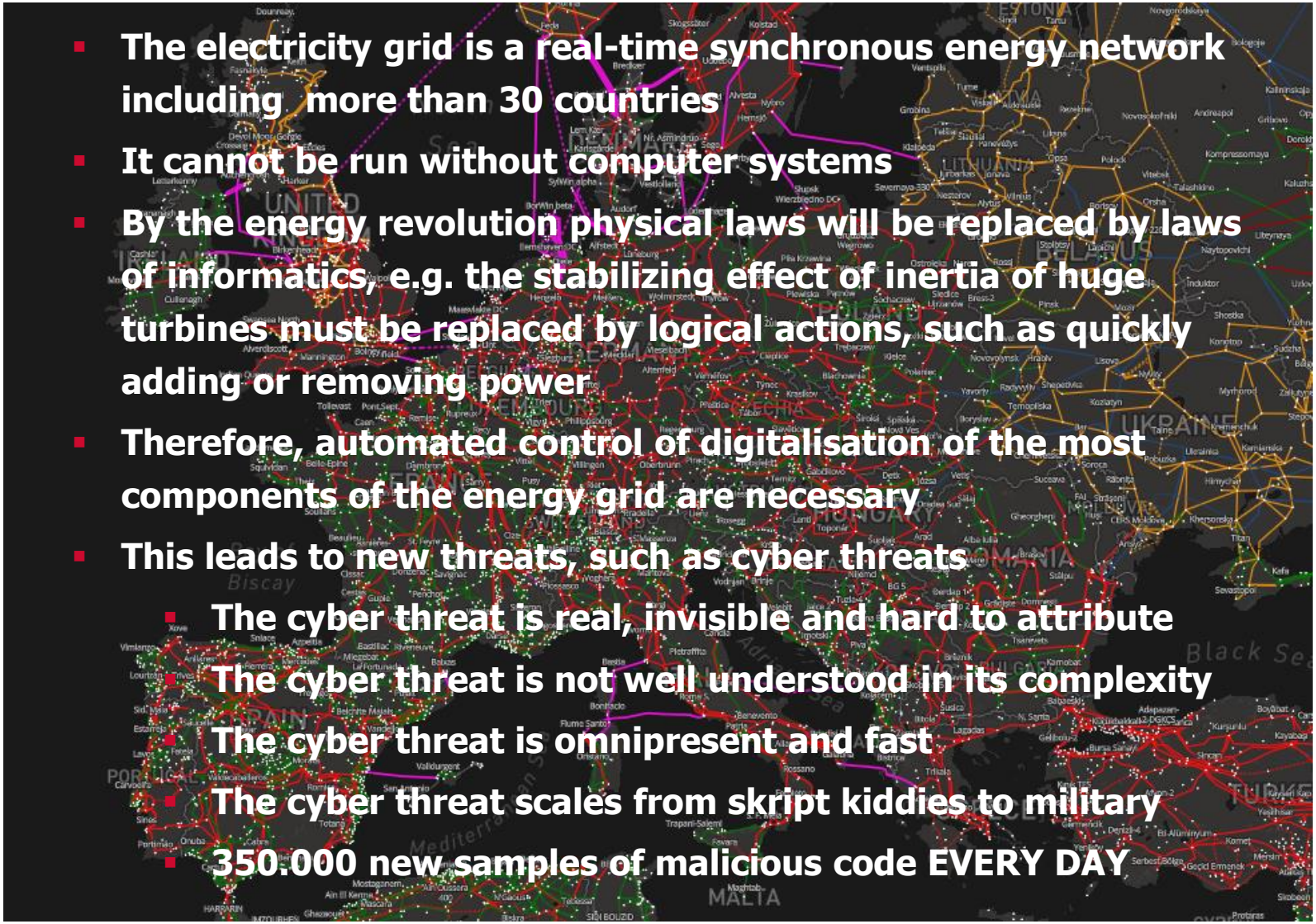
Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for Security
and Safety

Vienna Forum on European Energy Law

The Cybersecurity Perspective

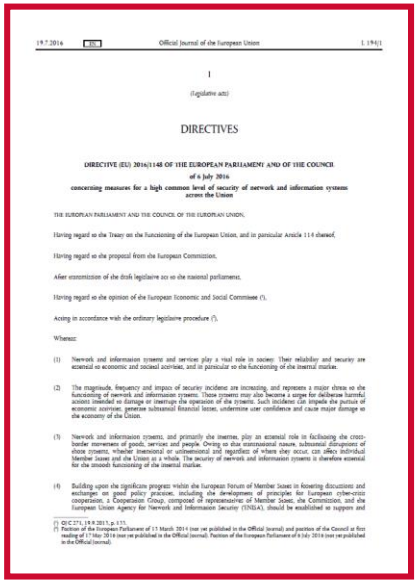
Guido Gluschke – Vienna - September 28, 2018

Current Situation In The EU Energy Sector



- The electricity grid is a real-time synchronous energy network including more than 30 countries
- It cannot be run without computer systems
- By the energy revolution physical laws will be replaced by laws of informatics, e.g. the stabilizing effect of inertia of huge turbines must be replaced by logical actions, such as quickly adding or removing power
- Therefore, automated control of digitalisation of the most components of the energy grid are necessary
- This leads to new threats, such as cyber threats
  - The cyber threat is real, invisible and hard to attribute
  - The cyber threat is not well understood in its complexity
  - The cyber threat is omnipresent and fast
  - The cyber threat scales from skript kiddies to military
  - 350.000 new samples of malicious code EVERY DAY

The European Commission Addressed Basic Cyber Security Elements In Its Legislation (NIS DIRECTIVE)



19.7.2016 EN Official Journal of the European Union L 194/1

I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 6 July 2016
concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

(2) The magnitude, frequency and impact of security incidents are increasing, and represents a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

(4) Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), should be established to support and

(1) OJ C 271, 19.9.2013, p. 133.
(2) Position of the European Parliament of 13 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 17 May 2016 (not yet published in the Official Journal). Position of the European Parliament of 6 July 2016 (not yet published in the Official Journal).

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

The NIS Directive Brings together Stakeholders BUT Focuses On National Responsibility

Member State

- identification of operators of essential services
- list of the essential services
- assessment of operators
- minimum capabilities on NIS
- security and notification requirements
- stable arrangements with operators
- academia/universities/innovation
- Competent Authority/national single point of contact
- participate in exercises
- report incidents of a suspected serious criminal nature
- encourage compliance or conformity with specified standards

National CAs or CSIRTs

- notifications of incidents
- communication with member states
- have compatible capabilities
- cooperation at Union level and internationally
- published information on incidents
- adopt national guidelines

National Operators

- forster culture of risk management
- risk assessment and the implementation of security measures
- security and notification requirements should apply

EU Cooperation Group

- discussions with relevant stakeholders
- discussion of capabilities and preparedness
- information exchange
- exchange of good policy practices
- assist its members in evaluating national strategies
- cooperate with relevant Union institutions
- cooperate with law enforcement authorities
- cyber-crisis cooperation
- anonymous notifications of incidents
- discuss the strategic decisions regarding exercises

EU ENISA

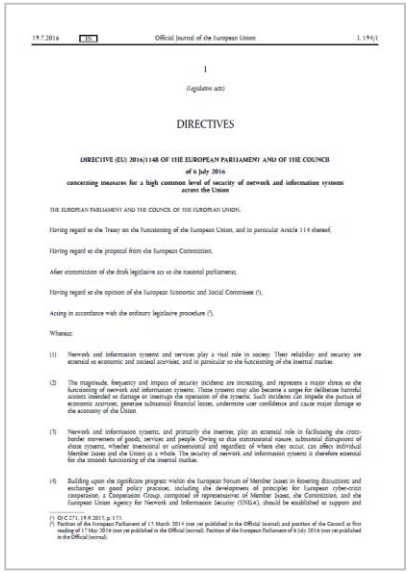
- providing expertise and advice to CG
- assist Member States in implementing the policies necessary to meet the legal and regulatory requirements
- running of European Union exercises
- development of guidelines for sector-specific criteria
- CyberEurope cycle of exercises

Digital service providers

- ensure the security of the network and information systems which they use
- security and notification requirements should apply
- designate a representative

IT Security Act As The German Legislation Of A National Implementation Of The NIS Directive

European Commission



DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

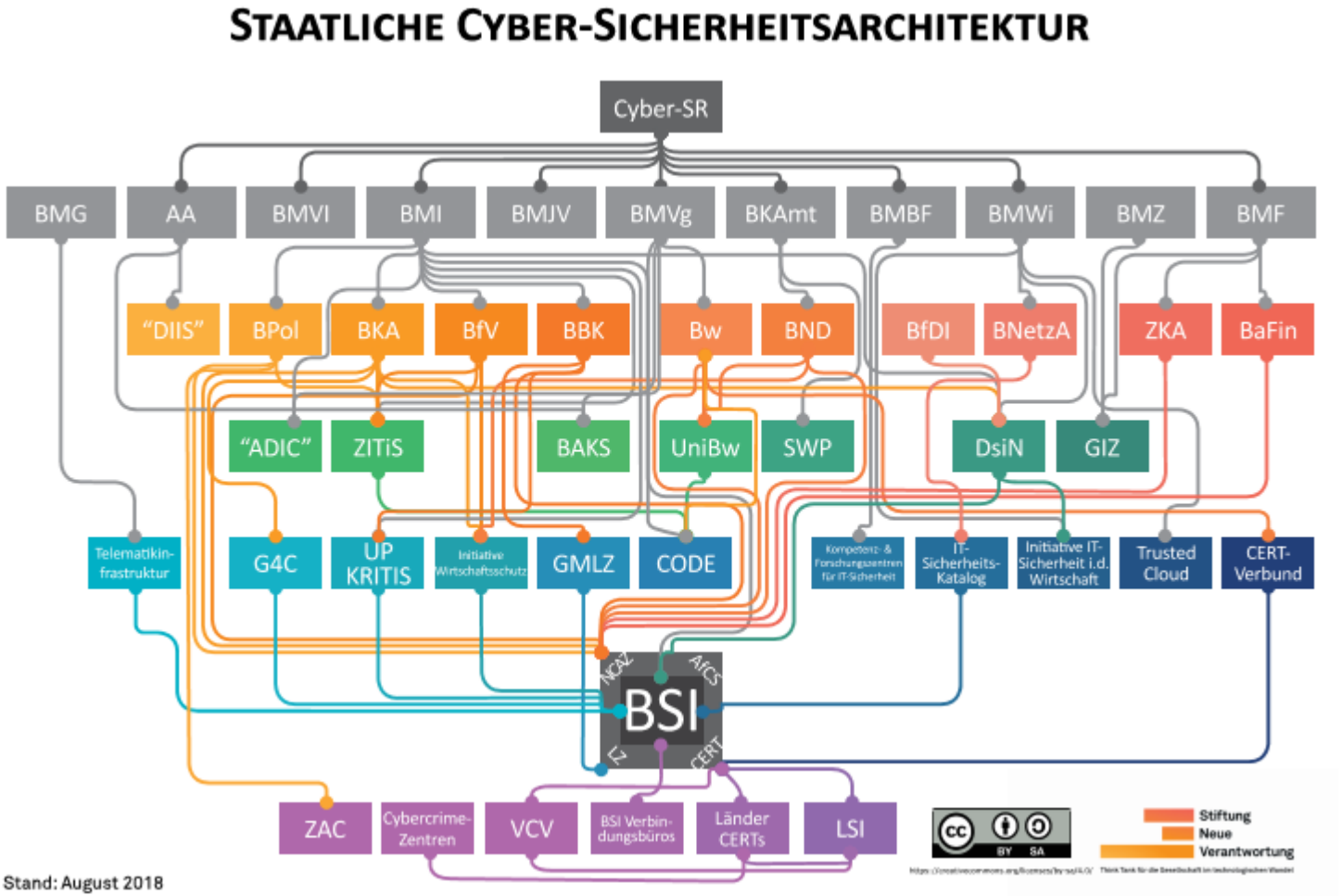
Federal Ministry of the Interior

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)* Vom 17. Juli 2015

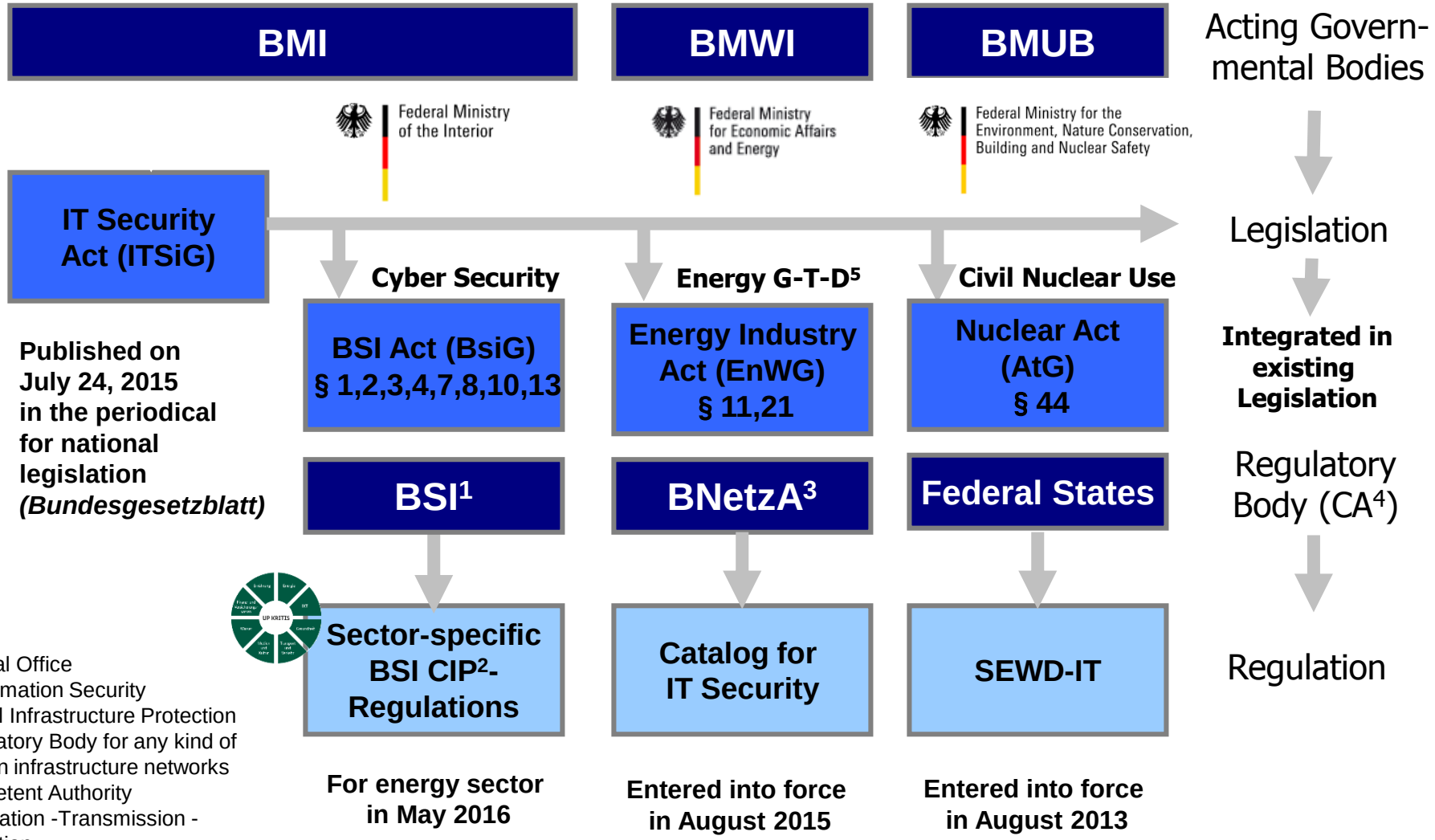
German IT Security Act

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015

How To Deal With German‘s Fragmented Cyber Security Responsibilities?

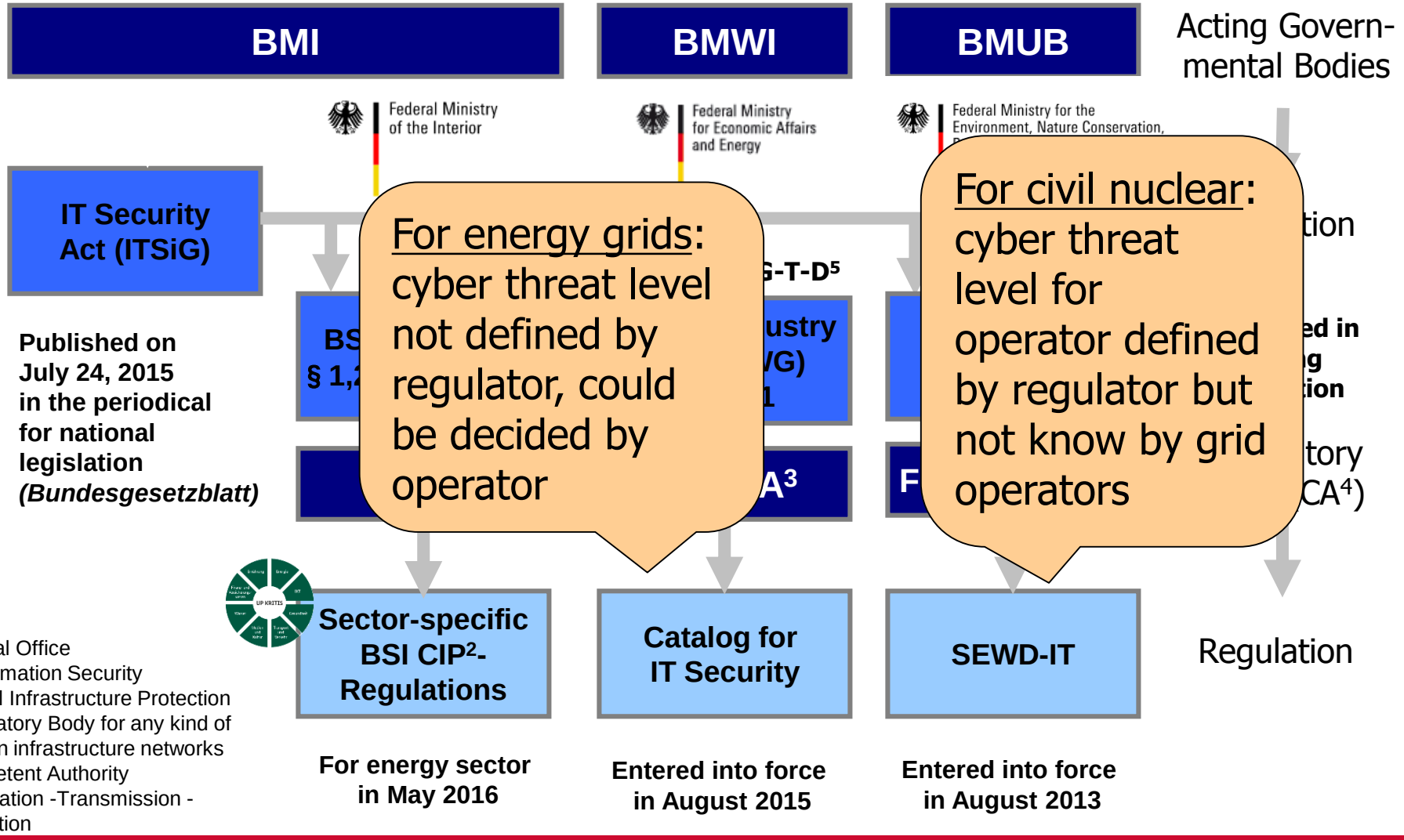


Consequence: Different Regulations For Energy Operators Working In The Same Energy Grid



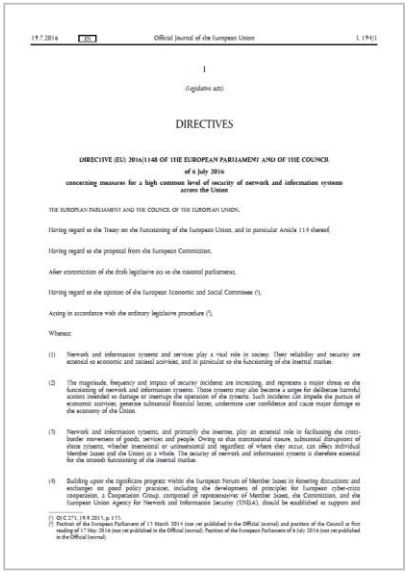
[1] Federal Office for Information Security
[2] Critical Infrastructure Protection
[3] Regulatory Body for any kind of comman infrastructure networks
[4] Competent Authority
[5] Generation -Transmission - Distribution

Consequence: Different Ways In Handling Cyber Threats Within The Same Energy Grid



[1] Federal Office for Information Security
[2] Critical Infrastructure Protection
[3] Regulatory Body for any kind of comman infrastructure networks
[4] Competent Authority
[5] Generation -Transmission - Distribution

DG ENER‘s Cyber Security Initiative EECSP Working On Improvements For The Energy Sector



19.7.2016 EN Official Journal of the European Union L 194/1

I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 6 July 2016
concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

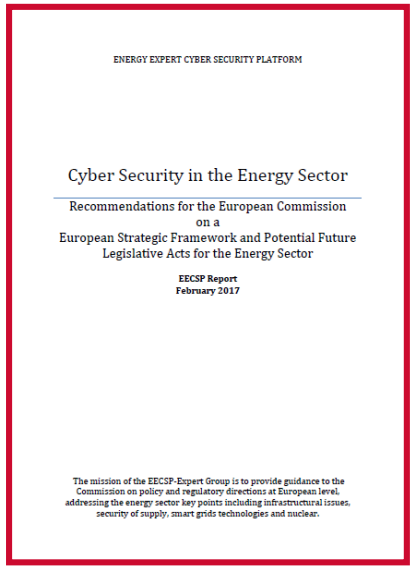
(2) The magnitude, frequency and impact of security incidents are increasing, and represents a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

(4) Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security (ENISA), should be established to support and

(1) OJ C 271, 19.9.2013, p. 133.
(2) Position of the European Parliament of 13 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 17 May 2016 (not yet published in the Official Journal). Position of the European Parliament of 6 July 2016 (not yet published in the Official Journal).

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union



ENERGY EXPERT CYBER SECURITY PLATFORM

Cyber Security in the Energy Sector

Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector

EECSP Report
February 2017

The mission of the EECSP-Expert Group is to provide guidance to the Commission on policy and regulatory directions at European level, addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies and nuclear.

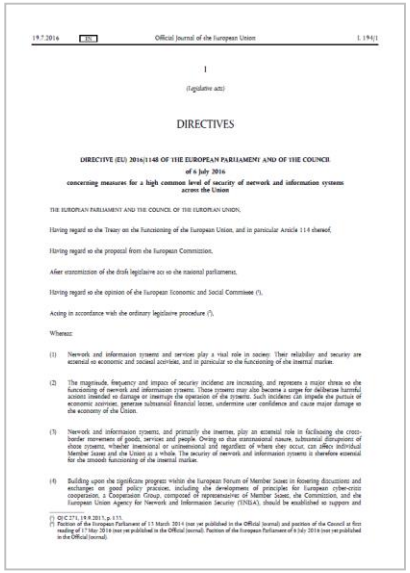
Cyber Security in the Energy Sector - Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, EECSP-Report, European Commission, Brussels, Feb 2017

EECSP:
European Energy Cyber Security Platform - Expert Group

EECSP Report Results - Strategic Priorities and Recommendations For The EC

Strategic Priorities		Strategic Areas		Areas of Actions
I	Set-up an effective threat and risk management system	1	European threat and risk landscape and treatment	(1) Identification of provider of essential services for the energy sector at EU level.
		2	Identification of provider of essential services	(2) Risk analysis and treatment.
		8	Best practice and information exchange	(3) Framework of rules for a regional cooperation.
		9	Forster international collaboration	(4) EU framework for vulnerabilities disclosure for the energy sector.
II	Set-up an effective cyber defence framework	3	Cyber response framework	(5) Define and implement cyber response framework and coordination.
		4	Crisis management	(6) Implement and strengthen the regional cooperation for emergency handling
III	Continuously improve cyber resilience	5	European cyber security maturity framework	(7) Establish a European cyber security maturity framework for energy.
		6	Supply chain integrity framework for components	(8) Establish a cPPP for supply chain integrity
		8	Best practice and information exchange	(9) Foster European and international collaboration
		10	Awareness campaign from top level EU institutions	
IV	Build-up the required capacity and competences	7	Capacity & competence build-up	(10) Capacity and competence build-up.

EECSP Recommendations Now Translated Into Binding Network Codes For TSOs And DSOs



19.7.2016 EN Official Journal of the European Union L 194/1

I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 6 July 2016
concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

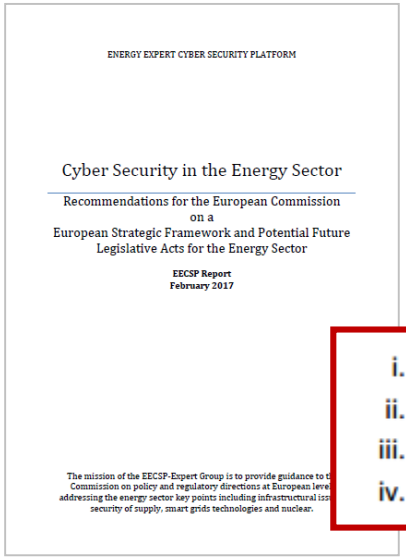
(1) Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

(2) The magnitude, frequency and impact of security incidents are increasing, and represents a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

(4) Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security (ENISA), should be established to support and

(1) OJ C 271, 19.9.2013, p. 133.
(2) Position of the European Parliament of 13 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 17 May 2016 (not yet published in the Official Journal). Position of the European Parliament of 6 July 2016 (not yet published in the Official Journal).



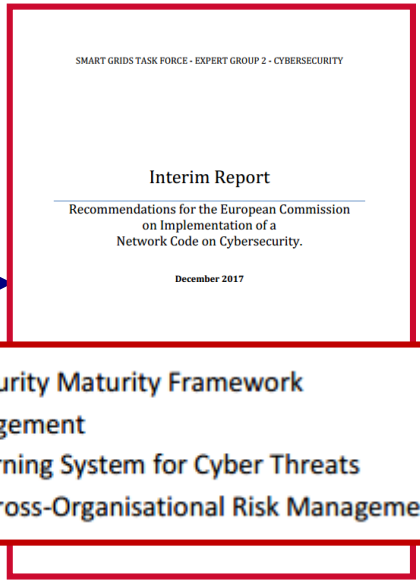
ENERGY EXPERT CYBER SECURITY PLATFORM

Cyber Security in the Energy Sector

Recommendations for the European Commission
on a
European Strategic Framework and Potential Future
Legislative Acts for the Energy Sector

EECSP Report
February 2017

The mission of the EECSP-Expert Group is to provide guidance to t
Commission on policy and regulatory directions at European leve
addressing the energy sector key points including infrastructural iss
security of supply, smart grids technologies and nuclear.



SMART GRIDS TASK FORCE - EXPERT GROUP 2 - CYBERSECURITY

Interim Report

Recommendations for the European Commission
on Implementation of a
Network Code on Cybersecurity.

December 2017

i. European Cybersecurity Maturity Framework
ii. Supply Chain Management
iii. European Early Warning System for Cyber Threats
iv. Cross-Border and Cross-Organisational Risk Management

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Cyber Security in the Energy Sector - Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, EECSP-Report, European Commission, Brussels, Feb 2017

SMART GRIDS TASK FORCE – EXPERT GROUP 2 - CYBERSECURITY Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity Brussels, December 2017

Additional Initiatives On Cyber Security in Energy With Impact On Europe

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Systems of Cyber Resilience: Electricity

Details: 07-08th May, 2018: Geneva, Switzerland

Objective
This workshop kicks off the World Economic Forum's 'Systems of Cyber Resilience: Electricity' initiative, by convening a multi-stakeholder group of global cyber resilience experts.

Monday 07th May 2018

18:30 – 19:00 Reception
19:00 – 21:00 Networking dinner in 'Restaurant de Parc des Eaux Vives', Geneva.
Remarks by Troels Oerting, *Head of Global Centre for Cybersecurity, World Economic Forum*

Tuesday 08th

08:30 – 09:00

09:00 – 09:10

Cybersecurity in the energy sector

High-level conference

11 October 2018
European Commission / Charlemagne Building, Brussels

e 2 0
u 1 8
. a t

Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for Security
and Safety

Thank you for your attention!

g.gluschke@uniss.org
www.uniss.org