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

Economic and Social Council

Distr.: General
11 September 2019

Original: English

Economic Commission for Europe

Steering Committee on Trade Capacity and Standards

Working Party on Regulatory Cooperation and Standardization Policies (WP.6)

Twenty-ninth session
Geneva, 20–22 November 2019
Item 10(b) of the provisional agenda
International regulatory cooperation:
Sectoral Projects

Report on the sectoral initiative on cyber security

Submitted by the secretariat

Summary

This document contains a proposal for a common regulatory framework on cybersecurity and is hereby submitted for decision by the Working Party.

Proposed decision:

"The Working Party adopts the proposal for a common regulatory framework as contained in this draft proposal".

It requests that the proposal be published. It also requests the secretariat to continue to report on the progress of the initiative.

I. Introduction

1. At its twenty-seventh annual session, the Working Party approved the proposal for a new sectoral initiative on cybersecurity (Decision 21, ECE/CTCS/WP.6/2017/2).

2. Further to this decision, a partnership was established with the International Electrotechnical Commission (IEC) Conformity Assessment Board Working Group 17, and

GE.19-15565(E)
1915565

the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE), which have been actively supporting the project.

3. Discussions were held and drafts proposals for a common regulatory framework in cybersecurity were presented to meetings of the Group of Experts on Risk Management in Regulatory Systems in 2018 and 2019.

4. The present document describes a systematic methodology for a systems approach to cybersecurity within a regulatory framework. It is different from other methodologies in that in addition to modelling the technical system, carrying out a risk identification, risk assessment and a requirement gap analysis, it also includes an analysis of the conformity assessment and market surveillance needs. It is a flexible methodology applicable to many varied technical systems within different economic sectors.

5. The present document is based on the life-cycle approach, which requires proper inspection, maintenance, repair and upgrade of the technical system. This approach guarantees effective and efficient cybersecurity over time as the system itself evolves and as the nature of the threat evolves.

6. This document sets out essential elements of regulatory processes that can be used by authorities and policymakers especially in sectors where no cyber security regulation currently exists. It identifies standards that can be useful reference in regulatory documents. It is a living document and it will be updated as the cyberenvironment changes.

II. Rationale for international cooperation in cybersecurity regulation

7. In the digital era, cybersecurity is essential element for economic competitiveness and continuity for all kinds of organizations.

8. Guaranteeing a high level of cyber resilience across the world is of paramount importance for ensuring essential services and achieving consumer trust in the digital era, and for the further development of a safer, more innovative, competitive, sustainable and affluent world.

9. Cyber threats are a worldwide phenomenon that crosses national, regional and international borders. Cybersecurity therefore requires an integrated approach at all levels.

10. Since cyber threats can be nationally, regionally or internationally based, international best practices are most appropriate. The International Organization for Standardization (ISO) and IEC International Standards are increasingly adopted by countries, as part of their obligation to fulfil the World Trade Organization Technical Barriers to Trade (WTO/TBT) objectives, at the regional and national level.

11. In most cases, the existence or use of disparate requirements and procedures in sectors that operate as truly global and integrated applications may, in and of itself, constitute an increased risk. It is however possible that in certain cases, the use of a multiple and different requirements represents a way of mitigating risks and increasing safety (i.e. to prevent spreading vulnerabilities).

12. To be efficient, cybersecurity measures on business, national and international level should be based on results of a systemic risk management process, with involvement of all relevant stakeholders.

III. The purpose of the CROs

13. The Common Regulatory Objectives (CROs) presented in this document have been drawn up in accordance with Recommendation L and Recommendation R of the Working Party on Regulatory Cooperation and Standardization Policies (Working Party 6) of the United Nations Economic Commission for Europe (ECE/TRADE/378 – ECE Recommendations on Standardization Policies).

14. The purpose of the CROs is twofold. On the one hand, they can be used as a model to draw up legislative instruments in countries that do not currently have regulations in this sector. On the other hand, they can be used to align existing national regulation with an internationally harmonized best practice.

15. The document describes a regulatory framework that countries can adopt to achieve common cybersecurity regulatory objectives. The document can be used as a basis for:

- Setting regulatory objectives in cybersecurity;
- Identifying and assessing cybersecurity risks;
- Identifying international standards that can be applied as a basis for cybersecurity regulations;
- Establishing conformity assessment procedures in cybersecurity; and
- Implementing a market surveillance process.

16. Countries wishing to establish special operational transnational arrangements can use the CROs in accordance with the process described in Recommendation L, Annex C.

17. A national regulatory framework can use the model described in the document for certain critical sectors and applications or require that the commercial players in those same sectors and applications, or others, use the model to satisfactorily demonstrate compliance. Third party conformity assessment should only be required where appropriate, according to the results of the risk analysis.

18. The application of the common regulatory framework will:

- Promote a globally harmonized legislation;
- Promote legislation which is proportionate to the risks it was set out to address;
- Ensure mutual acceptance of test and assessment procedures and results among the test houses; and
- Strive for consistent and comparable procedures for the assessment and implementation of actions for cybersecurity.

19. Additionally, applying the document will promote the convergence of national technical regulations currently in place, or yet to be put in place, towards a shared framework that is based on a risk-based approach and other international best practices. This will reduce barriers to trade for components, equipment, qualified persons and services and will encourage competition, increase market choice and reduce costs.

IV. Common regulatory objectives in cybersecurity

20. Regulatory framework on cybersecurity aims at contributing to ensuring the general wellbeing and prosperity of a country’s citizens through:

(a) Data protection;

(b) Reliability;

(c) Continuity;

(d) Safety; and

(e) Security

of critical infrastructures, such as electrical energy supply, clean water supply, waste-water treatment, gas and fuel supply, banking, health, transport and other essential services, as defined or limited by Section V (scope).

21. Regulators of specific sectors can build on these CROs to harmonize regulations internationally as a basis for sector-specific legislation on cybersecurity and minimize any special requirements that are justifiable based on idiosyncratic national risks.

22. Setting regulatory objectives should be based on the principle that zero risk cannot be an achievable regulatory objective. Determining the tolerable level of risk and risk appetite should be performed as described in Recommendation R.

V. Scope statement of the Common Regulatory Objectives

23. This CROs is superseded by existing dedicated regulatory regimes where these exist or are in the process of being developed.

24. Products and processes covered by CROs include:

- Physical applications, so called Operations Technology (OT) systems, such as critical infrastructure and smart systems, and processes to keep those systems running (as for example covered by the IEC 62443 series of international standards); and
- Informational systems, so called Information Technology (IT) systems, with the need to protect data and keep it flowing securely (as for example covered by the ISO/IEC 27000 series of international standards).

25. The CROs address the requirements for system's technology including:

(a) Data, connectivity, components, equipment, applications and service delivery;

(b) the competency and qualifications of persons; and

(c) the management processes including,

(i) component design; and

(ii) systems integration and realisation, operation, maintenance, upgrade, and so on.

26. A generic matrix model should be used to identify all components of the technical system (Annex A).

VI. Identification of cybersecurity risks

27. Cybersecurity risks are incidents or events that can impact the delivery of cybersecurity objectives, as defined earlier in the document. Clarity in identifying generic and specific risks assists the assessment of risk and identification of controls to manage the risk to a tolerable level.

28. The following international standards and other cybersecurity frameworks may be applied for the identification of cybersecurity risks, including:

- ISO/IEC 27000 series of standards;
- IEC 62443 series of standards;
- ISO 31000 series of standards;
- National Institute of Standards and Technology (NIST) Framework v1.1;
- Bank for International Settlements (BIS) – Basel 2/3, Operational Risk;
- Control Objectives for Information and related Technology -COBIT 5; and
- Open Web Application Security Project - OWASP-Top10

29. It is apparent that cyber protection requires a holistic, systems-wide approach.

30. The generic matrix model (see Annex A) may be used to determine the points at which cybersecurity risk identification should be performed and assessments made.

31. When performing the identification of cybersecurity risks the following factors (see the "adversary model", Annex B, describing the motivations and potential scenarios of cybersecurity risks that could occur throughout the technical system, with an illustrative list shown below should be considered:

- Hacktivist;
- Cybercriminal;
- Insiders;
- Cyber Espionage;
- Cyber Terrorist;
- Cyber Warfare; and
- etc.

See Annex B for a comprehensive list of factors and their description (currently under development).

32. Examples of cybersecurity risks and related vulnerabilities include:

i. Loss or unauthorised access to data, non-compliance with regulations (e.g. General Data Protection Regulation (GDPR) and other data regulations);

ii. Disruption of or unauthorised access to systems and applications;

iii. Breakdown or lack of support of legacy systems;

iv. Loss of service/support from third party suppliers;

v. Overloading of systems (system crash) through external attack/over use;

vi. Accidental virus infection;

vii. Inadequate expertise to maintain legacy systems and develop responses to current/future needs; and

viii. Inadequate executive skills to understand and develop strategy to exploit cyber opportunities (e.g. Cloud Technology)

33. Regulatory authorities should monitor evolving cybersecurity threats, as past history is no longer a comprehensive predictor for the future.

VII. Assessment of cybersecurity risks

34. When possible, quantification of cybersecurity risks should be performed, so that they could be prioritized and evaluated against the level of tolerable risk, as described in Recommendation R.

35. It is recognized that cybersecurity risk cannot be eliminated, and the level of tolerable risk should be defined.

VIII. Determining regulatory requirements to address cybersecurity risks and relevant international standards providing the presumption of conformity

36. When determining regulatory requirements, the ECE Working Party 6 Recommendation R "Risk Management in Regulatory Systems" should be used by regulatory authorities to ensure consistency and proportionality between the existing cybersecurity risks and respective regulatory requirements.

37. The basic principles for cybersecurity are well documented and continuously updated to the state of the art in international standards, examples are the IEC 62443 series and the ISO/IEC 27000 series of international standards.

38. Countries use standards in their regulations in different ways, including:

- by making reference to standards in legislative acts; and
- by making compliance with the standards a means of proving compliance with the essential requirements laid out in the legislation; under this approach, equipment, people qualifications, services, practices and processes that comply with the provisions of the standards are "deemed to comply" with the requirements specified in the regulations.

39. The identification of risks and analysis of different systems in different situations will lead to different needs for requirements. Regulatory Requirements will be based on international standards such as those of the IEC and ISO, or, if not available, then on regional standards or finally on national standards. Where no standards are available requirements may be based on market accepted best practices and procedures.

40. Examples of standards that might be used when establishing presumption of conformity with the relevant regulatory requirements are listed in the document. The list of standards is to be updated as frequently as necessary depending on the publication output of IEC or ISO/IEC International Standards relevant to the objectives of this regulation model.

41. If international standards are not available, regional standards or national standards should be applied in development of regulatory requirements.

Requirements for components, products, equipment

42. Requirements for components, products and equipment used as system elements may be based on international standards such as those of the IEC and ISO, such as:

i. IEC 62443-1-1 Ed. 2: Terminology, concepts and models (in development);

ii. IEC 62443-2-1 Ed. 2: Establishing an industrial automation and control system security program (in development);

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

iv. IEC 62443-2-4: Security program requirements for IACS service providers (adopted);

v. IEC 62443-2-2: IACS protection levels (in development);

vi. IEC 62443-3-2: Security risk assessment and system design (in development);

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

viii. IEC 62443-4-1: Secure product development lifecycle requirements (adopted);

ix. IEC 62443-3-3: System security requirements and security levels (adopted); and

x. IEC 62443-4-2: Technical security requirements for IACS components (in development)

43. Comprehensive list of standards will available on the website of the Initiative.

44. Production of equipment will be based on the comprehensive list of standards that will available on the website of the Initiative.

Requirements for personal competency

45. Requirements for personal competency will be based on available ISO and IEC international standards in this area, such as:

- ISO/IEC 27021 Ed. 1: Information technology - Security techniques - Competence requirements for information security management systems professionals

Requirements for processes

46. Requirements for processes will be based on applicable international standards such as those of the IEC and ISO, such as:

i. IEC 62443-4-1: Secure product development lifecycle requirements (adopted);

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

iii. IEC 62443-2-2: IACS protection levels (in development);

iv. IEC 62443-2-4: Security program requirements for IACS service providers (adopted); and

v. IEC 62443-3-2: Security risk assessment and system design (in development)

IX. Determining level of conformity assessment

47. Converging onto a common methodology based on harmonized international standards and international conformity assessment best practices presents several advantages. Among others, when third party conformity assessment is used to demonstrate conformity of components and technology, people competency and qualifications, recognition of this conformity in international trade and the movement of qualified persons, is facilitated.

48. The CROs are drawn up with reference to international standards and conformity assessment procedures such as those developed by IEC and ISO and to best practice in the assessment of conformity to such standards, as for example, within the IECEE and IECQ.

49. Countries should use a systematic methodology for determining an appropriate level of conformity assessment based on risk. It is apparent that, in a systems approach, stronger

and lesser forms of protection are appropriate, which means that stronger and less forms of confirming that the protective requirements have been met is also appropriate.

50. The level of conformity assessment that should be applied to the requirements will be determined by means of a risk assessment resulting in a risk rating of each point on the generic matrix model (Annex A). The analysis of different systems (see examples in Annex C) in different situations will lead to different risk ratings. High value points will afford higher levels of conformity assessment, as will high vulnerability points, while lower value and lower vulnerability points can afford lower levels of conformity assessment.

51. It is therefore apparent that a holistic cybersecurity approach should be neutral with respect to conformity assessment and accommodate different forms of conformity assessment – 1st party, 2nd party and 3rd party conformity assessment – according to the different levels of risk determined for the different system elements being protected.

52. When the risk analysis determines that 3rd party conformity assessment is appropriate, international best practices and global certification services, such as those offered by the IECEE and IECQ, when available and appropriate provides a useful reference.

Definition of applicable conformity assessment procedures

53. Compliance of the products/processes within the scope of the regulation in cybersecurity shall be achieved by an appropriate means of conformity assessment against requirements as specified in the specific application as determined by the process given part VIII of this document.

54. When third party conformity assessment is required, regulators, compliance with this CRO can be assured by use of an international certification scheme, such as the IECEE and IECQ, for direct market acceptance of products, persons, services and organizations carrying IECEE Certification or IECQ Certification. Alternatively, where national legislation does not allow for use of IECEE Certificates or IECQ Certificates, regulators are encouraged to seek national certification of compliance based on IECEE or IECQ testing, inspection and assessments.

Recognition of conformity assessment bodies

55. The qualification of conformity assessment bodies and test laboratories must follow the applicable ISO/IEC International Standards (see below). Accreditation bodies involved must be a member of International Laboratory Accreditation Cooperation/International Accreditation Forum. At least one member of the assessor team needs competence in the respective cybersecurity requirements (see e.g. the list of approved IECEE Assessors and IECQ Assessors).

56. Certificates must be in line with the requirements of the respective scheme type as described in the applicable ISO/IEC standard (see below).

57. The use of the IEC Conformity Assessment Systems, such as IECEE and IECQ, provides the presumption of conformity with the requirements of Part VIII. Other schemes may be considered as reference in a future edition of these CROs if they become available and are brought to the attention of the Initiative.

58. For these reasons, when third party conformity assessment is required, an internationally recognized certification scheme, such as the IECEE and IECQ, can reduce unnecessary costs associated with duplication of inspection, assessment, qualification and testing.

Conformity assessment standards

59. ISO/IEC 17065, ISO/IEC 17021, ISO/IEC 17024, ISO/IEC 17025, ISO/IEC 17040.

Fundamentals of product certification

60. ISO/IEC 17067.

X. Establishing market surveillance procedures

61. One final and essential element of the present document relates to market surveillance. Market surveillance is necessary to monitor the proper application of the CROs by industry and increase confidence in the effectiveness of the CROs. Common guidelines will be defined to support the national authorities defining and implementing actions and procedures, including for the removal of non-compliant system components and products from the national market.

62. Planning of market surveillance processes should be based, inter alia, on the ECE Working Party 6 Recommendation “S” on applying predictive risk management tools for targeted market surveillance.

63. In case of critical non-conformance, an international alert system should be put in place to inform all UN member States about recently detected risks.

64. Subject to appropriate review by the ECE management and governance bodies, in order to monitor proper compliance with the requirements of this model regulation in the marketplace, a network of market surveillance experts in cybersecurity is to be formed and operated.

XI. CROs – Part 7: ECE Cybersecurity Steering Committee

65. Subject to appropriate review by the ECE management and governance bodies, in order to monitor the implementation of the CROs in the countries that have based their national legislation on the ECE regulation model and to update the regulation model in the light of their experience, the ECE Cybersecurity Steering Committee is to be formed and will operate under the umbrella of ECE Working Party 6.

66. The Cybersecurity Steering Committee agrees on a constitution and other governing rules and procedures of the daily operations (e.g. voting procedures).

67. The Cybersecurity Steering Committee notifies the members of the ECE Standard Acceptance Group.

68. Members of the Cybersecurity Steering Committee with the right to vote are the representatives of those countries having implemented the regulation model. Observers who are also invited to attend the meetings are: representatives from IEC Standardization Management Board, IEC Conformity Assessment Board, IEC and ISO relevant Technical Committees, IEC Conformity Assessment Systems, the ECE Advisory Group on Market Surveillance. Advisors involved in pre-existing cyber security regulatory activities are invited to participate to the Steering Committee in their consultative capacity (e.g. WP.29 leadership and secretariat).

Annex A

Explanation of the Generic Matrix Model

1. The Generic Matrix Model (GMM) is a tool used to model a technical system and then to cross-reference that model with objects of conformity (or the things that can actually be assessed for conformity against requirements). The GMM is usually represented as a matrix with the system modelled vertically down the left-hand side and the objects of conformity listed across the top.

2. In a graphical representation of the GMM, horizontal lines are drawn from the system-model features across the page under the objects of conformity. Similarly, lines are drawn vertically downwards from the objects of conformity.

3. The GMM can be used to determine what is important for a given technical system when viewed through a specific lens. This will determine the most important features and sub-features that should be visible through that lens and that therefore should be apparent in the system-model. When cybersecurity is being viewed through the lens, the system may be modelled with such features as technology or components, interconnections, interventions, security zones, intrusion testing, and so on.

4. The requirements, around which a conformity assessment is to be made, typically, come in the form of best practices, qualifications, specifications, standards, or as a certain minimum or maximum result on standardized tests, and so on. To achieve the requirements, it may also be necessary to have a certain type or level of equipment, knowhow, skill-sets, competency, experience, and so on.

5. The act of making an assessment to see if the requirements have been fulfilled is the act of assessing conformity to the requirement. The formal term is conformity assessment. There are essentially three possible objects of conformity. They are products, people (competencies) and processes.

6. These three objects of conformity are the basic three. Many other objects of conformity have been proposed, such as services, data, installations, projects, bodies or organization, systems and external factors. But in reality, each of these is simply one or a combination of the three basics. For example, services are essentially just processes, performed by people (with the appropriate competencies), perhaps using appropriate products or equipment. There is nothing else. Therefore, services are already covered by the three basic objects of conformity and do not need a special category of their own.

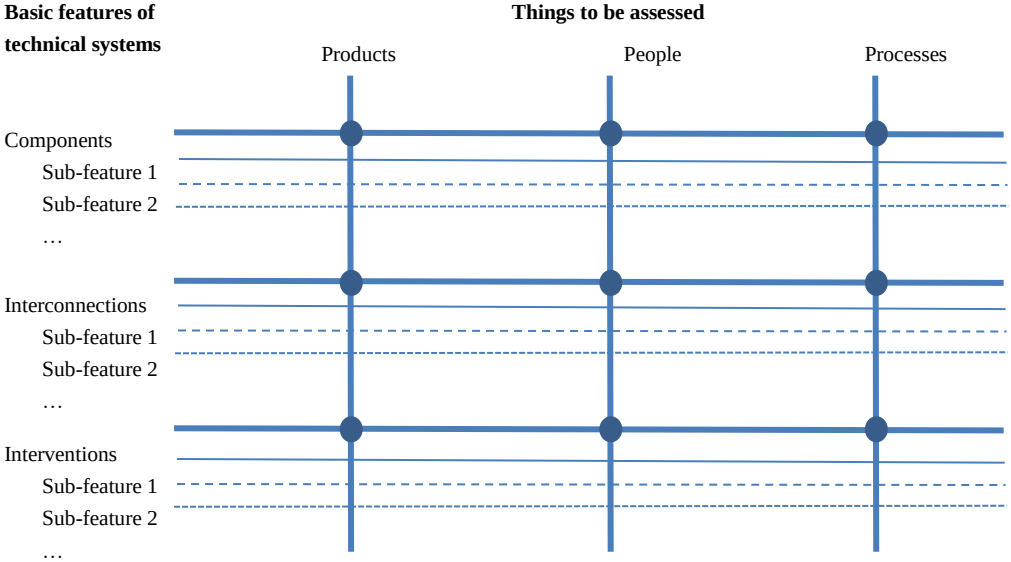
7. This having been said, if it serves a sector to specify more than the three basic objects of conformity, then the additional(s) object(s) of conformity should be included in the specific GMM.

8. At the intersection points of the system-model features and the objects of conformity is where the requirements can be applied. What the requirements are and whether they are available will be determined through a gap analysis.

9. Understanding the system, knowing where the value is and where the vulnerabilities are will then be used with a risk assessment of each of the intersection points to determine what kind of conformity assessment is needed against the requirements at each point. Risk assessment should be performed as described in part VII. Higher value or more vulnerable intersection points will need stronger conformity assessment, while lower value or lower vulnerability points will need lesser conformity assessment. The full range of conformity assessment options should be available for appropriate use. This means first party conformity assessment such as manufacturer’s or supplier’s declaration of conformity; second party

conformity assessment such as self-assessments and internal audits by the user or owner of the system; and third-party conformity assessment such as type 1 (ISO/IEC 17067) type-testing, or type 5, full certification of conformity, and so on. Most regulations should be neutral in terms of conformity assessment, and only specify what is appropriate according to the results of the risk analysis.

10. The vertical and horizontal intersection points of the GMM are where conformity assessment is done, and systems-approach is the overall matrix of requirements and conformity assessment activities.



Generic model of a system's approach to conformity assessment (simplest form)

What is a technical system?

11. Technical systems are not natural systems such as biological systems like the blood circulatory system, or environment systems like the weather system, or celestial systems like the solar system, etc, rather, technical systems are man-made systems.

12. The commonalities between railway systems, cloud computing, the smart grid, industrial control systems, a nuclear power plant and electric distribution system, an oil refinery, a gas distribution system, a banking and financial system, a health information system, smart homes, and so on are that they are all technical systems.

13. A technical system is considered to be:

- a group of interacting, interrelated, or interdependent elements forming a purposeful whole;
- and that those elements can be procedural, physical and/or virtual;
- and that those elements can be components that need to be designed and manufactured or created;

- and that the system itself will be designed and built (or systems-integrated) and that the elements of the system can be confined to a limited physical location, or can be spread out over a large physical distribution;
- and that those elements need periodically to be revised, maintained and/or updated/upgraded;
- and that some of those elements transmit and receive information between themselves;
- and that the system is in some way connected to the world beyond the system itself, either physically or virtually (eg: via the internet);
- and that the whole system itself is periodically or constantly undergoing modification and development through interventions that could be virtual, automated or human;

then, all technical systems are quite generic.

14. Although technical systems are quite generic, they are also quite complex and confusing. Therefore, to simplify, all technical systems can be considered as consisting of three basic features: Components, Interconnections and Interventions

15. These three features, as listed, are somewhat chronological in the lifecycle of a technical system. For example, components are designed and built, then systems integrators design the system, select the components, and then realise the system. The system is then operated through interventions. Each feature follows the other, but there are may also be many loop-backs. As a system ages and evolves, new and replacement components are needed often with new designs and technologies, thus looping-back to the components feature. The system itself may evolve with new or different needs requiring new types of components, concepts and technology to be integrated, thus looping-back to the interconnections feature. And as operational practices, regulations or standards, evolve and improve, new and different types of interventions are required over time.

16. Components: Every technical system has components which are physical but can also be virtual (such as control software, or data, etc). Each component has a purpose and a reason to be part of the system. Components need to be designed for their purpose and then realised (manufactured, developed, etc). Components sometimes need to be repaired, upgraded or replaced. Sometimes there can be a long lead-time (interval) for components, between realisation and integration into a system (the shelf-life). This lead-time needs to be managed to ensure the integrity of the component and the system.

17. Interconnections: This is the systems integration. It is how the components interact, communicate and work together. This can be accomplished through physical interconnections such as parts moving through a manufacturing system, or trains on tracks, or transmission wires carrying electricity, or cables carrying control signals. It can be information flows through cables or wireless. The tracks, transmission wires and signal cables would all be components, but their function of carrying trains, electricity and signals, is the interconnection.

18. The systems integration needs to be designed, and sometimes the interconnections need to be repaired, upgraded or replaced. In some situations, the interconnections change dynamically, either continually, such as the internet, or sporadically such as with a smart grid (with new generating capacity and new loads coming-on and going-off in an uncontrolled organic development).

19. Interventions: These can be human, virtual or automatic. Interventions are mostly involved with the operations of the system throughout its lifecycle, and can be based upon

best practices, processes and procedures. They can also involve services provided internally or out-sourced, such as vender services. Some interventions can be automated such as the automatic upgrading of anti-virus/hacking protection software in IT systems, or the automatic handshaking and virtual certificate control of incoming data. Often interventions are mundane but some include important human best practices such as regularly changing passwords, or reporting and cancelling lost passkeys or badges, etc.

20. This concept of three basic features is the very high level, generic view of a system. Below each of these three features there will always be sub-features that provide greater detail about the system. Many of the sub-features will be the same from one system to another, but their individual importance may differ greatly from one system to another. And some systems will have sub-features that are unique to that particular system. Depending on the level of detail required, a large number of sub-features may be defined, and even sub-categories may be required within some of the sub-features.

Annex B

Adversary Model

See the website of the Initiative (http://www.unece.org/tradewelcome/tradewp6/groups/cybersecurity.html currently under development).

Annex C

Examples of the Generic Matrix Model used in different application sectors

See the website of the Initiative (http://www.unece.org/tradewelcome/tradewp6/groups/cybersecurity.html) currently under development).