Cybersecurity & Privacy Innovation Forum

28. April – 29. April 2015

Cyber-Security and Privacy in Vertical Supply Chains

Dr. Nicola Jentzsch
DIW Berlin

Cyber-Security and Privacy in Vertical Supply Chains

Table of Contents

Cyber-Security and Privacy in Vertical Supply Chains

I. Rationale of Industrial Policy

Goal: Strengthening domestic industries through targeted measures. In a social market economy, actors typically seek an **explicit justification** of industrial policy.

The **justifications** used are:

- Market failure (natural monopolies, externalities, information asymmetries)
- Correction of politically unwanted market results
- Correction of policy failure (repeated intervention)

3

Cyber-Security and Privacy in Vertical Supply Chains

I. Rationale of Industrial Policy

Are there any **special justifications** for targeting cyber-security and privacy industries?

- **Strong tendencies of externalities:** interdependent security (weakest link)
- **National security:** If critical infrastructures are attacked, severe disturbances of the public order can result (security of supply)
- Strengthen **future industries and markets** to increase European competitiveness

4

Cyber-Security and Privacy in Vertical Supply Chains

II. Perceived Weaknesses

Top-Rankings

Top-20 cyber-security firms: Only 3 from Europe

Top-10 semiconductor firms: 0 from Europe

Top-10 software firms: Only 1 from Europe

R&D Expediture

ICT R&D as percentage of ICT gross value added is 12% in the US compared to 6% in Europe (Digital Scoreboard 2012).

5

Cyber-Security and Privacy in Vertical Supply Chains

II. Perceived Weaknesses

"There is a risk that Europe not **only becomes excessively dependent on ICT produced elsewhere**, but also on **security solutions developed outside its frontiers**.
It is key to ensure that hardware and software components produced in the EU and in third countries that are used in **critical services and infrastructure** and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data."

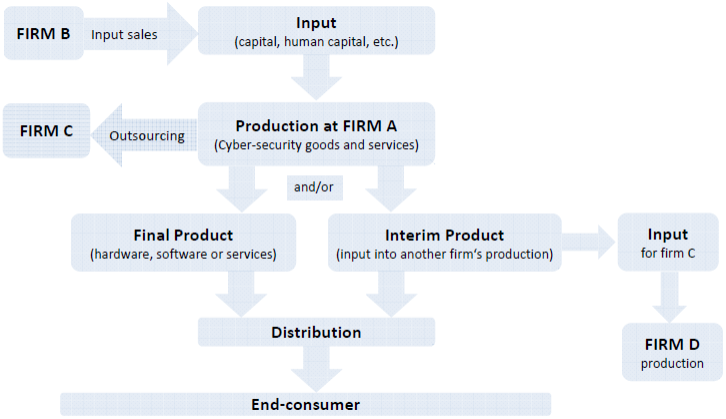
Joint EU Communication on Cybersecurity Strategy for the European Union (7/2/2013)

Analysis of **technological dependencies** of the industries in Europe

6

Cyber-Security and Privacy in Vertical Supply Chains

III. Vertical Supply Chains



Source: Jentzsch (2015)

Cyber-Security and Privacy in Vertical Supply Chains

III. Vertical Supply Chains

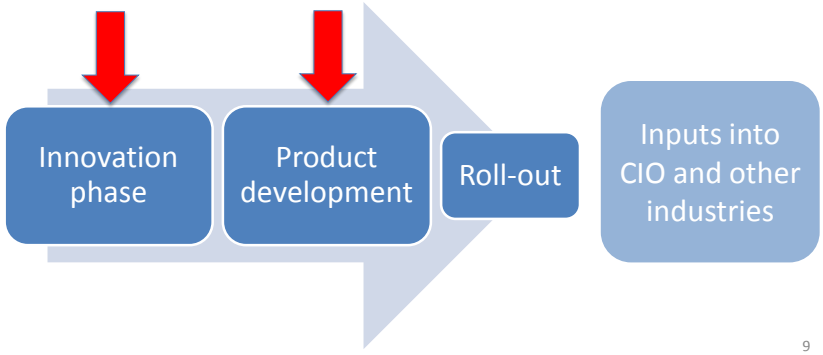
Example: PrivatOS

- Operating system used in BlackPhone
- Dual elliptic curve deterministic random bit generator (Dual_EC_DRBG) published by National Institute of Standards and Technology
- NSA has tampered with this crypto algorithm
- NYT Sept 5, 2013: NSA spends $250 million per year to insert backdoors in software and hardware as part of the Bullrun program
- Dual_EC_DRBG was used in many appliances, one of them the BlackPhone
- April 2014: NIST drops algorithm from recommendations

Cyber-Security and Privacy in Vertical Supply Chains

III. Vertical Supply Chains

Cyber Supply Chain Security



9

Cyber-Security and Privacy in Vertical Supply Chains

III. Vertical Supply Chains

Secure the vertical supply chains in the cyber-security industry

Analyze the potential weaknesses in the inputs

Direct targeted measures at securing the inputs

Cyber-Security and Privacy in Vertical Supply Chains

IV. Conclusions

Cyber-Security and Privacy in Vertical Supply Chains

IV. Conclusions

- Clearly identify **vertical weaknesses** of the cyber-security and privacy industry
- Set out a clear goal & strategy to remedy weaknesses
- Strengthen EU cyber-security and privacy products through public procurement policies
- Develop European security profile