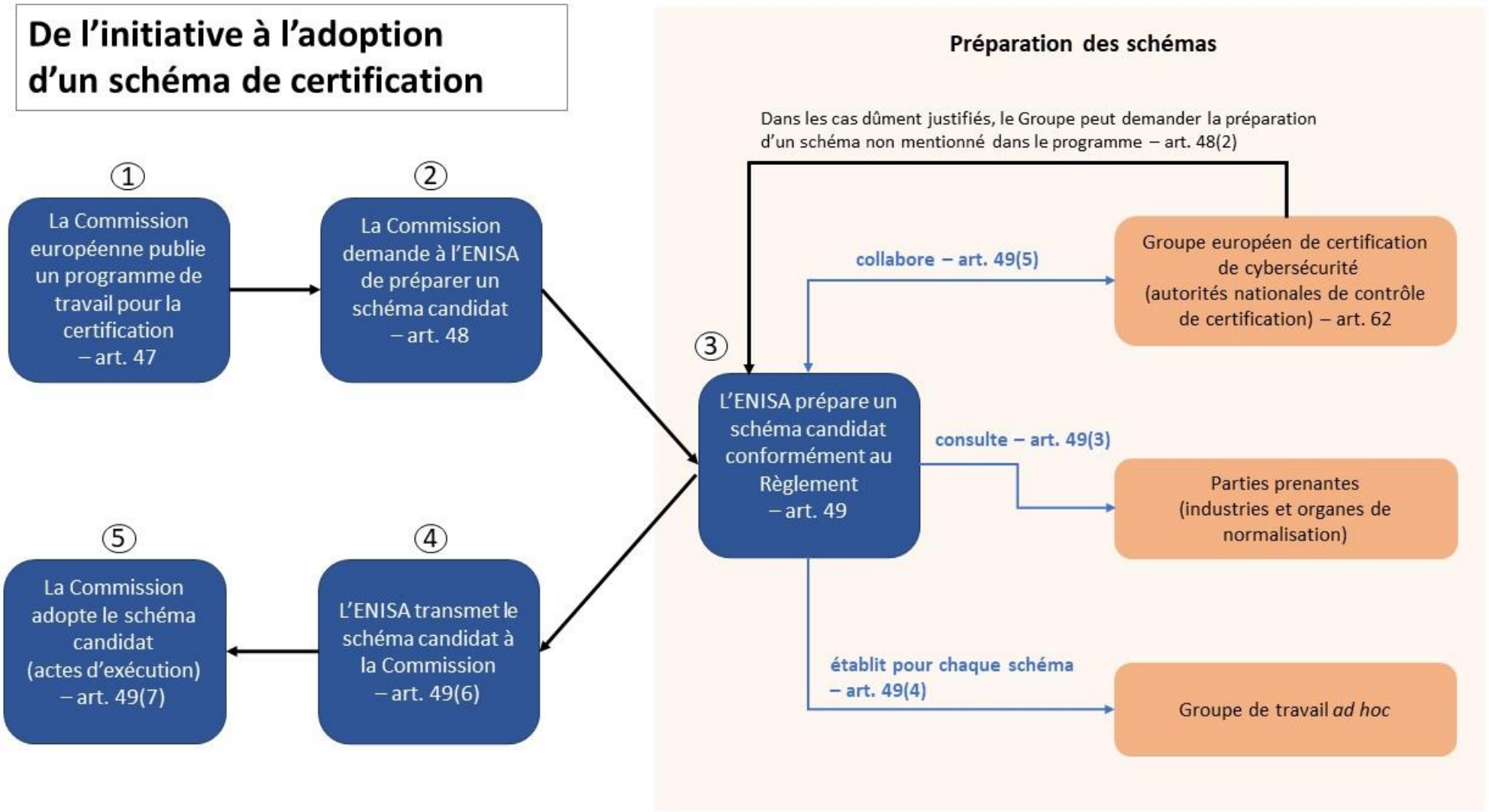
L'ENISA travaille en étroite collaboration avec le ECCG, qui fournit à l'ENISA une assistance et un avis d'expert sur la préparation du schéma candidat. L'ENISA est tenue de prendre en compte l'avis du ECCG avant de transmettre le schéma candidat à la Commission. Cet avis n'est cependant pas juridiquement contraignant.

- **Actes d'exécution (article 49(7))**

La Commission, se fondant sur le schéma candidat proposé par l'ENISA, peut adopter des actes d'exécution, qui prévoient des schémas européens de certification de cybersécurité pour les produits, services et processus TIC.

- **Evaluation et révision des schémas (article 49(8))**

L'ENISA évalue au moins tous les cinq ans les schémas européens de certification de cybersécurité adoptés en prenant en compte les retours des parties prenantes concernées. Si nécessaire, la Commission ou le ECCG demande à l'Agence de commencer le processus d'élaboration d'un schéma révisé candidat.


De l'initiative à l'adoption d'un schéma de certification
Préparation des schémas
Dans les cas dûment justifiés, le Groupe peut demander la préparation d'un schéma non mentionné dans le programme – art. 48(2)
①
La Commission européenne publie un programme de travail pour la certification – art. 47
②
La Commission demande à l'ENISA de préparer un schéma candidat – art. 48
③
L'ENISA prépare un schéma candidat conformément au Règlement – art. 49
collabore – art. 49(5)
Groupe européen de certification de cybersécurité (autorités nationales de contrôle de certification) – art. 62
consulte – art. 49(3)
Parties prenantes (industries et organes de normalisation)
établit pour chaque schéma – art. 49(4)
Groupe de travail ad hoc
④
L'ENISA transmet le schéma candidat à la Commission – art. 49(6)
⑤
La Commission adopte le schéma candidat (actes d'exécution) – art. 49(7)

Niveaux d'assurance (article 52)

Un schéma européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants : élémentaire, substantiel et/ou élevé, pour les produits, services et processus TIC certifiés dans le cadre de ce schéma. Le niveau d'assurance est proportionnel au niveau de risque, en termes de probabilité et d'impact d'un incident. Ce niveau dépend aussi de l'usage qui est fait du produit, service ou processus.

Les niveaux d'assurance élémentaire, substantiel ou élevé font référence à un certificat ou à une déclaration de conformité délivrés dans le cadre d'un schéma européen de certification. Chaque niveau d'assurance est assorti d'exigences de sécurité, notamment relatives aux fonctions de sécurité et au degré d'effort nécessaire pour l'évaluation du produit, processus ou service. Le certificat ou la déclaration de conformité se caractérise par une référence aux spécifications techniques, standards et procédures s'y afférant, notamment les contrôles techniques, dont l'objectif est de réduire le risque d'incidents de cybersécurité.

Les niveaux d'assurance élémentaire, substantiel et élevé satisfont respectivement aux critères suivants :

a) Élémentaire : un certificat européen de cybersécurité ou une déclaration de conformité UE qui atteste d'un niveau d'assurance « élémentaire » fournit l'assurance que les produits, services et processus TIC respectent les exigences de sécurité qui s'y affèrent, notamment les fonctions de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques connus de cyber-incidents ou de cyber-attaques.

→ Les activités d'évaluation comprennent au moins un examen de la documentation technique, ou à défaut, des activités de substitution à effet équivalent.

b) Substantiel : un certificat européen de cybersécurité qui atteste d'un niveau d'assurance « substantiel » fournit l'assurance que les produits, services et processus TIC respectent les exigences de sécurité qui s'y affèrent, notamment les fonctions de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les cyber-risques, cyber-incidents et cyber-attaques menés par des acteurs aux compétences et ressources limitées.

→ Les activités d'évaluation comprennent au moins :
-l'examen de la non applicabilité de vulnérabilités connues ;
-la vérification que les produits, services ou processus mettent correctement en œuvre les fonctions de sécurité ;
-à défaut, des activités de substitution à effet équivalent.

c) Élevé : un certificat européen de cybersécurité qui atteste d'un niveau d'assurance « élevé » fournit l'assurance que les produits, services et processus respectent les exigences de sécurité qui s'y affèrent, notamment les fonctions de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques de cyber-attaques de pointe menées par des acteurs dotés d'importantes compétences et ressources.

→ Les activités d'évaluation comprennent au moins :
-l'examen de la non applicabilité de vulnérabilités connues ;
-la vérification que les produits, services ou processus mettent correctement en œuvre les fonctions de sécurité avancées ;

-l'évaluation de la résistance à des attaqueurs expérimentés via le *penetration testing* ;
-à défaut, des activités de substitution.

Un schéma de certification peut préciser plusieurs niveaux d'évaluation, en fonction de la rigueur ou profondeur de la méthodologie d'évaluation. Chacun des niveaux d'évaluation correspond à un des niveaux d'assurance et est défini par une combinaison adéquate de composants d'assurance.

Auto-évaluation de conformité (article 53)

Un schéma européen de certification peut permettre que l'évaluation de conformité soit réalisée par le fabricant ou le fournisseur de produits et services. Une telle évaluation n'est possible que pour les produits et services à faible risque, qui correspondent au niveau d'assurance élémentaire.

Le fabricant ou fournisseur de produits ou services émet alors une déclaration de conformité qui indique que toutes les exigences du schéma sont respectées. Il doit garder la déclaration de conformité et la documentation technique à disposition des autorités nationales de contrôle de la certification. Une copie de la déclaration de conformité est soumise aux autorités nationales et à l'ENISA. La déclaration de conformité émise doit être reconnue dans tous les Etats membres.

Délivrance du certificat européen de cybersécurité (article 56)

Les certificats sont émis pour la période définie dans le schéma de certification et peuvent être renouvelés, à condition que les exigences soient toujours respectées. Un certificat européen de cybersécurité émis conformément à cet article doit être reconnu dans tous les Etats membres.

En ce qui concerne la délivrance du certificat européen de cybersécurité, il faut distinguer deux cas de figure : 1) celui où le certificat atteste d'un niveau d'assurance élémentaire ou substantiel, 2) celui où le certificat atteste d'un niveau d'assurance élevé.

1) Niveau d'assurance élémentaire ou substantiel

Un certificat européen de cybersécurité qui atteste d'un niveau d'assurance élémentaire ou substantiel est délivré par un organisme d'évaluation de la conformité sur la base des critères mentionnées dans le schéma.

Par dérogation à la disposition susmentionnée, dans les cas dûment justifiés, un schéma européen de certification peut disposer qu'un certificat européen de cybersécurité résultant dudit schéma ne peut être émis que par un organisme public. Un tel organisme peut être (a) une autorité nationale de contrôle de la certification ou (b) un organisme public accrédité en tant qu'organisme d'évaluation de la conformité.

2) Niveau d'assurance élevé

Dans le cas où le schéma européen de certification de cybersécurité requiert un niveau d'assurance élevé, le certificat ne peut être émis que par une autorité nationale de contrôle de la certification ou par un organisme d'évaluation de la conformité dans les conditions suivantes :

(a) Chaque certificat individuel émis par l'organisme d'évaluation de la conformité doit être préalablement validé par l'autorité nationale de contrôle de certification ;
ou
(b) L'autorité nationale de certification de cybersécurité a préalablement délégué ses missions à un organisme d'évaluation de la conformité.

Quel que soit le niveau d'assurance, le titulaire du certificat est tenu d'informer l'organisme émetteur du certificat d'une quelconque vulnérabilité détectée ultérieurement ou d'irrégularités concernant les processus, produits ou services certifiés qui pourraient avoir un impact sur les exigences liées à la certification.

De la certification volontaire à la certification obligatoire (article 56(3))

Il est explicitement stipulé dans le règlement que la certification est volontaire, sauf si la législation européenne ou nationale en dispose autrement.

Cependant, la Commission doit évaluer régulièrement, au plus tard le 31 décembre 2023 et au moins tous les deux ans par la suite, l'efficacité et l'usage des schémas de certification adoptés. La Commission doit notamment évaluer si un schéma en particulier devrait être rendu obligatoire par le biais d'une législation européenne pertinente, afin de garantir un niveau adéquat de cybersécurité et d'améliorer le fonctionnement du marché intérieur. En se fondant sur son évaluation, la Commission identifie les produits, services et processus couverts par un schéma de certification existant qui devraient être couverts par un schéma obligatoire.

La Commission doit prioritairement se focaliser sur les secteurs listés dans l'Annexe II de la Directive 2016/1148 (NIS), qui doivent être évalués au plus tard deux ans après l'adoption du premier schéma.

Les organismes d'évaluation de la conformité (article 60)

Pour chaque schéma européen de certification de cybersécurité, les autorités nationales de contrôle de la certification notifient à la Commission les organismes d'évaluation de la conformité accrédités pour délivrer des certificats aux niveaux d'assurance spécifiés. Un an après la date d'entrée en vigueur d'un schéma européen de certification de cybersécurité, la Commission publie au Journal officiel une liste des organismes d'évaluation de la conformité notifiés. Les autorités nationales sont tenues d'informer la Commission, sans délai indu, de toute modification ultérieure apportée à cette liste.

Une autorité nationale de contrôle de la certification peut présenter à la Commission une demande visant à retirer de la liste un organisme d'évaluation de la conformité notifié par l'autorité en cause. La Commission publie au Journal officiel de l'Union européenne les modifications correspondantes apportées à la liste dans un délai d'un mois à compter de la date de réception de la demande présentée par l'autorité nationale.

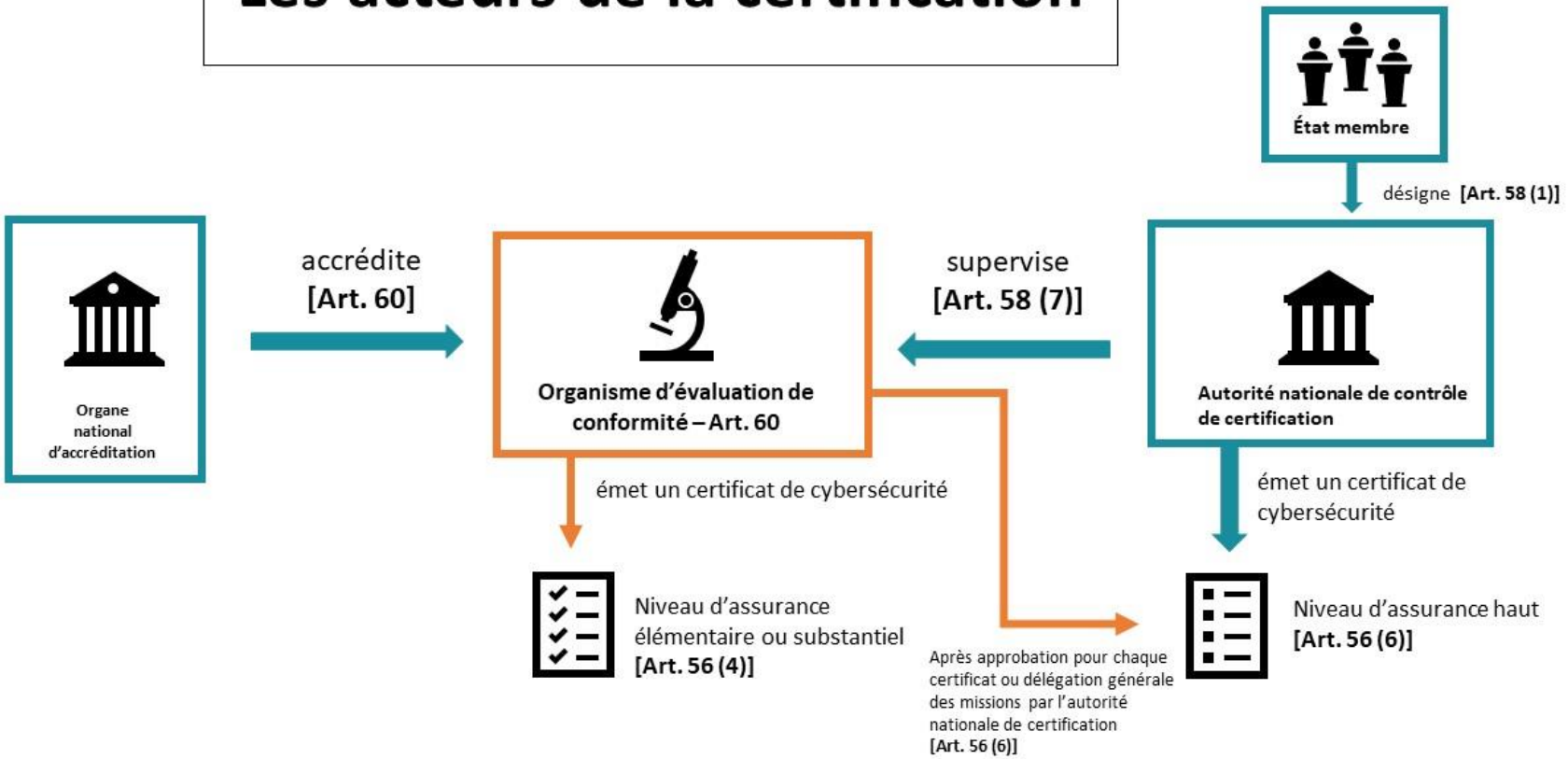
Les exigences à remplir par les organismes d'évaluation de la conformité en vue de l'accréditation sont détaillées en annexe de l'annexe du règlement. Un organisme d'évaluation de la conformité doit notamment être une entité indépendante de l'organisation ou des produits ou services TIC qu'il évalue. Néanmoins, une entité rattachée à une association ou une fédération professionnelle qui représente des entreprises impliquées dans la fabrication, l'usage ou le maintien de produits ou

services TIC peut, si son indépendance et l'absence de conflit d'intérêt sont démontrées, être considéré comme un organisme d'évaluation de la conformité.

Entrée en vigueur et mise en application du règlement (article 69)

Le *Cybersecurity Act* entrera en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne. Il commencera à s'appliquer à partir du [date à définir] sauf pour les articles 58, 60, 61, 63, 64 et 65, qui traitent des autorités nationales de contrôle de certification et des organismes d'évaluation de conformité. Ces articles commenceront à s'appliquer 24 mois après la date de publication du règlement au Journal officiel de l'Union européenne.

Les acteurs de la certification



Conclusion

Le *Cybersecurity Act* répond sans aucun doute aux enjeux contemporains de cybersécurité. Il révèle une prise de conscience de la nécessité d'avoir une Agence permanente avec des compétences élargies afin de soutenir les Etats membres et les institutions dans leurs efforts pour accroitre la cybersécurité en Europe.

Le titre III du règlement sur la certification est une réponse nécessaire aux problèmes de fragmentation du marché unique en Europe. L'ACN se félicite des trois niveaux d'assurance (élémentaire, substantiel, élevé) et des exigences en termes d'évaluation qui leur sont associées. Comme le souhaitait l'ACN, la certification à un niveau d'assurance élevé requiert l'utilisation du *penetration testing*, tandis que l'auto-évaluation est suffisante pour le niveau élémentaire. Ce système multi-niveaux correspond bien aux besoins du marché en termes de sécurité, réactivité et coûts.

En outre, la version finale du *Cybersecurity Act* donne aux autorités nationales et aux parties prenantes concernées une importance accrue. Ce point est absolument crucial car le cadre européen de certification ne peut être adapté aux réalités de l'industrie que si toute l'expertise en la matière est utilisée lors de l'élaboration des schémas européens de certification. Il était donc indispensable que le ECCG ait un pouvoir d'initiative dans les cas dûment justifiés, de même qu'une voix au chapitre lors de l'élaboration des schémas par l'ENISA. De même, l'ACN est satisfaite de la création du *Stakeholder Cybersecurity Certification Group*, qui regroupe des experts reconnus à même de conseiller l'ENISA sur les points stratégiques liés à la certification.

L'impact du *Cybersecurity Act* reste pour l'instant difficile à mesurer. Il pourrait être élevé, surtout si les fabricants et fournisseurs de produits, services et processus TIC s'emparent des schémas européens de certification. Le règlement aura des conséquences d'autant plus importantes que certains schémas de certification pourront être rendus obligatoires par la suite.

L'incertitude demeure également quant à la réelle répartition des rôles qui s'établira entre les organismes d'évaluation de la conformité et les autorités nationales de contrôles de certification. Il reste à voir à quel point ces dernières souhaiteront conserver ou non le monopole de la délivrance des certificats pour certains schémas. La situation pourrait être variable d'un Etat membre à l'autre, en fonction des choix faits par les autorités nationales. L'instauration d'un mécanisme de *peer review* est un garde-fou adéquat pour éviter que les procédures d'accréditation des organismes d'évaluation, de délivrance des certificats ou de contrôle de conformité varient trop grandement d'un Etat l'autre.

Enfin, l'impact du *Cybersecurity Act* dépend aussi en partie de la proposition de règlement établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination (COM(2018) 630). Le Centre a en effet pour mission d'accélérer les processus de normalisation et de certification, en particulier ceux liés aux schémas de certification de cybersécurité.

A propos de l'ACN

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (leaders mondiaux, PME, et ETI) du secteur de la confiance numérique notamment celles de la cybersécurité, de l'identité numérique, des communications sécurisées, de la traçabilité / lutte anti-contrefaçon et de la safe city. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur.

On dénombre environ 850 entreprises réalisant en France près de 9 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (plus de 12% de croissance chaque année depuis 2014).

Les membres de l'Alliance pour la Confiance Numérique (ACN), dont 65% de PME-ETI, représentent plus de 70% du chiffre d'affaires du secteur de la Confiance Numérique repartis sur l'ensemble de la chaine de valeur (fabricants de matériel, éditeurs de logiciels, intégrateurs, services, recherche,…).

L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication) et participe activement aux travaux du CSF (Comité Stratégique de Filière) des Industries de Sécurité, en cours de création.

Par ailleurs, l'ACN est également membre fondateur de l'ECSO (European CyberSecurity Organisation).

www.confiance-numerique.fr