EOS
EUROPEAN ORGANISATION FOR SECURITY

Moving towards a sustainable European cybersecurity industry

July 2014

EXECUTIVE SUMMARY

The pervasiveness of ICT in our everyday lives is growing rapidly through the increased use of different products and services. The market for cybersecurity is dominated by global suppliers and Europe is lagging behind. This is coupled with ever increasing issues of technological independence, sovereignty, privacy and market fragmentation. European industry needs to position itself firmly in the market by taking into account the European needs/approach.

As such, EOS calls for the fast implementation of a European Cybersecurity Industrial Policy (CY-SIP) linked to the European Cybersecurity Strategy of the EC and national cybersecurity strategies in order to secure European societies with European technology whilst boosting the European demand and competitiveness in cybersecurity and supporting the digital economy.

The key elements of such a strategy should include:

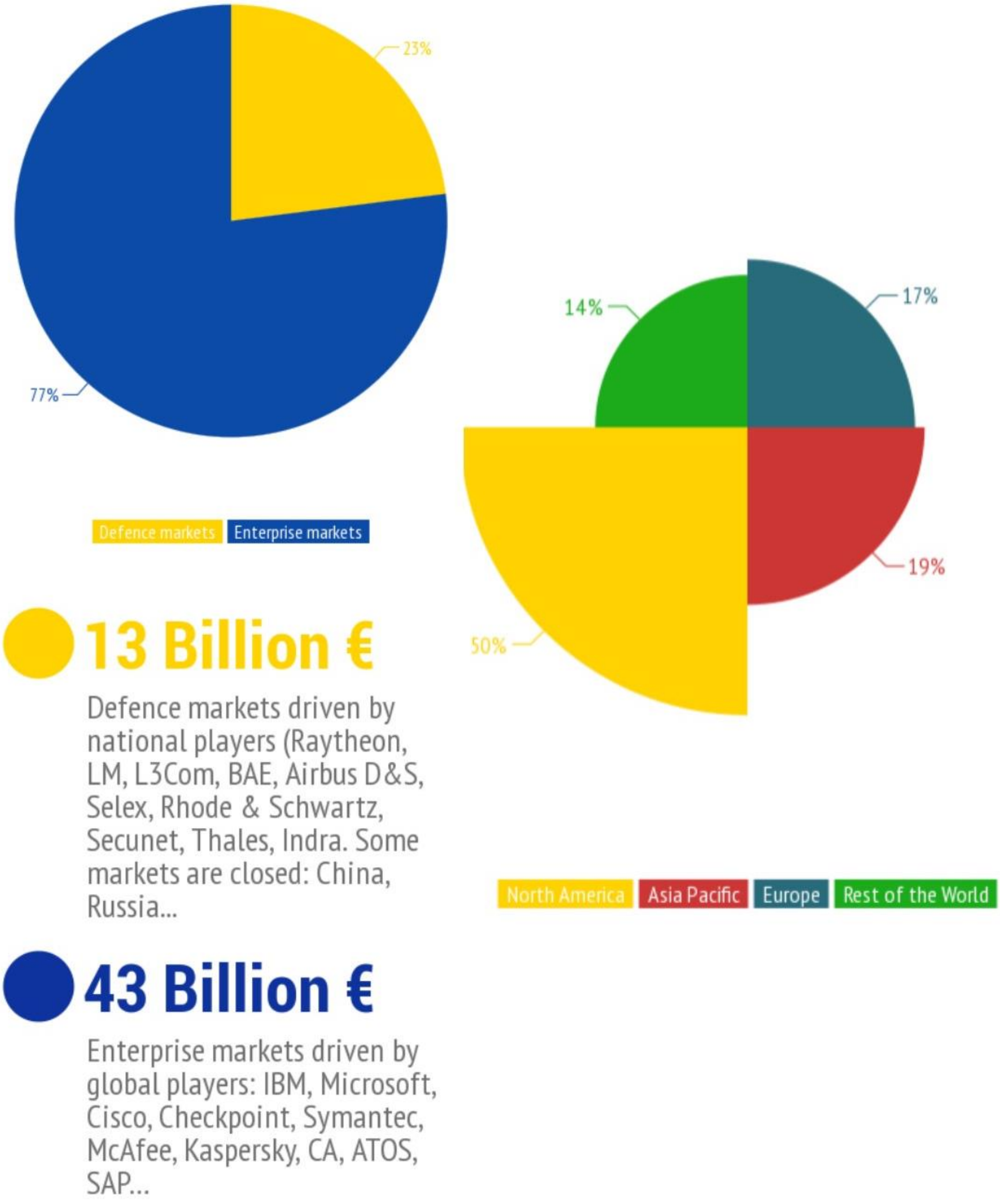
- *A **strategic vision** for a European Cybersecurity Industrial Policy*
- *An in-depth analysis of the **technological dependence** and its consequences on digital economy, sustainability, societal impacts and sovereignty issues*
- *A coordinated **R&I roadmap***
- *A coordinated **public procurement policy**, and*
- *A business-oriented, balanced and technology neutral **regulation framework***

EOS has outlined in this position paper the main issues in the present cybersecurity market suggesting a vision of what should be implemented at a European level.

Moving towards a sustainable European cybersecurity industry

A) THE CURRENT MARKET CONTEXT

***Global cybersecurity market dominated by global suppliers from North America*.** Our estimation[1] of the value of the global cybersecurity market is €56 billion , a large portion of which is made up of the North American market as illustrated in the figure below. The enterprise market is largely dominated by global cybersecurity suppliers such as Microsoft, IBM, CISCO, Symantec, etc.



13 Billion €

Defence markets driven by national players (Raytheon, LM, L3Com, BAE, Airbus D&S, Selex, Rhode & Schwartz, Secunet, Thales, Indra. Some markets are closed: China, Russia...

43 Billion €

Enterprise markets driven by global players: IBM, Microsoft, Cisco, Checkpoint, Symantec, McAfee, Kaspersky, CA, ATOS, SAP...

[1] ASDReports, Gartner, EOS members

Mature commodity market. Most IT hardware and software products are built outside the European Union. The market in "commodity" protection products, close to the ICT mass markets (firewalls, antivirus, IDS[2] software etc.) is already reaching maturity and is therefore more costly and complex to enter.

Which place for Europe? Considering the above, the two main questions for Europe are: a) what is the level of *strategic autonomy* that Europe needs to achieve in the cyber-security domain? and b) in which cybersecurity domains can European industry make a breakthrough and become a global and competitive player?

Objectives for a coordinated EU approach. Given these two questions, the answers must take into account market driven objectives and economic impact, and equally important objectives linked to societal and technological independence concerns, in order to see how these dimensions could justify a European approach to support the industry.

B) THE SITUATION IN EUROPE ON CYBERSECURITY

Cybersecurity is an evolving, ever-changing problem affecting the backbone of our society and economy whilst digital technologies are key enablers of freedom and prosperity. Securing public and private critical infrastructures, networks and information systems in the EU is essential to protect the lives of citizens and to boost market prosperity.

The Cybersecurity Strategy of the European Union outlines challenges in both political and market context. A Cybersecurity Industrial Policy will address such challenges by fostering the setting up of a European-wide market through high level investment in critical technologies and related services, and the development of a European cybersecurity offer.

A Cybersecurity Industrial Policy will only be feasible with strong political support from Member States, EU Institutions and Agencies, and if it is defined in strong cooperation with the industry stakeholders.

Political Dimension

Sovereignty. The current market fragmentation (explained below) is partly due to the fact that security in general, and cybersecurity in particular – especially as a component of critical infrastructures and national assets protection - remains within the EU treaties a national responsibility. Furthermore, cybersecurity cannot be isolated from cyber defence: in sensitive domains like cryptography, this would mean to continue developing, at least to a certain extent, country-specific solutions. Hence, there is a strong link between cybersecurity solutions and sovereignty matters for the Member States which can result in lack of cooperation and lead to increased market fragmentation.

Strategic autonomy. The EU is heavily dependent on non-EU technologies in many domains in the cybersecurity field. Whilst this is not necessarily an issue for commodity hardware and software solutions, it can become a major problem when considering devices manufactured by suppliers outside of Europe's legal frameworks and without full confidence that the devices do not include, for instance, built-in backdoors or are applying the same level of quality requirements. As acknowledged in the joint EU Communication on 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' *"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 vital to ensure that hardware and software*

[2] Intrusion Detection System

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".

Security vs privacy. Security and privacy pursue different goals, however one does not exclude the other and a good balance between the two has to be struck. Sensitiveness to data protection and privacy is particularly critical in the European market, but it is as much of an opportunity as it is a constraint. However, the European industry is ideally positioned to address this issue which has been recognised, by major non-European players, as complex to tackle from outside of Europe.

Market Dimension

EU industrial policies not yet addressing specific cybersecurity issues. Whilst the European Security Industrial Policy[3] and the Communication for a European Industrial Renaissance[4] set out the main roadmap for the development of a more competitive European security industry, they did not specifically address the main problems in the domain of cybersecurity.

Steady level of demand. As already mentioned, the pervasiveness of ICT in our everyday lives is growing rapidly through the increased use of different products and services such as electronic banking, e-commerce platforms, big data, cloud computing, e-supply chain, smart devices and internet of things among others. This is not specific to Europe, but as in any highly developed economy, many innovations in products and services are ICT-driven. The downside to becoming dependent on ICT is that we are increasingly vulnerable to the risks posed by cyber threats. The advantage is that the service based approach in which Europe has demonstrated strengths could be the one in which Europe can better compete.

Market fragmentation. The EU's 28 Member States have different regulations and approaches towards cybersecurity as well as data privacy concerns, which ultimately leads to the development of various specific solutions. More coordination in requirements would bring better interoperability, thus increasing the market size and creating larger opportunities for industry while decreasing development costs.

Innovation is strong in Europe, emanating from ICT labs, SMEs and large players, but not always properly funded due to a lack of a consistent transnational approach. Furthermore, weak entrepreneurial culture, lack of venture capital, and seed money calls for other ways to support innovation with the relevant financial effort and awarding mechanisms efficient enough to keep up with the pace of cyber threats.

Anticipated support from public procurement not yet in place. In its recent assessment of the progress made on the implementation of the EU Cybersecurity Strategy (EC Working Document dated 28 Feb. 2014), the Commission acknowledges (page 23) that concerning the action "*Develop, by the end of 2013, good practices to use the purchasing power of public administrations to stimulate the development and deployment of security features in ICT products and services*", no progress has been made and that *"such good practices will be developed in the near future".*

C) THE WAY FORWARD

Toward an EU cybersecurity industrial policy (CY-SIP)

Considering the situation described above, EU faces a double challenge:

- Enabling a real uptake of cybersecurity industry as a source of growth for the digital economy;
- Guaranteeing its technological independence (based on a logic of strategic autonomy) in such fields where relying mostly (if not only) on non-EU solutions might:

[3] COM (2012) 417 final Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee Security Industrial Policy: Action Plan for an innovative and competitive Security Industry

[4] COM (2014) 14/2 Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions For a European Industrial Renaissance

  - have a societal and cultural impact (this is already the case in ICT at large, where for instance the publishing policy on social networks is dominated by North-American criteria);
  - seriously put into question the protection of data from both an individual standpoint (data privacy) and a collective one (trade information confidentiality and intelligence);
  - represent a threat to critical infrastructures within the EU.

Hence, EOS believes that a comprehensive cybersecurity industrial policy at EU level would contribute to solving these issues by:

- Creating resilient European societies and infrastructures with European cybersecurity technology;
- Boosting the European cybersecurity demand;
- Establishing a competitive European cyber-industrial base;
- Highlighting the need for an international common effort to coordinate cybersecurity policy.

It would also contribute to sustaining the development of the European digital economy by increasing the level of trust in services and infrastructures.

Why do we need such an industrial policy?

Whilst being a strong promoter of free competition as the key engine of economic development, EOS believes that in the specific case of cybersecurity, the market alone will not enable us to solve the identified issues.

Such a policy would not start from scratch: whereas in ICT most hardware and software COTS (commercial off the shelf) products are procured outside the EU, Europe still has a very strong telecommunications industry and a highly developed IT services sector. This is linked to the fact that IT applications development and operations reflect specific business models and local situations (e.g. tax collection applications, social security systems, ICT for mass transportation) which might lead to very different solutions from a Member State to another.

This is also true for network and information systems security, since the deployment of cybersecurity solutions and services impacts business processes, especially with regards to the trade-off between privacy and efficiency on one hand, and protection on the other hand. In other words, ICT in general and cybersecurity in particular have a cultural dimension linked to societal factors that cannot be left aside.

Hence, the setup and implementation of such a policy in Europe would respond not only to legitimate economic and competitiveness objectives, but also to key political priorities.

What would be the elements of a strong EU cybersecurity industrial policy?

There is not much difference between an EU CY-SIP and an industrial policy in other sectors. Ideally, it would rely upon the following pillars:

- A **strategic vision** based on market assessment and “make-or-buy” orientations.
- An in-depth analysis of the **technological dependence** and its consequences on digital economy sustainability, critical national infrastructures, societal impacts and sovereignty issues.
- A coordinated **R&I roadmap**
- A coordinated **public procurement policy:**
  - for the protection of state-owned / operated infrastructures and large governmental ICT systems;
  - for the protection of EU Institutions critical assets.
- A business-oriented, balanced and technology-neutral **regulation framework:**

EOS proposes the following key action points to be taken into account when developing an EU Cybersecurity Industrial Policy:

ACTION: **European strategic vision in cybersecurity industrial policy should contain the following elements:**

- securing European societies with European cybersecurity technology;

- ensuring security of the ICT supply chain;

- encouraging a strong industrial base for a European cybersecurity market with European solutions and services;

- sustain the development of the European digital economy.

ACTION: **European Cybersecurity Industrial Policy should set up a pan-European programme ensuring the protection of EU and national assets and reducing the technological dependency by implementing the following steps:**

- set up major EU cybersecurity investments tied to existing or future assets (border management systems, Galileo, EU networks and the smart grids) and to EU programmes (SESAR, Copernicus);

- set up a coordinated public procurement policy that sets a higher level of coordinated public investment at EU and MS level, analyses how such funds should be used in order to shape EU industrial players, and provides better support mechanisms for high tech SMEs through capital investments;

-promote industry participation in the pan-European cyber exercises whilst gradually extending such exercises into structured activities between European public and private stakeholders.

ACTION: **A coordinated R&I roadmap in cybersecurity should be based on the following:**

- a consistent, overarching strategy that aligns multiple current and future initiatives (TDL, CSP, CYSPA, ACDC, SecCord, etc.);

- R&I work programmes governance procedures should be revisited (procedures of setting up the work programme should take into account lessons learnt);

- a timely and simple administrative processes;

- implementation of PCP schemes to bridge the innovation-to-market gap and harmonisation of specifications.

Beyond the cybersecurity industrial policy, EOS proposes the following action points:

ACTION: **The regulation and policy framework should be more coordinated and harmonised and promote the following:**

- setting up of a European Cybersecurity Coordinator;

- ensure a level-playing field throughout Europe in terms of cybersecurity obligations and responsibilities;

- reach the right balance between incentives and mandatory measures;

- compensate efforts by co-funding and (EU) labelling/certification measures;

- optimise business models linking labelled cybersecurity solutions with insurance premiums;

- promote European standards taking into account international practices;

- invest in awareness and training at all levels (e.g. starting from school to programmes focused on mobility of researchers between academia and industry);

- promote the data protection and privacy culture whilst enabling the take up of new solutions based on such needs;-ensure liability as appropriate, adequate legal response and efficient law enforcement mechanisms.