Recent Developments of Cybersecurity Legislation in the EU: From Voluntary Approaches Back to Regulation?

RIPE 69, London — November, 2014 — Dr. Tatiana Tropina

Public-private collaboration

Before recent attempts to "legislate" cybersecurity:

- Self and co-regulation, voluntary collaboration
- Bottom-up approaches
- Necessity for public-private collaboration
- Multi-faceted strategies
- Recognition of the significant role that industry plays in the securing the information networks

Cybersecurity and law: misconceptions

A great cybersecurity pyramid?

Recent developments: EU and member states

What happened to voluntary collaboration?

Subjects of mandatory reporting obligation - here we go again?

Current discussion (October, 2014)

NIS Directive: current status

Towards more structured approaches?

Information society services

Council amendments to NIS / German IT Security Law (Draft)

Exposing information society services to additional obligations:

- without precedent
- disproportionate

? Legal certainty in cross-border environment

Opponents of regulation

From voluntary approaches to a heavy burden...

- Neo-classical economic assumption that customer demands security and regulation is only theoretical
- Relation to to obligatory reports regarding data protection
- Voluntary mechanisms already regarded as trusted are ignored
- Obligations fall on those who already 'do something'
- Possible costs
- Static compliance approach – reactive approach
- Impact on research and development
- Undermining the concept of PPPs

And here we fail....

Misconceptions lead to a call for regulation!

And here we fail....

- The overall impact of the mandatory obligation on the developments on securing cyberspace in the multi-faceted, multi-stakeholder environment.

Are we moving back from collaboration towards regulation? What should be the role of the industry in cybersecurity governance?

Are we moving "back" to regulation?

- Attempts to legislate cybersecurity
- Mandatory obligations vs. multi-faceted, multi-stakeholder environment
- Are we moving 'back' from collaboration towards regulation?
- What should be the role of the industry in cybersecurity governance?

Transparency and enforceability?

Top-down vs. Bottom-up regulation

- Information sharing between industry players and governments: can it be enforced?
- Voluntary sharing vs. the obligation to share
- The enforceability of reporting obligations: how will the governments do the checks?

Compatibility of approaches

EU vs. USA?

- USA: Presidential executive order 2013+Framework: using no mandatory reporting. Non-regulatory approach with incentives for compliance.
- EU vs. US approach to global issue?
- Gaps in cybersecurity frameworks and systems of regulation?
- Differences in the EU-US approaches – how does this fit for purpose of the NIS Directive?

Thank you!

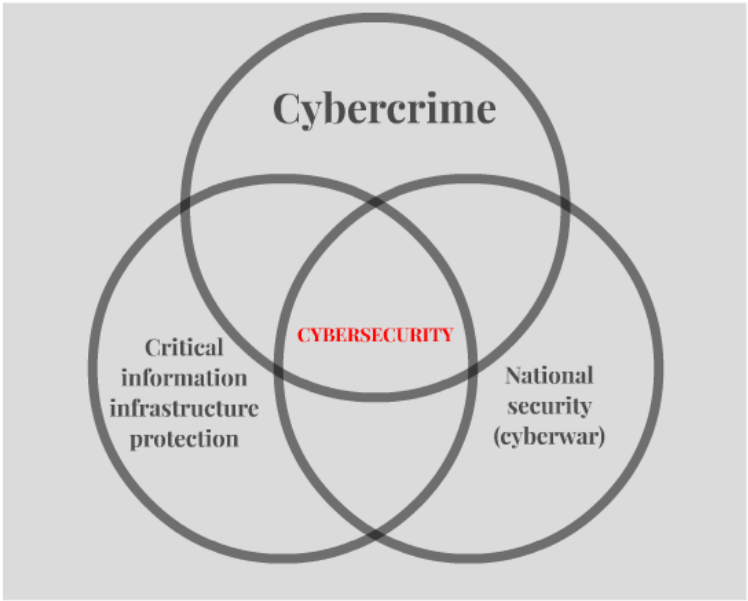
RIPE 69, London — November, 2014 — Dr. Tatiana Tropina

Recent Developments of Cybersecurity Legislation in the EU: From Voluntary Approaches Back to Regulation?

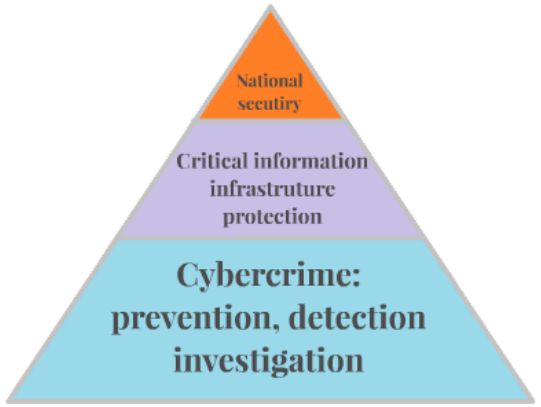
RIPE 69, London | November, 2014 | Dr. Tatiana Tropina

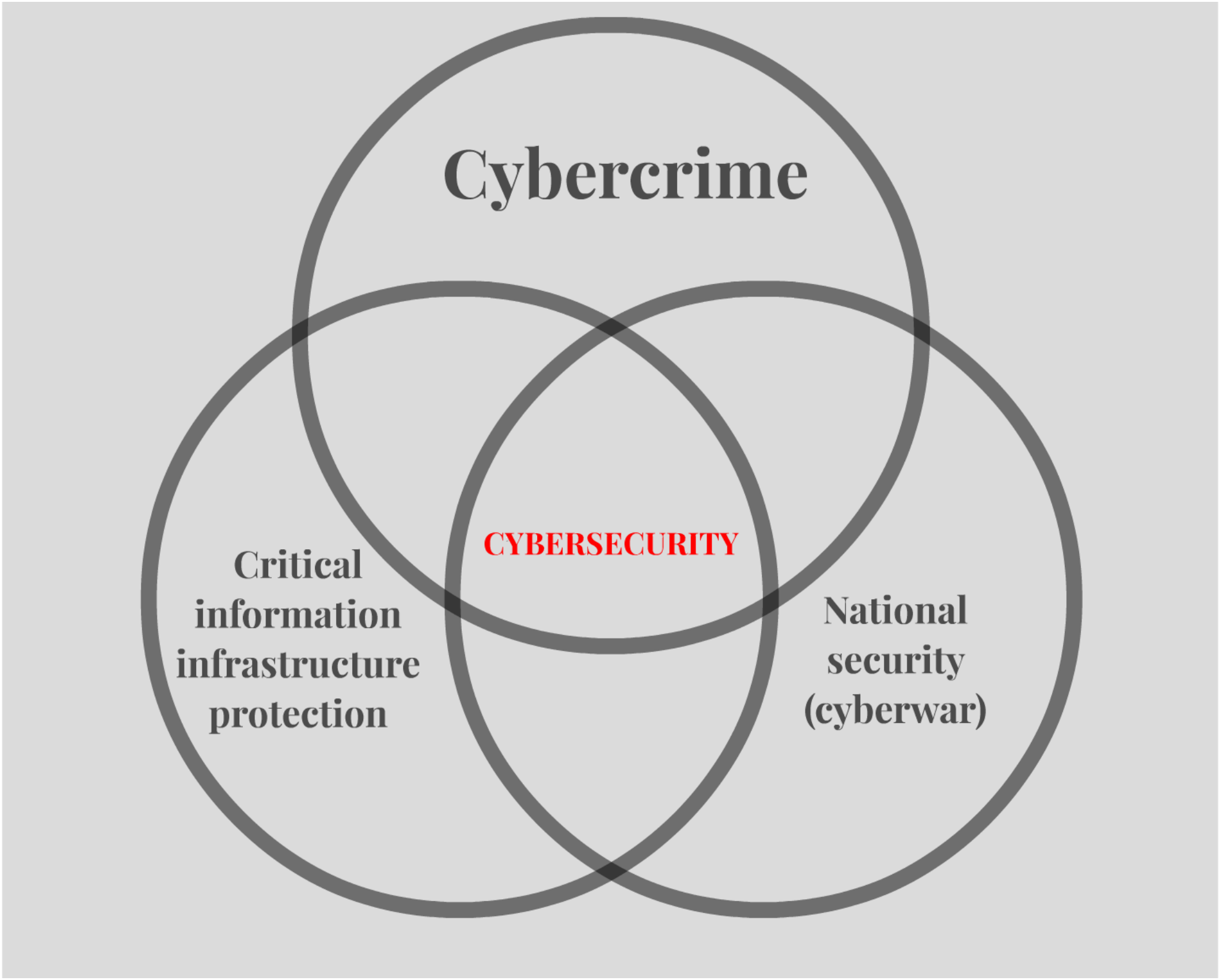
Cybersecurity and law: misconceptions

Different dimensions and blurring borders

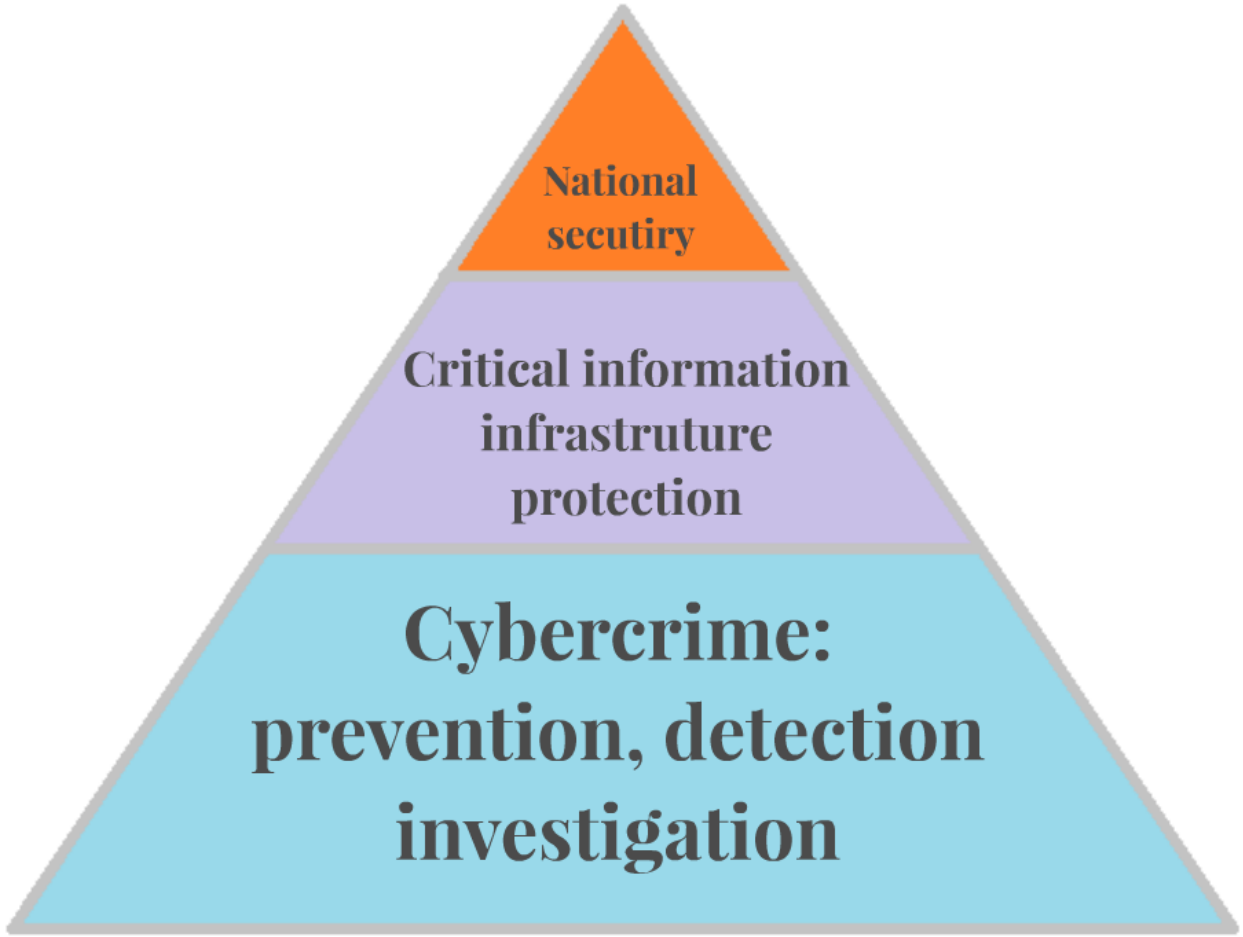


A great cybersecurity pyramid?




Cybercrime
CYBERSECURITY
Critical information infrastructure protection
National security (cyberwar)

A great cybersecurity pyramid?



Public-private collaboration

Before recent attempts to "legislate" cybersecurity:

- Self and co-regulation, voluntary collaboration
- Bottom-up approaches
- Necessity for public-private collaboration
- Multi-faceted strategies
- Recognition of the significant role that industry plays in the securing the information networks

Recent developments: EU and member states

What happened to voluntary collaboration?

EU: Network and Information security (NIS) Directive (Draft)

- Introduced mandatory reporting of security incidents instead of voluntary collaboration
- In March 2014, the EU Parliament excluded the information society services from the scope of the directive
- **However:** Internet Exchange Points should still be subject to the obligatory reporting imposed by the directive

Germany: Draft IT Security Law

- demands critical information infrastructure companies to report hacker attacks

- requires telecommunication providers to notify the government in case of network impairment or services that might lead to security violations and unauthorised user access to the systems

- obliges information society services providers, **which had been excluded from the scope of the EU Draft NIS Directive (March, 2014),** to implement protection measures and to secure authentication procedure.

EU: Network and Information security (NIS) Directive (Draft)

- Introduced mandatory reporting of security incidents instead of voluntary collaboration
- In March 2014, the EU Parliament excluded the information society services from the scope of the directive
- **However:** Internet Exchange Points should still be subject to the obligatory reporting imposed by the directive

Germany: Draft IT Security Law

- demands critical information infrastructure companies to report hacker attacks

- requires telecommunication providers to notify the government in case of network impairment or services that might lead to security violations and unauthorised user access to the systems

- obliges information society services providers, **which had been excluded from the scope of the EU Draft NIS Directive (March, 2014),** to implement protection measures and to secure authentication procedure.

Proponents of regulation:

"The amended version of the Directive approved by the Parliament is a major watering down of the regulatory scheme <...> The bad guys must be laughing their heads off!"

Stewart Room, Partner at Field Fisher Waterhouse, source: DataGuidance

Opponents of regulation

From voluntary approaches to a heavy burden...

- Neo-classical economic assumption that customer chooses security and reputation is only theoretical
- Relation to to obligatory reports regarding data protection
- Voluntary mechanisms already regarded as trusted are ignored
- Obligation fall on those who already "do something"
- Possible costs
- Static compliance approach + reactive approach
- Impact on research and development
- Undermining the concept of PPPs

European Council, October 2014 :

> ...some delegations point to the fruitful experience gained on the basis of voluntary notification and argue that **trust cannot be imposed** whereas others, on the other hand, believe that the Directive **should result in firm commitments** as well as allow for the building of confidence and trust over time"

source: European Council, Interinstitutional File: 2013/0027 (COD)

Subjects of mandatory reporting obligation - here we go again?

Current discussion (October, 2014)

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL
ANNEX II	**ANNEX II**	**ANNEX II**
List of market operators	**List of market operators**	**List of ~~market~~ ~~operators~~ types of entities for the purposes of Article 3(8)**[24]
Referred to in Article 3(8) a):	AM132 ***deleted***	~~Referred to in Article 3(8) a):~~
		0. In the field of infrastructure enabling the provision of information society services:
		Internet exchange points
		national domain name registries
		web hosting services
1. e-commerce platforms	AM132 ***deleted***	e-commerce platforms
2. Internet payment gateways		Internet payment gateways
3. Social networks		Social networks
4. Search engines		Search engines
5. Cloud computing services		Cloud computing services
6. Application stores		Application stores

source: European Council, Interinstitutional File: 2013/0027 (COD)
available at: http://www.statewatch.org/news/2014/oct/eu-council-NIS-prep-trilogue-13848-14.pdf

ent discussion (October, 2014)

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL
ANNEX II	ANNEX II	ANNEX II
List of market operators	List of market operators	List of ~~market~~ ~~operators~~ types of entities for the purposes of Article 3(8)[24]
Referred to in Article 3(8) a):	AM132 *deleted*	~~Referred to in Article 3(8) a):~~
		0. In the field of infrastructure enabling the provision of information society services:
		Internet exchange points
		national domain name registries
		web hosting services
1. e-commerce platforms	AM132 *deleted*	e-commerce platforms
2. Internet payment gateways		Internet payment gateways
3. Social networks		Social networks
4. Search engines		Search engines
5. Cloud computing services		Cloud computing services
6. Application stores		Application stores

pean Council, Interinstitutional File: 2013/0027 (COD)
http://www.statewatch.org/news/2014/oct/eu-council-NIS-prep-trilogue-13848-14.pdf

Council amendments:

3(8) "operator" means a public or private entity referred to in Annex II, which provides an essential service in the fields of infrastructure enabling the provision of information society services, energy, transport, banking, financial markets, health and water supply <...>
Each Member State shall identify on its territory entities, which meet the above definition of operator.

source: European Council, Interinstitutional File: 2013/0027 (COD)

Information society services

Council amendments to NIS + German IT Security Law (Draft)

Exposing information society services to additional obligations:

- without precedent
- disproportionate

? Legal certainty in cross-border environment

Transparency and enforceability?

Top-down vs. Bottom-up regulation

- Information sharing between industry players and governments: can it be enforced?

- Voluntary sharing vs. the obligation to share

- The enforceability of reporting obligations: how will the governments do the checks?

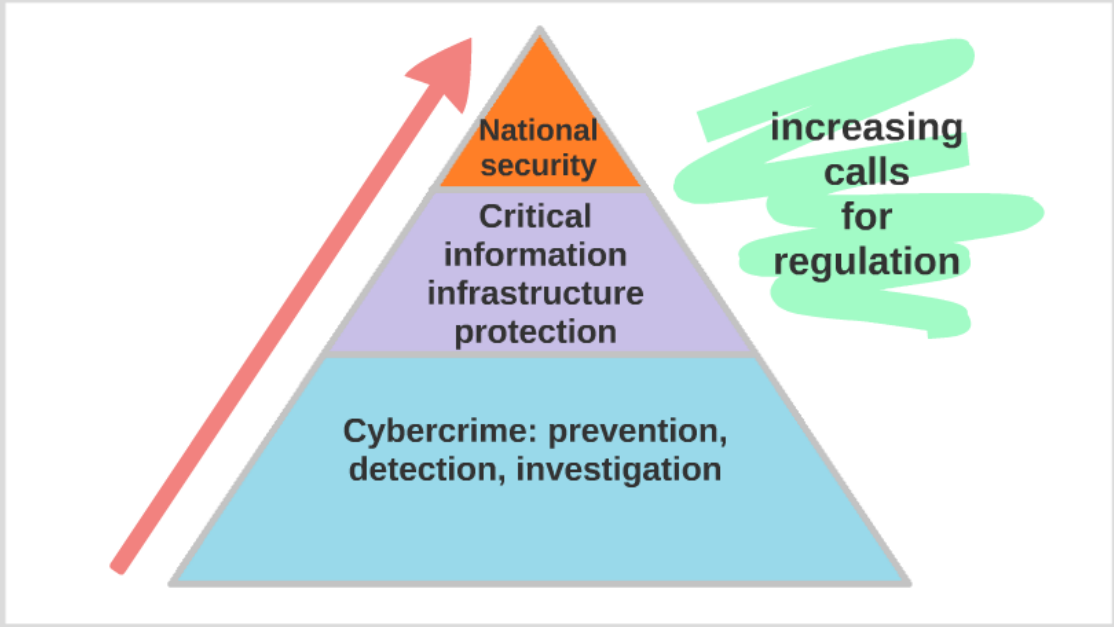
Compatibility of approaches

EU vs. USA?

- USA: Presidential executive order 2013+Framework 2014: no mandatory reporting. Non-regulatory approach with incentives for compliance.
- EU vs. US approach to global issue?
- Gaps in cybersecurity frameworks and systems of regulation?
- Differences in the EU MS' approaches - how does this fit for purpose of the NIS Directive?

And here we fail....

Misconceptions lead to a call for regulation!



Are we moving "back" to regulation?

- Attempts to legislate cybersecurity
- Mandatory obligations vs. multi-faceted, multi-stakeholder environment
- Are we moving "back" from collaboration towards regulation?
- What should be the role of the industry in cybersecurity governance?

Thank you!

RIPE 69, London November, 2014 Dr. Tatiana Tropina