TOWARDS EUROPEAN DIGITAL STRATEGIC AUTONOMY

Bactech
Business Card Associates
Cabinet Louis Reynaud
CEA Leti
Eurosmart
FingerPrint Cards AB
Giesecke+Devrient Mobile Security GmbH
IN Groupe
Infineon Technologies AG
Institut Mines-Télécom
Keolabs
NEDCARD
NXP
Pôle SCS
Red Alert Labs
Sarapis
SGS
ST Microelectronics
Trusted Objects
Winbond
YesWeHack

10 POINT-MANIFESTO FOR EUROPEAN DIGITAL STRATEGIC AUTONOMY

The Digital Single Market represents a unique opportunity to enhance citizens' confidence in their digital experience and for Europe to lead the worldwide digital revolution. Europe should take advantage of its digital strategic autonomy and rely on the EU to strengthen its cybersecurity capacities. As cyber threats become increasingly sophisticated, Europe's preparation and response to these threats must also evolve. EU countries need to heavily invest in key technologies. At the same time, it is crucial to ensure that these technologies provide the same security level across Europe, especially for critical infrastructures, which is why European cybersecurity certification and ethical hacking should be encouraged.

To enhance its digital autonomy and to protect its digital sovereignty, the European Union must cater for the entire cybersecurity lifecycle within its legislation and initiatives: prediction, prevention, detection and response.

Furthermore, in a geopolitically changing world, trust among EU Member States is a real asset that should be valued. With the cybersecurity industry holding the potential to become one of the most important economic drivers in Europe, products certified under the European certification framework should be promoted. European start-ups should be supported to give them the opportunity to scale up and reach critical mass. Europe currently has a trade deficit for cybersecurity solutions which could be addressed by helping Member States become leaders in the field which in time may enable Europe to become a net exporter.

The fact that European cybersecurity experts can be found around the world working for global leaders demonstrates Europe's expertise in the field. If the EU could incentivise experts to stay in Europe, it could considerably strengthen its cybersecurity ecosystem.

All these issues should be tackled at the European level. The digital world knows no borders and Member States should join forces within the EU. A comprehensive European cybersecurity strategy is needed to achieve digital strategic autonomy, protect Europe's digital sovereignty and compete on the global market.

1 BOOST THE DEVELOPMENT AND DEPLOYMENT OF KEY TECHNOLOGIES

In order to secure Europe against emerging threats the development and deployment of key technologies should be supported. Europe should be at the leading edge of cybersecurity technologies to compete on the world stage. Incentives and fully-fledged policies should support the deployment of secure biometrics, advanced cryptography and trustworthy artificial intelligence. These reliable new solutions are the building blocks of a successful European Digital Single Market.

2 SECURITY AND PRIVACY BY DESIGN

Security and Privacy by Design should underpin any further development of the European Digital Single Market policy. This means that manufacturers and providers should be held responsible for the security and privacy of the entire product lifecycle from design to distribution and use. This is particularly true for connected devices (IoT) aimed at consumers. The possibility for data anonymisation and/or data encryption should be a prerequisite for the EU launch of a product or service which handles personal data. This is a matter of respect for the European fundamental values which apply to every European citizen's digital life.

3 ENHANCE THE EUROPEAN DATA ECONOMY

Data is the critical resource of the digital world and Europe should make the most of its own data. Europe should develop its capabilities in data management. Industrial data, raw sensor and machine data, combined with big data represent valuable industrial capital which is necessary to build artificial intelligence (AI) algorithms. The European Union should protect this capital, safeguard corporate interests, and support research and innovation in this field through dedicated programmes. It should also grant access to relevant data sets.

4 REINFORCE THE GLOBAL POSITION OF THE EUROPEAN STANDARDISATION

The European Single Market should promote open, transparent and secure solutions. The digital transformation necessitates the constant development of interoperable solutions and standards. Europe should rely on the European standardisation organisations (CEN, CENELEC and ETSI) to develop open European standards and to adopt trustworthy worldwide standards. Furthermore, the European Union must make sure that these organisations are well represented within the international standardisation organisations in order to be in a position to influence forthcoming standardisation initiatives and promote EU standards through collaborative initiatives.

5 FOSTER EUROPEAN CYBERSECURITY CERTIFICATION

The European cybersecurity certification framework must ensure the reliability and robustness of information and communications technology (ICT) products, services and processes. By adopting this framework in future European and/or Member State legislation, cybersecurity requirements may become mandatory for new products or services. For these reasons the EU should establish trustworthy cybersecurity certificate schemes according to the potential risk level and based on EU or internationally recognised standards.

In addition, mandatory cybersecurity baseline requirements should be adopted at the European level, for new ICT products and services.

ENISA has the mandate to draw up and manage the European cybersecurity certification scheme framework. In order to do this, it now needs to be allocated the appropriate human and financial resources. For the framework to be a success the cybersecurity community will need to provide the relevant expertise, skills and fairness.

6 PROMOTE AND RELY ON ETHICAL HACKING AND PENETRATION TESTING

Research organisations and industry throughout Europe have a long track record in penetration testing as well as dealing with ethical and white hat hacking which places Europe at the cutting-edge of worldwide cybersecurity. While automatic testing is increasingly being used in low-level security evaluation methodologies, a human must be involved to reach higher levels of security.

This “State of the Art” testing must be supported through European funding programmes (e.g. Horizon Europe and Digital Europe), as well as European certification and standardisation.

7 PROMOTE THE CYBERSECURITY INDUSTRY

The EU cybersecurity policy is unique due to its advanced right to privacy and the level of security required in the digital world which is more advanced in Europe than anywhere else. Europe has been developing advanced cybersecurity and data management technologies and is home to the most important hardware security companies in the world. This is a considerable asset for European citizens who now have reliable technology at their disposal.

The European Union should nurture the cybersecurity industry to enable it to compete on the global stage. A comprehensive and inclusive European cybersecurity industrial strategy should be established with the involvement of the whole ecosystem: industry, SMEs, RTOs, academics, ESOs and the European institutions. This community of stakeholders should be representative of the whole value chain and be underpinned by the principles of transparency and fairness.

Europe’s excellence in cybersecurity should be continuously promoted and valued. Cybersecurity solution providers could benefit from the high quality of the European cybersecurity certification. Together with the certification framework this provides a strong incentive for non-EU industry to certify their products in Europe.

Specific attention should also be paid to SMEs, EU security laboratories and conformity assessment bodies who together represent a significant part of industrial cybersecurity know-how. A large community of experts should be created and supported through specific cascade funding.

A consolidated EU cybersecurity ecosystem should allow European cybersecurity champions to emerge who will be influential on the global market.

8 RELIABILITY OF THE SUPPLY CHAIN AND RESPONSIBILITY OF ACTORS

IDigital is everywhere and involves a large range of actors. In addition to complying with safety standards, connected products and services must include cybersecurity protections. Cybersecurity is a dynamic and constantly evolving field which requires both supply chain actors and the public authorities to anticipate new threats. The EU has a role to play in the definition of the rules for responsibility and reliability of these actors. Continuous effort must be made to prevent, detect and respond to potential attacks. In addition to data protection and ethical hacking, providers should ensure continuous protection throughout the lifecycle of a product or service. This may take the form of updates, patches and upgrades backed by a European vulnerability disclosure and response incident network (yet to be developed).

9 ESTABLISH AN EUROPEAN FRAMEWORK AND INFRASTRUCTURE FOR SECURE APPLICATIONS

Trust over the internet is necessary to ensure strategic digital autonomy. Public Key Infrastructures (PKIs) allow for mutual authentication of parties (client-side and server-side) which creates secure communication channels for data. Currently, however, many PKI applications are not widely accepted due to the lack of access to open, trustworthy, affordable and well-recognised PKI infrastructure.

Decentralised technologies represent one of the most significant innovations in the digital economy. Blockchain, for instance, is very good at creating trust in information and processes in situations where there are large, heterogeneous sets of stakeholders or users. If European infrastructure is set up correctly it will enable European industries to create a network of trust. This in turn will accelerate the digitalisation of business, government agencies and institutions by simplifying the process of building applications which are interoperable within the EU.

The European Union should support the development of an EU Public Key Infrastructure common harmonisation framework. This will enable the development of interoperable solutions for a secure digital space (e.g. cross-border applications for eHealth, eID, intelligent transport systems and e-government services).

Furthermore, the European Union should start an international discussion to negotiate the governance of the DNS with the involvement of ICAAN, ITU and the Member States together with technical support from JRC and ENISA, aimed at guaranteeing the protection of European interests, security and autonomy in DNS governance.

10 CYBERSECURITY EDUCATION

The European cybersecurity strategy should raise civil society's awareness of cyber threats. This is key to enhancing cyber resilience within Europe. This educational effort should span school training to life-long learning. The European Union should invest in its current potential by stepping up its efforts to create advanced scientific curricula especially in emerging technologies. It should also support the cybersecurity research ecosystem and pay particular attention to gender equality.

Finally, while Europe produces a few world-class experts in advanced technologies, it suffers from the brain-drain effect. Without the right expertise, the European cybersecurity industry cannot compete and innovate.

AN INITIATIVE CONDUCTED BY

BACTECH
Biometrics And Cryptography TECHnologies (made easy for you)
business card associates
Ad Usque Fidelis
Cabinet Louis Reynaud
leti
ceatech
EUROSMART
The Voice of the Digital Security Industry
FINGERPRINTS
G+D
Mobile Security
IN GROUPE
infineon
Institut Mines-Télécom
KEOLABS
NEDCARD
NXP
POLESCS
RED ALERT LABS
IoT Security
SARAPIS
SGS
ST
life.augmented
gemalto
a Thales company
TRUSTED OBJECTS
winbond
YES WE HACK