|  |  |
| --- | --- |
| Description: Consumer Rights 9.png |  |
| Association For Consumer Rights (Malta)  Pope Pius XII, Flat 4, Mountbatten Street, Blata l-Bajda  Hamrun HMR 1579, Malta  Tel no 356 21246982, 356 21248881  Email: associationforconsumerrights@gmail.com |

**Association for Consumer Rights AGM 2019**

**Title of Resolution**

**Cybersecurity and Financial payment: The need for a secure ecosystem**

***Name of individual submitting the resolution***

**Grace Attard, ACR General Secretary**

**Background Information**

Cybersecurity is critical to both prosperity and national security, as well as to the very functioning of our democracies, freedoms and values. “Cybersecurity is an ecosystem where laws, organisations, skills, cooperation and technical implementation need to be in harmony to be most effective", states the [UN's Global Cybersecurity Index](https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjbkMTcpvXYAhVDIVAKHa6BCw0QFgg2MAA&url=https%3A%2F%2Fwww.itu.int%2Fdms_pub%2Fitu-d%2Fopb%2Fstr%2FD-STR-GCI.01-2017-PDF-E.pdf&usg=AOvVaw1_QMdsEagc2ghcHlyAc_Ez), adding that cybersecurity is "becoming more and more relevant in the minds of countries' decision makers”

A 2014 study estimated that the economic impact of cybercrime in the Union amounted to 0.41% of EU GDP (i.e. around EUR 55 billion) in 2013[[1]](#footnote-2).

The need for a secure ecosystem is becoming crucial **due to the Internet revolution**. This revolution has not only redefined business-to-consumer (B2C) industries such as media, retail and financial services; it is also reshaping manufacturing, energy, agriculture, transport and other industrial sectors of the economy that, together, account for nearly two-thirds of the global gross domestic product, as well as utilities' infrastructure and people's interactions with public administration

**Justifications, reasons and current situations to be addressed**

**The Digital Single Market Strategy** is built around improving access to goods, services and content, creating the appropriate legal framework for digital networks and services, and reaping the benefits of a data-based economy. It has been estimated that the strategy could contribute EUR 415 billion per year to the EU economy.

A 2014 study estimated that **the economic impact of cybercrime in the Union amounted to 0.41% of EU GDP (i.e. around EUR 55 billion) in 2013[[2]](#footnote-3).**

According to Special Eurobarometer 464a on "Europeans' attitudes towards cyber security", 73% of Internet users are concerned that their online personal information might not be kept secure by websites and 65% that it might not be kept secure by public authorities. Most respondents are concerned about being the victims of various forms of cybercrime, and especially about malicious software on their devices (69%), identity theft (69%) and bank card and online banking fraud (66%)[[3]](#footnote-4).

**So far, no legal framework has been able to cope with the pace of digital innovation**, and a number of legal texts are contributing item by item to establishing an appropriate framework: the revision of the Telecoms Code, the General Data Protection Regulation (GDPR), the Directive on network and information systems security (NIS Directive), the Regulation on electronic identification and trust services for electronic transactions in the internal market (e-IDAS R The regulation), the EU-US Privacy Shield, the Directive on non-cash payment frauds, and so on.

The Cybersecurity Act (2017) proposes **an enhanced role for ENISA** as the EU agency for cybersecurity, granting the agency a permanent mandate. On top of its current responsibilities, ENISA is expected to cover new supporting and coordination tasks related to support for the implementation of the National Information Security (NIS) Directive, the EU Cybersecurity Strategy, Blueprint, capacity building, knowledge and information, awareness raising, market-related tasks such as support for standardisation and certification, research and innovation, pan-European cybersecurity exercises, and the secretariat of the Computer Security Incident Response Team (CSIRT) Network.

**ENISA: *The European Union Agency for Network and Information Security*** (ENISA) is a centre of expertise for cyber security in Europe. The Agency is located in Greece with its seat in Athens and a branch office in Heraklion, Crete.

ENISA's new permanent mandate as proposed by the Commission will significantly contribute to enhancing the resilience of European systems.

**Proposals/Recommendations**

However, the accompanying provisional budget and resources allocated to ENISA will not besufficient for the agency to fulfil its mandate.

All Member States should establish a clear and equivalent counterpart to ENISA, as most of them have not done it yet.

The Agency

* should prioritise actions to support e-government,
* should provide regular reports on the cyber-readiness of Member States focusing on sectors identified in Annex II to the NIS Directive and
* monitor the performance and decision-making of national certification supervisory authorities.

The proposal to create a cybersecurity competence network sustained by a **Cybersecurity Research and Competence Centre** (CRCC) should be a priority .

The human factor constitutes one of the most important causes of cyber accidents. There is a **need to build a strong cyber skills base** and improve cyber information and practice also through awareness campaigns among individuals and businesses.

The cybersecurity skills gap for professionals working in the private sector in Europe is predicted to be 350 000 by 2022[[4]](#footnote-5).

The envisaged European Cybersecurity Certification Group supported by ENISA should be made up of national certification supervisory bodies, private sector stakeholders, scientific and civil society actors.

* Certification activities should include a proper labelling system, to be applied also to imported products to reinforce consumers trust.
* The creation of an EU-certified curriculum for high schools and professionals is an important step to ensure professionals are well trained in cybersecurity developments
* A certification framework and schemes for the different sectors could provide a common baseline.

In terms of capacity building, ENISA should prioritise actions to support e-government[[5]](#footnote-6). EU/worldwide digital identity for persons, organisations and objects which is key, to preventing and combating ID theft and online fraud should be a priority.

ENISA should provide regular reports on the cyber-readiness of Member States, primarily focusing on sectors identified in Annex II to the NIS Directive. A yearly European cyber exercise should assess the readiness of Member States and the effectiveness of the European cyber crisis response mechanism, and should produce recommendations

**Security by design is key** to providing high quality goods and services: smart devices are not that smart if they are not secured, and the same is true of smart cars, smart cities and smart hospitals – they all require built-in security for devices, systems, architectures and services.

**The future**

There are many different organisations further to ENISA, the "EU Cybersecurity Agency", dealing with cybersecurity issues: Europol; Cert-EU (Computer Emergency Response Team of the European Union); the EU Intelligence and Situation Centre (EU INTCEN); European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA); Information Sharing and Analysis Centres (ISACs); the European Cyber Security Organisation (ECSO); the European Defence Agency (EDA); the NATO Cooperative Cyber Defence Centre of Excellence; and the UN GGE (United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security).

The Cybersecurity Package includes a joint communication reviewing the previous European cybersecurity strategy (2013), as well as a Cybersecurity Act focusing on ENISA's new mandate and a proposed certification framework.

* The strategy is structured around three main sections:
* resilience, deterrence and international cooperation.
* The deterrence part focuses mainly on cybercrime issues, including the Budapest Convention, and
* the international cooperation part looks at cyber defence, cyber diplomacy and cooperation with NATO.

The proposal sets out new initiatives such as:

* building a stronger EU cybersecurity agency;
* introducing an EU-wide cybersecurity certification scheme;
* swiftly implementing the NIS Directive.
* The resilience part proposes cybersecurity-related actions addressing in particular: market issues, the NIS Directive, rapid emergency response, the development of EU competence, education, training – in cyber skills and cyber hygiene – and awareness).

With regards to funding, Europe should scale up investments converging different EU funds, national funds and private-sector investments towards strategic objectives in strong public-private cooperation, and future Research Framework Programme

Finally, the EESC believes a minimum security level is necessary for "ordinary" "Internet of People" (IoP) devices. In this case, certification is a key method of providing a higher level of security. Internet of Things (IoT) security should be a priority.

1. [Commission Staff Working Document – Impact Assessment, accompanying the Proposal for a Regulation of the European Parliament and of the Council, Part 1/6, p. 21, Brussels, 13/9/17](https://ec.europa.eu/digital-single-market/en/news/impact-assessment-modernisation-eu-copyright-rules). [↑](#footnote-ref-2)
2. [Commission Staff Working Document – Impact Assessment, accompanying the Proposal for a Regulation of the European Parliament and of the Council, Part 1/6, p. 21, Brussels, 13/9/17](https://ec.europa.eu/digital-single-market/en/news/impact-assessment-modernisation-eu-copyright-rules). [↑](#footnote-ref-3)
3. [Special Eurobarometer 464a – Wave EB87.4 – Europeans' attitudes towards cyber security, September 2017.](https://data.europa.eu/euodp/fr/data/dataset/S2171_87_4_464A_ENG) [↑](#footnote-ref-4)
4. [OJ JOIN/2017/0450 final](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450). [↑](#footnote-ref-5)
5. Digital Single Market/Mid-term revie [↑](#footnote-ref-6)