Nations Unies ECE/CTCS/WP.6/2019/9

Conseil économique et social

Distr. générale
11 septembre 2019
Français
Original : anglais

Commission économique pour l'Europe

Comité directeur des capacités et des normes commerciales

Groupe de travail des politiques de coopération en matière de réglementation et de normalisation (WP.6)

Vingt-neuvième session
Genève, 20-22 novembre 2019
Point 10 b) de l'ordre du jour provisoire
Coopération internationale en matière de réglementation :
Projets sectoriels

Rapport sur l'initiative sectorielle sur la cybersécurité

Communication du secrétariat

Résumé

Le présent document contient une proposition de cadre réglementaire commun sur la cybersécurité ; il est soumis au Groupe de travail pour décision.

Décision proposée :

« Le Groupe de travail adopte la proposition de cadre réglementaire commun telle qu'elle est présentée dans le présent projet de proposition. ».

Il demande que la proposition soit publiée. Il prie également le secrétariat de continuer de rendre compte de l'état d'avancement de cette initiative.

I. Introduction

1. À sa vingt-septième session annuelle, le Groupe de travail a approuvé la proposition relative à une nouvelle initiative sectorielle sur la cybersécurité (décision 21, ECE/CTCS/WP.6/2017/2).

2. Comme suite à cette décision, un partenariat a été établi avec le Groupe de travail 17 du Bureau d'évaluation de la conformité de la Commission électrotechnique internationale (CEI) et le Système d'évaluation de la conformité des matériels et composants électrotechniques (IECEE) de la CEI, qui soutiennent activement ce projet.

3. Des débats ont eu lieu et des projets de propositions relatives à un cadre réglementaire commun sur la cybersécurité ont été présentés à des réunions du Groupe d'experts de la gestion du risque dans les systèmes de réglementation, en 2018 et 2019.

4. Le présent document décrit une méthode systématique à l'appui d'une approche systémique de la cybersécurité, dans un cadre réglementaire. Elle se distingue des autres méthodes par le fait qu'en plus de la modélisation du système technique, de la détermination et de l'analyse des risques et de l'appréciation des lacunes concernant les prescriptions, elle comprend une analyse des besoins en ce qui concerne l'évaluation de la conformité et la surveillance des marchés. Il s'agit d'une méthode souple qui est applicable à des systèmes techniques nombreux et variés dans différents secteurs de l'économie.

5. Le présent document s'inspire de l'approche fondée sur le cycle de vie, qui exige que le système technique soit convenablement inspecté, entretenu, réparé et mis à niveau. Cette approche garantit l'efficacité et l'efficience de la cybersécurité au fil du temps, à mesure que le système proprement dit évolue, de même que la nature de la menace.

6. Le présent document met en relief les éléments fondamentaux des processus réglementaires qui peuvent servir aux autorités et décideurs, particulièrement dans les secteurs qui ne disposent pas encore de réglementation en matière de cybersécurité. Y sont mentionnées plusieurs normes qui peuvent s'avérer utiles pour l'élaboration de documents de réglementation. Il s'agit d'un document en devenir, qui sera actualisé à mesure de l'évolution du cyberespace.

II. Fondements de la coopération internationale dans le domaine de la réglementation en matière de cybersécurité

7. À l'ère du numérique, la cybersécurité est un élément essentiel de la compétitivité économique et de la continuité des opérations pour tous types d'organisations.

8. Il est d'une importance capitale de garantir un niveau élevé de cyber-résilience dans le monde entier pour être à même d'assurer les services essentiels et de gagner la confiance des consommateurs dans l'environnement numérique, ainsi que d'œuvrer à l'avènement d'un monde plus sûr, innovant, compétitif, durable et prospère.

9. Le phénomène mondial des cybermenaces traverse les frontières nationales, régionales et internationales. Au nom de la cybersécurité, il est donc capital d'adopter une approche intégrée à tous les niveaux.

10. Les cybermenaces pouvant être nationales, régionales ou internationales, les pratiques exemplaires internationales sont les plus appropriées. Les normes internationales de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (CEI) sont de plus en plus adoptées par les pays qui souhaitent respecter leur obligation de réalisation des objectifs fixés par l'Organisation mondiale du commerce (OMC) en ce qui concerne les obstacles techniques au commerce, aux plans régional et national.

11. Dans la plupart des cas, l'existence ou l'utilisation de prescriptions et de procédures disparates dans des secteurs dont les domaines d'application sont réellement mondiaux et intégrés peuvent fondamentalement aggraver les risques encourus. Dans certains cas toutefois, l'application de prescriptions multiples et différentes est une façon d'atténuer les risques et de renforcer la sécurité (en évitant de reproduire les vulnérabilités).

12. Pour être efficaces, les mesures de cybersécurité sur le plan commercial et aux niveaux national et international devraient être fondées sur les résultats d'un processus de gestion des risques systémiques, et toutes les parties prenantes concernées devraient être associées au processus.

III. Objet des ORC

13. Les objectifs de réglementation communs (ORC) examinés dans le présent document ont été élaborés conformément aux recommandations L et R du Groupe de travail des politiques de coopération en matière de réglementation et de normalisation (WP.6) de la Commission économique pour l'Europe (ECE/TRADE/378 − Recommandations de la CEE sur les politiques de normalisation).

14. Les ORC ont un double objectif. D'une part, ils peuvent servir de modèle aux fins de l'élaboration de textes législatifs dans les pays qui ne disposent pas encore de réglementation dans ce secteur. D'autre part, ils peuvent servir à aligner la réglementation nationale en vigueur sur une bonne pratique harmonisée à l'échelle internationale.

15. Le présent document décrit un cadre réglementaire que les pays peuvent adopter en vue d'atteindre les objectifs réglementaires communs en matière de cybersécurité. Il peut servir de base pour :

- Établir des objectifs de réglementation en matière de cybersécurité ;
- Déterminer et évaluer les risques en matière de cybersécurité ;
- Définir quelles normes internationales peuvent être appliquées pour mettre au point la réglementation en matière de cybersécurité ;
- Définir des procédures d'évaluation de la conformité en matière de cybersécurité ;
- Mettre en place un processus de surveillance des marchés.

16. Les pays qui souhaitent établir des procédures spéciales interétatiques peuvent mettre à profit les ORC en suivant le processus défini dans l'annexe C de la recommandation L.

17. Les autorités compétentes peuvent appliquer le modèle décrit dans le présent document à leur cadre réglementaire national pour certains secteurs et applications essentiels, ou exiger que les acteurs commerciaux intervenant dans le cadre de ces mêmes secteurs et applications, ou d'autres, l'utilisent pour faire dûment la preuve de la conformité. L'évaluation de la conformité par un tiers ne devrait être exigée qu'en cas de besoin, en fonction des résultats de l'analyse des risques.

18. L'application du cadre réglementaire commun permettra :

- De promouvoir une législation harmonisée à l'échelle mondiale ;
- De promouvoir une législation proportionnée aux risques qu'il est prévu de prendre en compte ;
- De garantir l'acceptation réciproque des procédures d'essai et d'évaluation et des résultats entre les laboratoires d'essai ; et
- D'œuvrer à mettre en place des procédures cohérentes et comparables pour l'évaluation et l'application des mesures de cybersécurité.

19. De plus, l'application du présent document permettra de promouvoir la convergence des réglementations techniques nationales déjà en place ou à mettre en place dans ce secteur, dans l'optique d'établir un cadre commun reposant sur une approche fondée sur le risque et s'inspirant d'autres pratiques exemplaires internationales. On pourra, ce faisant, réduire les obstacles au commerce de composants, de matériel, de personnel qualifié et de services, favoriser la concurrence, élargir les options disponibles sur le marché et diminuer les coûts.

IV. Objectifs de réglementation communs en matière de cybersécurité

20. Le cadre de réglementation en matière de cybersécurité a pour objet de favoriser le bien-être général et la prospérité globale des citoyens en garantissant :

a) La protection des données ;

b) La fiabilité des systèmes ;

c) La continuité des activités ;

d) La sûreté ; et

e) La sécurité

s'agissant des infrastructures critiques telles que les installations de fourniture d'électricité et d'eau salubre, de traitement des eaux usées, ainsi que d'approvisionnement en gaz et en carburant, les réseaux bancaires, les systèmes de santé, les infrastructures de transport et les autres services essentiels, tels qu'ils sont décrits ou définis dans la section V du présent document (énoncé des ORC).

21. Les autorités chargées de la réglementation de secteurs particuliers peuvent s'inspirer de ces ORC dans l'optique d'harmoniser la réglementation à l'échelle internationale afin d'élaborer une législation sectorielle en matière de cybersécurité et ainsi d'éviter au maximum d'avoir recours à d'éventuelles prescriptions spéciales au motif des risques propres aux différentes situations nationales.

22. Les objectifs de réglementation devraient être établis en gardant à l'esprit que le risque zéro n'est pas un objectif réalisable. Il convient donc de définir un niveau de risque et d'appétence pour le risque acceptable, en s'inspirant de la recommandation R.

V. Énoncé des objectifs de réglementation communs

23. Les ORC sont remplacés par des régimes réglementaires spéciaux lorsque de tels régimes existent ou sont en cours d'établissement.

24. Les produits et processus visés par les ORC sont :

- Les applications physiques, qui relèvent des systèmes de technologies d'exploitation, telles que les infrastructures critiques et les systèmes intelligents, ainsi que les processus qui permettent de garantir le fonctionnement de ces systèmes (tels que ceux qui sont visés par la série CEI 62443 de normes internationales) ; et
- Les systèmes d'information, qui relèvent des systèmes de technologies de l'information et dont les données doivent être protégées et les flux d'information sécurisés (tels que ceux qui sont visés par la série ISO/CEI 27000 de normes internationales).

25. Les ORC portent sur les prescriptions applicables aux technologies employées dans les différents systèmes, notamment :

a) Les données, la connectivité, les composants, le matériel, les applications et les services ;

b) Les compétences et qualifications du personnel ; et

c) La gestion des processus, à savoir :

i) La conception des composants ; et

ii) L'intégration, la réalisation, le fonctionnement, l'entretien et la mise à niveau des systèmes, entre autres choses.

26. Il serait utile d'utiliser un modèle de matrice générique pour définir tous les composants des systèmes techniques (annexe A).

VI. Définition des risques en matière de cybersécurité

27. Les risques en matière de cybersécurité sont des incidents ou événements qui peuvent avoir un effet sur la réalisation des objectifs de cybersécurité, tels qu'ils ont été définis ci-dessus. Si les risques génériques et les risques particuliers sont clairement définis, on est à même de bien les évaluer et de prévoir des mesures de contrôle afin de maintenir ces risques à un niveau acceptable.

28. On trouvera ci-après une liste de normes internationales et autres cadres relatifs à la cybersécurité qui peuvent être appliqués pour définir les risques en matière de cybersécurité :

- Série ISO/CEI 27000 de normes ;

- Série CEI 62443 de normes ;
- Série ISO 31000 de normes ;
- Cadre v1.1 du National Institute of Standards and Technology (NIST) ;
- Banque des règlements internationaux (BRI) – Bâle II/III, risque opérationnel ;
- Objectifs de contrôle de l'information et des technologies associées (COBIT 5) ; et
- Open Web Application Security Project − (OWASP)-Top 10.

29. De toute évidence, la cyberprotection doit reposer sur une démarche globale et applicable à l'ensemble du système.

30. Le modèle de matrice générique (voir annexe A) peut servir à déterminer les points pour lesquels il convient de définir et d'évaluer les risques en matière de cybersécurité.

31. Lorsqu'on définit les risques en matière de cybersécurité, il convient de prendre en compte les facteurs suivants (voir le « modèle fondé sur les menaces » à l'annexe B, dans lequel sont décrits les motifs et les scénarios potentiels associés aux différents risques qui sont susceptibles de se matérialiser dans un système technique, dont une liste est fournie ci-dessous à titre d'exemple) :

- Cyberactivisme ;
- Cybercriminalité ;
- Menaces de l'intérieur ;
- Cyberespionnage ;
- Cyberterrorisme ;
- Cyberguerre ;
- Autres.

Voir l'annexe B pour une liste détaillée des facteurs et leur description (actuellement en cours d'élaboration).

32. Parmi les risques en matière de cybersécurité et les vulnérabilités connexes, on peut citer les exemples suivants :

i. Perte de données ou accès non autorisé à des données, ou non-respect de la réglementation (règlement général sur la protection des données ou autres règlements sur les données) ;

ii. Perturbation de l'accès ou accès non autorisé au système ou aux applications ;

iii. Défaillance d'un système ancien ou insuffisance du service ;

iv. Perte de service d'un fournisseur tiers ;

v. Surcharge du système (panne) imputable à une attaque provenant de l'extérieur ou à une surexploitation ;

vi. Contamination accidentelle du système par un virus ;

vii. Manque de connaissances chez les personnes chargées d'administrer les systèmes anciens ou d'anticiper les besoins actuels et futurs ;

viii. Insuffisance des compétences dont disposent les décideurs pour définir et élaborer une stratégie afin de mettre à profit les possibilités des cybertechnologies (telles que l'informatique en nuage).

33. Les autorités de réglementation devraient surveiller l'évolution des menaces pour la cybersécurité, sachant qu'on ne peut plus anticiper la totalité des risques à venir en se fondant sur l'étude des événements passés.

VII. Évaluation des risques en matière de cybersécurité

34. Lorsque cela est possible, il convient de quantifier les risques en matière de cybersécurité pour qu'ils puissent être traités par ordre de priorité et évalués compte tenu du niveau de risque acceptable, tel que celui-ci est décrit dans la recommandation R.

35. Il est entendu que les risques en matière de cybersécurité ne peuvent pas être éliminés complètement et qu'un niveau de risque acceptable doit être défini.

VIII. Définition de prescriptions réglementaires relatives aux risques en matière de cybersécurité et spécification de normes internationales permettant d'établir la présomption de conformité

36. Lorsqu'il s'agit de définir des prescriptions réglementaires, la recommandation R du Groupe de travail WP.6 de la Commission économique pour l'Europe (CEE), intitulée « Gestion du risque dans les cadres réglementaires », devrait être utilisée par les organismes de réglementation pour assurer la cohérence et la proportionnalité entre les risques existants en matière de cybersécurité et les prescriptions réglementaires.

37. Les principes de base de la cybersécurité sont bien documentés et régulièrement mis à jour en fonction des progrès des normes internationales. On peut citer à titre d'exemple les séries CEI 62443 et ISO/CEI 27000 de normes internationales.

38. Les pays utilisent les normes dans leurs réglementations de différentes manières, notamment :

- En renvoyant à ces normes dans les textes législatifs ; et
- En faisant du respect des normes un moyen de prouver la conformité aux prescriptions essentielles énoncées dans la législation ; selon cette approche, le matériel, les qualifications du personnel, les services, les pratiques et les processus qui sont conformes aux dispositions des normes sont « réputés conformes » aux prescriptions réglementaires.

39. La détermination des risques et l'analyse de différents systèmes dans différentes situations conduiront à des besoins différents en matière de prescriptions. Les prescriptions réglementaires seront fondées sur des normes internationales comme celles de la CEI et de l'ISO ou, en l'absence de telles normes, sur des normes régionales, ou enfin sur des normes nationales. En l'absence de normes, les prescriptions peuvent être fondées sur les meilleures pratiques et procédures acceptées par le marché.

40. On trouvera dans le présent document des exemples de normes qui peuvent servir à établir la présomption de conformité avec les prescriptions réglementaires pertinentes. Cette liste de normes doit être fréquemment mise à jour, en fonction de la publication des normes internationales CEI ou ISO/CEI se rapportant aux objectifs du présent règlement type.

41. À défaut de normes internationales, il convient d'appliquer des normes régionales ou nationales pour l'élaboration de prescriptions réglementaires.

Prescriptions relatives aux composants, aux produits et au matériel

42. Les prescriptions relatives aux composants, aux produits et au matériel utilisés en tant qu'éléments d'un système peuvent être fondées sur des normes internationales comme celles de la CEI et de l'ISO, parmi lesquelles :

i. CEI 62443-1-1, 2e éd. : Terminology, concepts and models (en cours de mise à jour) ;

ii. CEI 62443-2-1, 2e éd. : Establishing an industrial automation and control system security program (en cours de mise à jour) ;

iii. CEI 62443-2-3 : Patch management in the IACS environment (adoptée) ;

iv. CEI 62443-2-4 : Exigences de programme de sécurité pour les fournisseurs de service IACS (adoptée) ;

v. CEI 62443-2-2 : IACS protection levels (en cours d'élaboration) ;

vi. CEI 62443-3-2 : Évaluation des risques de sécurité et conception des systèmes (en cours de mise à jour) ;

vii. IECEE OD-2061 : Industrial Cyber Security Program ;

viii. CEI 62443-4-1 : Exigences applicables au cycle de vie de développement sécurisé des produits (adoptée) ;

ix. CEI 62443-3-3 : Exigences de sécurité des systèmes et niveaux de sécurité (adoptée) ; et

x. CEI 62443-4-2 : Exigences de sécurité technique des composants IACS (en cours de mise à jour).

43. On trouvera la liste complète des normes pertinentes sur le site Web de l'initiative.

44. La production de matériel devra être fondée sur la liste en question.

Prescriptions relatives aux compétences personnelles

45. Les prescriptions relatives aux compétences personnelles devront être fondées sur les normes internationales ISO et CEI existantes dans ce domaine, par exemple :

- La norme ISO/CEI 27021, 1re éd. : Information technology − Security techniques − Competence requirements for information security management systems professionals.

Prescriptions relatives aux processus

46. Les prescriptions relatives aux processus devront être fondées sur les normes internationales ISO et CEI applicables, telles que les suivantes :

i. CEI 62443-4-1 : Exigences applicables au cycle de vie de développement sécurisé des produits (adoptée) ;

ii. CEI 62443-2-1 : Establishing an IACS security program ;

iii. CEI 62443-2-2 : IACS protection levels (en cours d'élaboration) ;

iv. CEI 62443-2-4 : Exigences de programme de sécurité pour les fournisseurs de service IACS (adoptée) ; et

v. CEI 62443-3-2: Évaluation des risques de sécurité et conception des systèmes (en cours de mise à jour).

IX. Détermination du niveau d'évaluation de la conformité

47. La convergence vers une méthode commune fondée sur des normes internationales harmonisées et sur les meilleures pratiques internationales en matière d'évaluation de la conformité présente plusieurs avantages. Entre autres, lorsque l'évaluation de la conformité par une tierce partie est utilisée pour établir la conformité des composants et de la technologie ainsi que des compétences et des qualifications du personnel, la reconnaissance de cette conformité dans le commerce international et la circulation des personnes qualifiées s'en trouve facilitée.

48. Les ORC sont élaborés compte tenu des normes et des méthodes d'évaluation de la conformité internationales, telles que celles élaborées par la CEI et l'ISO, ainsi que des pratiques exemplaires en matière d'évaluation de la conformité à ces normes, par exemple dans le cadre de l'IECEE et du système d'évaluation de la qualité des composants électroniques de la CEI (IECQ).

49. Les pays devraient employer une méthode systématique pour déterminer un niveau approprié d'évaluation de la conformité en fonction du risque. Il est évident que, dans une approche systémique, des formes de protection plus ou moins contraignantes sont appropriées ; partant, des modalités plus ou moins contraignantes sont également indiquées s'agissant de vérifier que les exigences de protection ont été respectées.

50. Le niveau d'évaluation de la conformité qui devrait être appliqué aux prescriptions sera déterminé au moyen d'une évaluation des risques qui se traduira par une notation des risques pour chaque point du modèle de matrice générique (annexe A). L'analyse de différents systèmes (voir exemples dans l'annexe C) dans différentes situations conduira à différentes notations des risques. Les points de valeur élevée, tout comme les points de vulnérabilité élevée, se traduiront par des niveaux plus élevés d'évaluation de la conformité tandis que les points de valeur et de vulnérabilité plus faibles conduiront à des niveaux inférieurs d'évaluation de la conformité.

51. Il est donc évident qu'une approche globale de la cybersécurité devrait être neutre en ce qui concerne l'évaluation de la conformité et devrait tenir compte des différentes modalités d'évaluation − évaluation de la conformité par la première partie, la deuxième partie et la troisième partie − selon les différents niveaux de risque déterminés pour les divers éléments du système à protéger.

52. Lorsque l'analyse des risques conclut que l'évaluation de la conformité par une tierce partie est appropriée, les meilleures pratiques internationales et les services de certification mondiale tels que ceux offerts par l'IECEE et l'IECQ peuvent, lorsque ceux-ci sont disponibles et pertinents, donner des indications précieuses.

Définition des procédures applicables en matière d'évaluation de la conformité

53. La conformité des produits et processus dans le cadre de la réglementation applicable en matière de cybersécurité sera vérifiée à l'aide d'un mécanisme approprié d'évaluation de la conformité aux prescriptions indiquées dans l'application spécifique telle que déterminée par le processus décrit dans la partie VIII du présent document.

54. Lorsque la conformité doit être évaluée par une tierce partie, le respect du présent ORC par les autorités de réglementation peut être évalué à l'aide d'un système international de certification tel que l'IECEE et l'IECQ pour l'acceptation directe sur le marché des produits, personnes, services et organisations certifiés par ces organismes. Sinon, dans les pays où la législation ne permet pas le recours à des certificats de l'IECEE ou de l'IECQ, il est recommandé aux autorités de réglementation de s'employer à obtenir une certification nationale de la conformité fondée sur les essais, les inspections et les évaluations prévus dans le cadre des organismes susmentionnés.

Reconnaissance des organes d'évaluation de la conformité

55. La qualification des organes d'évaluation de la conformité et des laboratoires d'essai doit être conforme aux normes internationales ISO/CEI applicables (voir ci-dessous). Les organes d'agrément sollicités doivent être membres de la Conférence internationale sur l'agrément des laboratoires d'essai et du Forum international de l'accréditation. Au moins un des membres de l'équipe d'évaluateurs doit posséder des compétences correspondant aux prescriptions pertinentes en matière de cybersécurité (voir par exemple la liste des évaluateurs agréés de l'IECEE et de l'IECQ).

56. Les certificats doivent être conformes aux prescriptions relatives au type de système correspondant, telles qu'indiquées dans la norme ISO/CEI applicable (voir ci-dessous).

57. Le recours aux systèmes d'évaluation de la conformité, tels que ceux de l'IECEE et de l'IECQ, permet d'établir la présomption de conformité aux prescriptions énoncées dans la partie VIII du présent document. S'ils sont portés à l'attention de l'initiative, d'éventuels autres mécanismes pourront être qualifiés de références dans une future version des ORC.

58. Ainsi, lorsque la conformité doit être évaluée par une tierce partie, le recours à un mécanisme de certification reconnu à l'échelle internationale, tel que celui de l'IECEE ou de l'IECQ, peut permettre de réduire les coûts inutiles liés à la répétition des inspections, évaluations et essais et au chevauchement des compétences.

Normes d'évaluation de la conformité

59. ISO/CEI 17065, ISO/CEI 17021, ISO/CEI 17024, ISO/CEI 17025 et ISO/CEI 17040.

Notions fondamentales de la certification des produits

60. ISO/CEI 17067.

X. Établissement de procédures de surveillance des marchés

61. Le dernier volet, par ailleurs essentiel, du présent document est celui de la surveillance des marchés. Cette surveillance est nécessaire si l'on veut pouvoir s'assurer de la bonne réalisation des ORC par les professionnels et renforcer la confiance dans l'efficacité de ces objectifs. Des lignes directrices communes seront élaborées pour aider les autorités nationales à définir et à mettre en œuvre des mesures et des procédures pertinentes, notamment pour retirer du marché national des composants et des produits non conformes.

62. La planification des mécanismes de surveillance des marchés devrait être fondée, entre autres, sur la recommandation S du WP.6 relative à l'application d'outils de gestion prédictive du risque à la surveillance ciblée des marchés.

63. En ce qui concerne les cas de non-conformité critique, un système international d'alerte devrait être mis en place pour être à même d'informer tous les États Membres des Nations Unies des risques récemment détectés.

64. Sous réserve d'un examen approprié effectué par les organes de gestion et de gouvernance de la CEE, il est prévu de créer un réseau d'experts de la surveillance des marchés spécialisés dans la cybersécurité pour surveiller la conformité aux prescriptions du présent règlement type sur les marchés.

XI. ORC − Partie 7 : Comité directeur de la cybersécurité de la CEE

65. Sous réserve d'un examen approprié effectué par les organes de gestion et de gouvernance de la CEE, il est prévu de constituer un comité directeur de la cybersécurité de la CEE, qui sera placé sous l'égide du WP.6 et dont la tâche consistera à suivre la réalisation des ORC dans les pays qui auront fondé leur législation nationale sur le règlement type de la CEE et à actualiser ce règlement au regard de l'expérience acquise.

66. Le Comité directeur adopte des statuts et d'autres règles et procédures de fonctionnement (modalités de vote, par exemple).

67. Le Comité directeur fait rapport aux membres du Groupe de l'acceptation des normes de la CEE.

68. Les membres du Comité directeur de la cybersécurité qui ont le droit de vote sont les représentants des pays qui appliquent le règlement type. Peuvent également participer aux réunions en qualité d'observateurs les représentants du Conseil de gestion de la normalisation de la CEI, du Bureau d'évaluation de la conformité de la CEI, des Comités techniques compétents de la CEI, des systèmes d'évaluation de la conformité de la CEI et du Groupe consultatif de la surveillance des marchés de la CEE. Les conseillers qui participent à des activités de réglementation déjà en cours dans le domaine de la cybersécurité sont invités à rejoindre le Comité directeur à titre consultatif (responsables du WP.29 et membres du secrétariat, par exemple).

Annexe A

Explication du modèle de matrice générique

1. Le modèle de matrice générique est un outil utilisé pour modéliser un système technique, puis pour comparer ce modèle avec certains objets (ou les éléments dont la conformité peut effectivement être évaluée au regard des prescriptions). Le modèle de matrice générique est généralement représenté sous la forme d'une matrice, le système étant modélisé verticalement sur le côté gauche et les objets à évaluer énumérés horizontalement en haut.

2. Dans une représentation graphique du modèle de matrice générique, des lignes horizontales sont tracées à partir des éléments du système modélisé à travers la page, sous les objets à évaluer. De même, des lignes sont tracées verticalement vers le bas à partir de ces objets.

3. Le modèle de matrice générique peut être utilisé pour déterminer ce qui est important pour un système technique donné lorsqu'on le considère sous un angle particulier. Cela permet de déterminer les éléments et sous-éléments les plus importants qui devraient être visibles sous cet angle et qui devraient donc être apparents dans le système modélisé. Lorsque l'on examine la question de la cybersécurité de la sorte, le système peut être modélisé avec des éléments tels que la technologie ou les composants, les interconnexions, les interventions, les zones de sécurité, les tests d'intrusion, etc.

4. En général, les prescriptions qui encadrent une évaluation de la conformité sont des pratiques exemplaires, des qualifications, des spécifications, des normes ou le résultat minimal ou maximal de tests normalisés, etc. Pour satisfaire aux prescriptions, il peut également être nécessaire de disposer d'un certain type ou niveau de matériel, de savoir-faire, de qualifications, de compétences, d'expérience, etc.

5. L'acte consistant à effectuer une évaluation pour vérifier le respect des prescriptions est un acte d'évaluation de la conformité aux prescriptions en question. La dénomination officielle de cette opération est « évaluation de la conformité ». On dénombre essentiellement trois objets possibles dont la conformité peut être évaluée : les produits, les personnes (compétences) et les processus.

6. Il s'agit là des trois principaux objets de l'évaluation de la conformité. De nombreux autres objets ont été proposés, tels que les services, les données, les installations, les projets, les organismes ou organisations, les systèmes et les facteurs externes. Mais en réalité, chacun d'entre eux correspond simplement à l'un des trois principaux objets ou à une combinaison des trois. Par exemple, les services ne sont essentiellement que des processus, exécutés par des personnes (possédant les compétences requises), éventuellement à l'aide de produits ou d'un matériel appropriés. Aucun autre objet ne peut concrètement être retenu. Ainsi, les services relèvent déjà d'un des trois principaux objets de l'évaluation de la conformité, ou plus, et n'ont pas besoin de s'inscrire dans une catégorie qui leur soit propre.

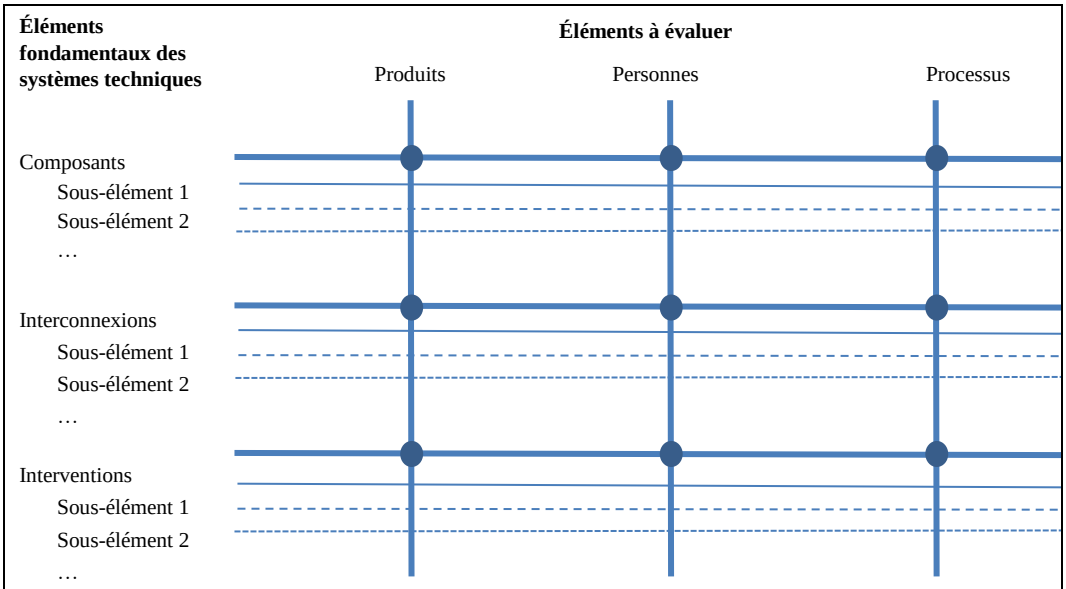
7. Cela étant dit, s'il est utile pour un secteur que soient indiqués d'autres objets en sus des trois principaux objets, alors le ou les objets supplémentaires doivent être ajoutés au modèle de matrice générique considéré.

8. C'est aux points d'intersection entre les éléments du système modélisé et les objets à évaluer que les prescriptions peuvent être appliquées. Une analyse des lacunes permettra de déterminer quelles sont les prescriptions et si elles existent.

9. Il faut d'abord comprendre le système et savoir où se trouve la valeur et où se trouvent les vulnérabilités, puis procéder à une évaluation des risques à chacun des points d'intersection pour déterminer quel type d'évaluation de la conformité est nécessaire par rapport aux exigences de chaque point. L'évaluation des risques doit donc être réalisée à la lumière de la partie VII du présent document. Les points d'intersection de grande valeur ou de grande vulnérabilité nécessiteront une évaluation de la conformité plus rigoureuse,

tandis que les points de faible valeur ou de faible vulnérabilité nécessiteront une évaluation de la conformité moins stricte. Il conviendrait que l'ensemble des options en matière d'évaluation de la conformité soient disponibles pour un usage approprié. Il s'agit là de l'évaluation de la conformité par une première partie, telle que la déclaration de conformité d'un fabricant ou d'un fournisseur ; de l'évaluation de la conformité par une deuxième partie, comme les auto-évaluations et les audits internes effectués par l'utilisateur ou le propriétaire du système ; et de l'évaluation de la conformité par une tierce partie, comme les essais de type 1 (ISO/CEI 17067) ou les essais de type 5, la certification complète de la conformité, etc. La plupart des réglementations devraient être neutres du point de vue de l'évaluation de la conformité et ne préciser que ce qui est approprié en fonction des résultats de l'analyse des risques.

10. Les points d'intersection verticaux et horizontaux du modèle de matrice générique sont les points d'intersection où se fait l'évaluation de la conformité, et l'approche systémique est la matrice globale des exigences et des activités d'évaluation de la conformité.



Modèle générique de l'approche systémique de l'évaluation de la conformité (forme la plus simple)

Qu'est-ce qu'un système technique ?

11. Un système technique n'est pas un système naturel comme un système biologique, par exemple le système circulatoire sanguin, ou un système environnemental, par exemple le système météorologique, ou encore un système céleste, par exemple le système solaire, etc. Un système technique est un système artificiel.

12. Le point commun entre les systèmes ferroviaires, l'informatique en nuage, les réseaux intelligents, les systèmes de contrôle industriels, une centrale nucléaire et un système de distribution d'électricité, une raffinerie de pétrole, un système de distribution de gaz, un système bancaire et financier, un système d'information sanitaire, des maisons intelligentes, etc., est que tous ces éléments sont des systèmes techniques.

13. Maintenant, si l'on considère qu'un système technique est :

- Un groupe d'éléments interactifs, étroitement liés ou interdépendants formant un tout cohérent ;
- Et que ces éléments peuvent être d'ordre procédural, physique et/ou virtuel ;
- Et que ces éléments peuvent être des composants qui doivent être conçus et fabriqués ou créés ;

- Et que le système proprement dit sera conçu et fabriqué (ou intégré dans des systèmes) et que les éléments du système peuvent être confinés dans un emplacement physique limité ou largement répartis ;
- Et que ces éléments doivent être périodiquement révisés, entretenus et/ou mis à jour/modernisés ;
- Et que certains de ces éléments transmettent des informations entre eux et en reçoivent ;
- Et que le système est d'une certaine manière connecté au monde au-delà du système lui-même, soit physiquement, soit virtuellement (par exemple par Internet) ;
- Et que l'ensemble du système proprement dit fait périodiquement ou constamment l'objet de modifications et d'améliorations du fait d'interventions qui peuvent être virtuelles, automatisées ou humaines ;

alors, tous les systèmes techniques sont de nature assez générique.

14. Bien que les systèmes techniques soient de nature assez générique, ils sont aussi assez complexes et déroutants. Par conséquent, pour simplifier, tous les systèmes techniques peuvent être considérés comme étant constitués de trois éléments fondamentaux, à savoir : composants, interconnexions et interventions.

15. Ces trois éléments, tels qu'ils sont présentés, interviennent de façon quasi chronologique dans le cycle de vie d'un système technique. Par exemple, les composants sont conçus et fabriqués, puis les intégrateurs de systèmes conçoivent le système, choisissent les composants et enfin réalisent le système. Celui-ci est ensuite exploité au moyen d'interventions. Tous les éléments se font suite mais l'ordre dans lequel ils interviennent n'est ni figé ni unidirectionnel À mesure qu'un système vieillit et évolue, de nouveaux composants et des composants de remplacement sont nécessaires, ce qui implique souvent d'avoir recours à de nouvelles conceptions et technologies, et de revenir à l'élément « composants ». Le système lui-même peut évoluer, la naissance de besoins nouveaux ou différents nécessitant l'intégration de nouveaux types de composants, de concepts et de technologies, entraînant ainsi un retour à l'élément « interconnexions ». Et à mesure que les pratiques opérationnelles, les règlements et les normes évoluent et s'améliorent, des types d'interventions nouveaux et différents s'imposent.

16. Composants : Chaque système technique comporte des composants qui peuvent être non seulement physiques, mais également virtuels (logiciels de contrôle, données, etc.). Chaque composant a une fonction et une raison d'être dans le système. Les composants doivent être conçus en fonction de leur destination, puis réalisés (fabrication, développement, etc.). Ils doivent parfois être réparés, mis à niveau ou remplacés. Il arrive aussi qu'il puisse y avoir un long délai (intervalle) entre la réalisation d'un composant et son intégration dans un système (durée de conservation avant utilisation). Ce délai doit être géré de manière à garantir l'intégrité du composant et du système.

17. Interconnexions : Il s'agit de l'intégration dans les systèmes. C'est la manière dont les composants interagissent, communiquent et travaillent ensemble. Cette interaction peut être assurée au moyen d'interconnexions physiques, comme des pièces passant par un système de fabrication, des trains sur rails, des câbles de transmission transportant de l'électricité ou des câbles pour des signaux de commande. Il peut également s'agir de flux d'informations par fil ou sans fil. Les voies ferrées, les fils de transmission et les câbles de signaux peuvent tous être apparentés à des composants mais leur fonction, à savoir le transport des trains, de l'électricité et des signaux est l'interconnexion.

18. L'intégration dans les systèmes est une fonction qui doit être conçue et, parfois, les interconnexions doivent être remises en état, mises à niveau ou remplacées. Dans certains cas, les interconnexions changent de manière dynamique, soit continuellement comme dans le cas d'Internet, soit occasionnellement, comme dans le cas des réseaux intelligents (dans lesquels entrent et sortent de nouvelles capacités de production et de nouvelles charges, suivant une dynamique organique incontrôlée).

19. Interventions : Elles peuvent être humaines, virtuelles ou automatiques. Les interventions sont essentiellement liées à l'exploitation du système tout au long de son cycle de vie, et peuvent reposer sur des pratiques exemplaires, des processus et des procédures. Elles peuvent également concerner des services fournis en interne ou externalisés, tels que les services de fournisseurs. Certaines interventions peuvent être automatisées, comme, par exemple, la mise à niveau automatique des logiciels de protection antivirus et de protection contre le piratage dans les systèmes informatiques, ou le contrôle automatique de la transmission et du certificat virtuel de données entrantes. Souvent, les interventions sont des tâches anodines, mais il peut s'agir de pratiques humaines exemplaires qui ont leur importance, comme le fait de changer régulièrement les mots de passe, signaler la perte des cartes magnétiques d'accès ou des badges et les invalider, etc.

20. Le concept décrit ci-dessus, qui repose sur trois éléments fondamentaux, correspond à une approche très globale d'un système. Pour chacun de ces trois éléments, on trouve toujours des sous-éléments qui fournissent plus de détails sur le système. Nombre des sous-éléments sont les mêmes d'un système à l'autre, mais leur importance peut varier sensiblement selon le système. Et certains systèmes comportent des sous-éléments qui leur sont propres. Selon le niveau de précision requis, on peut définir un grand nombre de sous-éléments dont certains peuvent même nécessiter des sous-catégories.

Annexe B

Modèle fondé sur les menaces

Voir le site Web de l'initiative (http://www.unece.org/tradewelcome/tradewp6/groups/cybersecurity.html, actuellement en cours de mise à jour).

Annexe C

Exemples d’utilisation du modèle de matrice générique dans différents secteurs d’application

Voir le site Web de l’initiative (http://www.unece.org/tradewelcome/tradewp6/groups/cybersecurity.html), actuellement en cours de mise à jour).