Center for Cyber Security and International Relations Studies

BALANCING CYBER SECURITY AND INTERNET FREEDOM

"Those who would give up essential liberty,
to purchase a little temporary safety,
deserve neither liberty nor safety"[1]
– Benjamin Franklin

In the modern society of information, whose roots are identified in the so-called Information and Communication Technologies (ICT), one of the main challenges is the hypothesis of a balance of two variables: cyber security and Internet freedom.
The need of balance refers to the peculiarity of the cyberspace to be the domain in which both the geopolitical limits and the rights of the users are redefined. Therefore, the necessity of protecting the security of both the individual and the nation becomes more and more essential.

Crucial is briefly defining the two variables before analysing the hypothesis of a balance. The International Telecommunication Union (ITU) defines the concept of cyber security as "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*"[2]. Nowadays cyber security becomes a continuous process of risk management, based on the ability of networks to resist and defend themselves against threats that may compromise their essential elements.

[1] *Reply to the Governor*, Pennsylvania Assembly, 11 November 1755; in The Papers of Benjamin Franklin, ed. Leonard W. Labaree, 1963, vol. 6, p. 242.

[2] UN ITU, Overview of Cybersecurity. Recommendation UTI-T X.1205, Ginevra, UN, 2008.

The idea underneath the concept of Internet freedom[3] refers here to the denomination "Open – Safe – Secure", proper of the Cybersecurity Strategy of the European Union (2013)[4]. The adjective "open" denotes a global and independent internet, as well as a shared resource among all citizens. An "open internet" is therefore able to promote a process of political and social inclusion by breaking down physical boundaries between countries, creating a forum for freedom of expression and giving power to common people in their search for more just and democratic societies (see, for example, the so-called 'Arab Spring'). Indeed, internet has become the backbone of our society and a resource on which both social interactions and the economies of the world rely (especially in sectors such as energy, transport, health, finance). The undisputed positive aspect of the internet, together with the consequent availability of services and applications, has resulted in an enormous boost to prosperity as well as in opportunities for personal development[5]. However, a negative consequence can be identified in the emergence of new ways of exercising power, which postulate themselves as expressions of a transnational power, often almost imperceptible.

Is therefore possible to guarantee the fundamental rights of citizens online[6] as well as cyber security in the new domain? After analysing several studies[7] and aware of the fact that a unique answer to this

[3] The term 'Internet freedom' consists of a set of rights and freedoms sanctioned and guarded by international conventions for decades. The same concept is a broad term that does not refer to new rights emerged in recent years, but to existing freedoms. It includes several other related terms, such as freedom of expression, right of access, net neutrality and digital rights.

[4] European Commission, February 7 2013, *JOIN(2013) 1 Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace*.

[5] The prerequisite to talk about Internet freedom is the access to the network, which can only be pursued together with non-discriminatory access to knowledge. Considering the pervasiveness of the same in our everyday life, limited or no internet access, as well as digital illiteracy, is today a disadvantage for citizens.

[6] In this context, the expression "fundamental rights of citizens online" especially refers to freedom of expression, protection of personal data and the right to privacy.

[7] Many scholars have questioned the application of the trade-off model. In his text "*Who holds the balance? A missing detail in the Debate over Balancing Security and Liberty*", Sagar expresses the desire to seek the conditions that allow a balance between security and freedom. However, at the end of his analysis, the author affirms that this balance is almost impossible to achieve and maintain over time, as the society is an asymmetric system in which citizens live in a situation of submission towards the 'state structure'. In Sagar's hypothesis, the origin of this imbalance can be found in the 'state secret', the legal constraint that allows the institutions of a given state not to disclose specific information and/or data, even though they can be memorized and reused for any purpose at an indefinite moment. According to this vision, in a process of promotion and accentuation of national security, priority will be given to the integrity of the state, rather than to the protection of individual liberties. Cfr. Sagar, R., *Who holds the balance? A missing detail in the Debate over Balancing Security and Liberty*, Polity 41.2, 2009.

specific question is not advanced by the institutional and governmental world yet, nor from the legal one, the idea of reducing the issue to a trade-off[8] is maybe the easiest one today. From this perspective, if we favour one of the two factors between cyber security and Internet freedom, the other one would decrease proportionally. Therefore, if we would favour safety in absolute terms, the rights of the citizen would slowly erode, possibly leading to the well-known idea of mass surveillance. On the other hand, if freedom on the internet would be fully encouraged in our democratic society, there will be the likelihood for more deviant behaviour to exist in the online environment. It is crucial to underline that is not the technology to be distorted, but the way in which the individual uses it. Is therefore surveillance really the only way to ensure cyber security and the decrease of cyber attacks? In this regard, is significant to underline that the trade-off model proves to be attractive and rather convincing as it is generally popular among those involved in decision-making processes, both at European and national level. Indeed, researches conducted by the institutional world with regard to a possible balance of the two variables addressed, are nowadays difficult to find. At this point of the analysis is important to ask ourselves one question: what do we value the most, security or our privacy?

On the European level[9], is central to highlight the discrepancy between the European discipline, which seems to offer a guarantee of personal data and the discipline of the Member States, characterized by a marked fragmentation and consequential absence of cooperation[10].

[8] The term trade-off means an inversely proportional relationship between two factors, a zero-sum game whereby the increase of one variable inevitably tends to decrease the other one.

[9] After analysing most of the ICT policies of the EU, such as: Bangemann Report (1994), Europe 2020 e Digital Agenda for Europe (2010), European Guidelines and Principles for Internet Resilience document (2011), EU Cybersecurity Strategy (2013), European Agenda on Security (2015), Digital Single Market Strategy (2015), Directive on security of network and Information System (2016), General Data Protection Regulation (2016).

[10] Trimintzios, P. et al. (2015) Common practices of EU-level crisis management and applicability to cyber crises, ENISA.

The protection of personal data has a legal basis in the Charter of Fundamental Rights of the European Union[11] of 7 December 2000 – in particular at articles 7 and 8[12], which has become a legally binding instrument for the European institutions and the Member States after the Lisbon Treaty[13].

With regard to the most recent European legislation, the two variables are analysed in the 2016/1148 Network and Information Security Directive (NIS)[14] and in the 2016/679 General Data Protection Regulation (GDPR)[15], both adopted in 2016 and entering into full force respectively 8 and 25 May 2018. Starting from the end of May 2018, the processing of personal data in Europe have reason to exist only if relevant and limited to the purposes set out, as well as only subject to the prior consent of the interested party, according to the principles of correctness and transparency. Within the same regulation, public administration as well as private companies are obliged to carry out the so-called "privacy impact assessment" to measure the risks associated to data processing in terms of rights and freedoms of the individual concerned. In the GDPR, the related principle of accountability is addressed, according to which 'data controllers' have to concretely demonstrate the adoption of all security measures necessary for the protection of the data in question, as well as having requested a consent to it. The GDPR is therefore to be considered as a first step towards a better protection of personal data of European citizens, even if not the point of arrival yet. At the European and national level, the treatment of personal data still needs greater attention from institutions and decision makers and has not to be subordinated to the security of states. Responding to today's technological developments and to the European economic growth, the GDPR finally sets the rules regarding data protection for all European Member States, conforming them to the same principles.

In the same way, the NIS Directive has to be remembered as a milestone towards the harmonization of Member States in the field of cyber security, as it outlines measures aimed at establishing a high

---

[11] *European Council – Nice 7–10 December 2000: Conclusions of the Presidency*, European Parliament, 11 December 2000, retrieved 23 December 2009.

[12] Article 7 sets out the following: "Everyone has the right to respect for his or her private and family life, home and communications", while Article 8 focuses on data protection, establishing that:

(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for the purpose of the person concerned or some other legitimate basis laid down by law. Everyone has the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority.

[13] European Union, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, 13 December 2007, 2007/C 306/01.

[14] European Parliament and Council of the European Union, July 6 2016, *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*.

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

and common level of security of networks and information systems. Finally, with regard to cooperation, the NIS Directive represents an important step towards improving the general level of security, trust and exchange of information between Member States.

Facing the difficulty of responding unequivocally to the dilemma of balancing cyber security and Internet freedom, a possible solution can be found in the current and future liability regimes.
The thesis of the responsibility of the Internet Service Provider (ISP) can indeed be considered as an initial answer to the impossibility of determining the responsible subjects lying behind cyber attacks. The ISPs are today the intermediaries between the network and the end user, as well as the providers of a service and with more responsibilities they could become the owners of both security and protection of personal data of those to whom they have sold the given network service. Similar to a traditional security system, ISPs would have the ability to observe and filter the traffic entering and leaving their networks, eventually suspending the access to that particular network for all users suspected of intentionally entering ambiguous traffic. Proof of the fact that the thesis of the responsibility of the ISP could actually work are to be found on a global perspective. In many other countries, governments are equipping themselves with measures to implement public-private partnerships (PPPs), in order to improve cyber security through direct cooperation with ISPs. Among these, Australia and Japan are two good examples. Specifically, the Australian government has instituted a so-called "voluntary code of practice"[16], which is a voluntary code of conduct for ISPs, asking them to implement a notification mechanism for all the devices considered to be infected, as well as an updated archive on cyber threats and a reporting system to inform the government directly[17]. Similarly, a collection of over 70 internet service providers has been set up in Japan strictly dedicated to improve IT security, known as the "Cyber Clean Center" (CCC)[18]. The activity of the CCC started in 2006 and is based on the collaboration between the government and the ISPs, according to which they will notify users of current cyber threats and the list of IT devices deemed to be infected. In 2010, Japanese ISPs who decided to participate in the CCC were responsible for

[16] Rowe, B. et al., *The Role of Internet Service Providers in Cyber Security*, Institute for Homeland Security Solutions, June 2011. Link: https://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf.

[17] Internet Industry Association. (2010). *Internet Service Providers Voluntary Code of Practice*. Retrived April 11, 2011. Link: http://iia.net.au/images/resources/pdf/icode-v1.pdf.

[18] OECD. 2010. The Role of Internet Intermediaries in Advancing Public Policy Objectives. Retrieved April 11, 2011. Link: http://www.oecd.org/dataoecd/8/59/45997042.pdf.

sending about 480,000 warning emails to 100,000 users. 31.6% of the alerted users took counter-measures in advance of the threats reported[19].

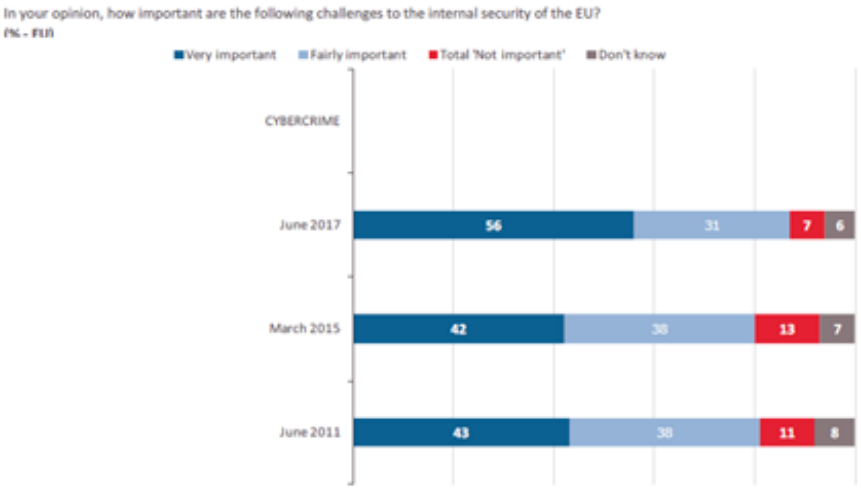
On a global perspective, the trend seems to be oriented towards greater responsibility for ISPs, but for most countries it remains only a hypothesis. The limitation of this thesis mostly regard the concrete possibility for ISPs to provide a 100% secure internet communication system and the economic barriers. In this regard, a problem concerns the economic return for ISPs on the investment linked to the supply of safety filters, additional to the service they offer today. However, a system of economic incentives towards the ISPs by governments or by the public-private partnership would also be conceivable[20].

The dilemma of balancing cyber security and Internet freedom faces another limit: the awareness of EU citizens. Thanks to the recent report called “Special Eurobarometer 464th: Europeans' attitudes towards cyber security", released by the European Commission in September 2017, is easier to highlight the problem.

[19] Cyber Clean Center, Project coordinated between Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry, 2010. Link: https://www.telecom-isac.jp/ccc/info/en_index.html#annual.

[20] In the European jurisdiction the ISP does not have an active role in the liability regime, but rather only the provision of tools that allow the user to perform online activities. According to this perspective, it is the user himself who responds to his activities on the internet. The European legislation, according to Directive 2000/31/EC, divides the activities carried out by the ISP between "mere conduit" (simple transport), "caching" (temporary storage) and "hosting". Despite the existence of a European legislation on the matter, the judges of the individual Member States gave different interpretations on the attributions of responsibility for the ISPs. In Italy the Directive 2000/31/EC was implemented with the legislative decree n.70 of April 9 2003 (See: Decreto legislativo 9 aprile 2003, n. 70, *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno*, pubblicato in G. U. n. 61 del 14.04.2003), which differentiated the liability regimes according to a proportionality principle, for which the responsibility of the ISP is related to the pervasiveness of the activity. In 2017, Gentiloni Silveri releases the law n.167 of November 20 2017, known as "Legge Europea 2017". The main provision of the law in question concerns a substantial extension from 2 to 6 years (72 months) of the data retention, which means the storage of data both by telephone and from the Internet (regardless of the presence or absence of an illegal behaviour) in the hands of providers and available to the judicial authorities. The most obvious contradiction lies in the application of this law in view of an adaptation to the community rules, when in reality the latter support the conservation and consultation of user data only if certain illicit activities exist.

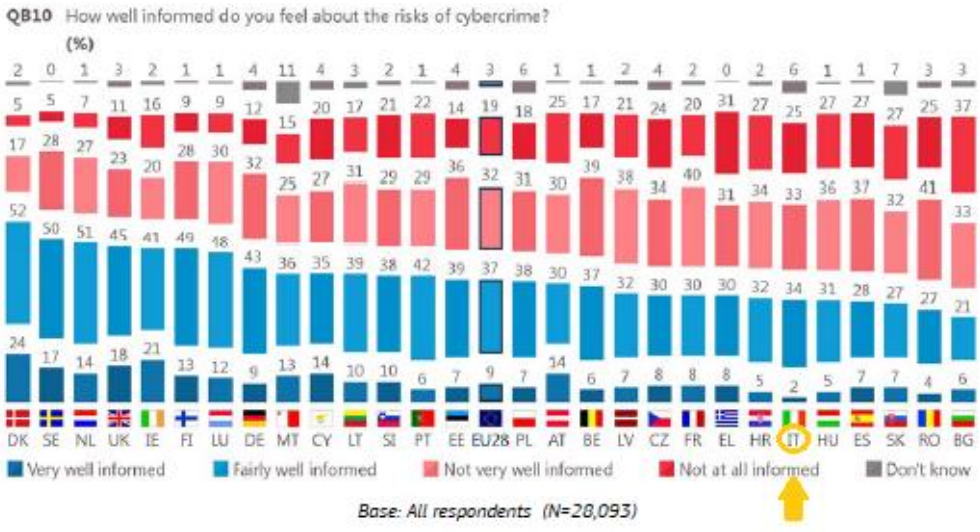
Figure 1. How important are the following challenges to the internal security of the EU?



"*Special Eurobarometer 464°: Europeans' attitudes towards cyber security*",
Directorate-General for Migration and Home Affairs, European Commission, 2017,
http://ec.europa.eu/commfrontoffice/publicopinion

The behaviours and perceptions of the 28,093 interviewees concerning the issue of cyber security highlight the consequential issue of the digital divide and the educational urgency[21] in the field, today necessary more than ever. It is clear that the reduced awareness related to both cyber security and the rights of the user in the online dimension, definitely leads to less effort to defend both.

Figure 2. How well informed do you feel about the risks of cybercrime?



"*Special Eurobarometer 464°: Europeans' attitudes towards cyber security*",
Directorate-General for Migration and Home Affairs, European Commission, 2017,
http://ec.europa.eu/commfrontoffice/publicopinion

[21] The expression 'educational urgency' refers to the need of educating citizens on a realistic understanding of the risks that every day they meet online and teaching them ways to avoid, or at least mitigate, the impact of cybercrimes.

When analysing the graphs and results of this report[22], it is crucial to bear in mind that the percentages reported so far refer to a sample of 28,093 citizens from 28 EU member countries, only partially considering the differences between the countries themselves. Looking at figure 2, if we compare the percentages of Italian citizens who consider themselves as 'very well informed' regard cybercrime to many countries in Northern Europe, the educational urgency in the field emerges.
In this regard, it should be considered that the lack of awareness inevitably feeds a feeling of fear originated by the citizens themselves, which will progressively increase the trade-off between the two variables. The more the citizens are frightened by the loss and/or the theft of their personal data, the more they will approach the idea that security measures are necessary to curb this possibility, at the cost of sacrificing their privacy in full. At the same time, without digital skills it will never be possible for citizens to defend themselves from any kind of surveillance.

In conclusion, is necessary to underline the urgency of an international regulatory framework for the cyberspace, which has to be recognized and accepted by both potential executors and victims of cyber attacks, since cyber security is a shared responsibility. As already highlighted, the main obstacle in this process, which will inevitably have to be realized in the near future, lies in cross-border cooperation[23] between States and in particular in the general reticence of European Member States in revealing their strategic assets[24].

[22] In light of the same report, it is clear that the percentage of European citizens who consider themselves sufficiently aware of cyber security surpass half of the sample.

[23] "Cross-border cooperation took place in a closed circle of trust" – European Commission, September 13 2017, SWD(2017) 295 final, *Assessment of the EU 2013 Cyber Security Strategy*, p.8.

[24] Trust among Member States is a crucial issue also for the biggest challenge, namely the construction of multi-level cyber resilience, the first line of defence against cybercrime. Nowadays, only a small number of IT accidents are communicated by the states in which they occur. In this regard, ENISA plays a key role in promoting a model of cyber security in which core values become transparency, followed by trust and information sharing.

BIBLIOGRAPHY

Bangemann Group, 1994, '*Report on Europe and the Global information Society*', Bulletin of the European Union, Supplement 2/94.

Cyber Clean Center, Project coordinated between Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry, 2010. Link: https://www.telecom-isac.jp/ccc/info/en_index.html#annual.

Decreto legislativo 9 aprile 2003, n. 70, *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno,* pubblicato in G. U. n. 61 del 14.04.2003.

European Commission, March 3 2010, *COM(2010) 2020 Europe 2020: a strategy for smart,sustainable and inclusive growth*.

European Commission, May 19 2010, *COM(2010) 240 Digital Agenda for Europe*.

European Commission, February 7 2013, *JOIN(2013) 1 Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace*.

European Commission, April 28 2015, *COM(2015) 185 The European Agenda on Security.*

European Commission, May 6 2015, *COM(2015) 192 A Digital Single Market Strategy for Europe.*

European Commission, September 13 2017, SWD(2017) 295 final, *Assessment of the EU 2013 Cyber Security Strategy*

European Parliament and Council of the European Union, July 6 2016, *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.*

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, September 13 2017, *JOIN(2017) 450 Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.*

European Council – *Nice 7–10 December 2000: Conclusions of the Presidency*, European Parliament, 11 December 2000, retrieved 23 December 2009.

European Parliament and Council of the European Union, July 6 2016, *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*.

European Union, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, 13 December 2007, 2007/C 306/01.

Internet Industry Association. (2010). *Internet Service Providers Voluntary Code of Practice*. Retrived April 11, 2011. Link: http://iia.net.au/images/resources/pdf/icode-v1.pdf.

OECD. 2010. The Role of Internet Intermediaries in Advancing Public Policy Objectives. Retrieved April 11, 2011. Link: http://www.oecd.org/dataoecd/8/59/45997042.pdf.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Reply to the Governor, Pennsylvania Assembly, 11 November 1755; in The Papers of Benjamin Franklin, ed. Leonard W. Labaree, 1963, vol. 6, p. 242.

Rowe, B. et al., *The Role of Internet Service Providers in Cyber Security*, Institute for Homeland Security Solutions, June 2011. Link: https://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf.

Sagar, R., *Who holds the balance? A missing detail in the Debate over Balancing Security and Liberty*, Polity 41.2, 2009.

Special Eurobarometer 464°: Europeans' attitudes towards cyber security", Directorate-General for Migration and Home Affairs, European Commission, 2017, http://ec.europa.eu/commfrontoffice/publicopinion

Trimintzios, P. et al. (2015) Common practices of EU-level crisis management and applicability to cyber crises, ENISA.

UN ITU, Overview of Cybersecurity. Recommendation UTI-T X.1205, Ginevra, UN, 2008.