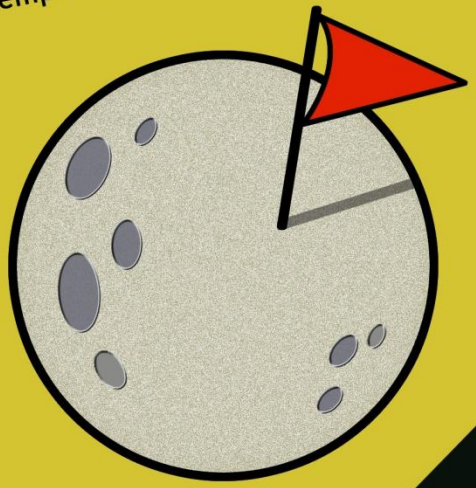
CYBERLAW by CIJIC

# DIREITO: A PENSAR TECNOLOGICAMENTE

Em pleno século XXI, o ciberespaço assume-se como o novo plano da acção. Este, representa, entre outras dimensões, um conjunto cada vez mais alargado e eficiente de meios de comunicação e de informação ao serviço do Homem. A sociedade hodierna, inebriada por esta revolução tecnológica, numa quase-metamorfose híbrida, adapta-se a esta tecno-dependência. Mas, será que compreendemos, minimamente, o advento do ciberespaço e do tempo moderno em que vivemos?



CIJIC
Centro de Investigação Jurídica do Ciberespaço
da Faculdade de Direito de Lisboa

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

CYBERLAW by CIJIC

CYBERLAW by CIJIC Revista científica sobre *cyberlaw* | Número 01 janeiro 2016 | Grátis

DIREITO: A PENSAR TECNOLOGICAMENTE

**cyber espaço**
novas fronteiras

**cyber ataques**
algumas estratégias de mitigação

**cyber segurança**
preocupação global

**outros**
- direito constitucional do Inimigo
- obscurantismo
- DOTMLPI-I
- ENISA


CYBERLAW
by CIJIC

CYBERLAW by CIJIC

# INTERVIEW WITH ENISA'S EXECUTIVE-DIRECTOR PROFESSOR UDO HELMBRECHT

# ENTREVISTA COM O DIRETOR-EXECUTIVO DA ENISA : PROFESSOR UDO HELMBRECHT


**Professor *Udo Helmbrecht***


## ABSTRACT

*ENISA is a well-established agency known by its relevant stakeholders. Via the so called Art. 14 procedure of our regulation, ENISA recommendations are quoted, and it is explicitly mentioned in EU sector directives.*

*Cyber security is a key priority for most EU Member States. However the approach each country takes on the topic is diverse and according to their national requirements. Harmonized implementation of legislation creates a level playing field and makes it easier for asset owners and users to operate across different EU countries. ENISA plays a key role in encouraging the harmonised implementation of security requirements.*



**Keywords:** ENISA; Cybersecurity, ICT; Privacy Enhancing Technologies; Trust;

# Interview Questions

«*Prof. Udo Helmbrecht is the Executive Director of ENISA since the 16th of October 2009. Prior to this, he was the President of the German Federal Office for Information Security, BSI, for six years, between 2003-2009.*[1]»

First of all, let me thank you for the immediate availability shown on helping us with the construction of the Cyber Law Research Centre at the Lisbon Law School.

This interview is intended to give the tone, the right one, for the beginning of our scientific research at the Centre.

Beyond this minor introductory part, I've picked one *résumé* from the ENISA's webpage. Your CV available at https://www.enisa.europa.eu/about-enisa/structure-organization/executive-director, almost *talks* for itself.

Let's start with a *slight* provocation,

1) Who is Udo Helmbrecht?

Looking to your motivation letter - to your visions - prior to your nomination, in 2009 (*also available at ENISA's website*), to last year's full trust vote, when the ENISA Management Board decided to extend your term of office for more five years, do you feel like the right man at the right track?

*Of course am I the right man at the right track; otherwise I would not do this job.*

2) And about ENISA, this laborious task of its implementation, winding its way slowly since 2004, after 10(ten years) of hard work… what's ENISA in the present moment?

*ENISA is a well-established agency known by its relevant stakeholders. Our recommendations are quoted, we are explicitly mentioned in sector directives like in the telecommunication package, eIDAS directive or the just negotiated NIS directive.*

1Text available at ENISA: https://www.enisa.europa.eu/about-enisa/structure-organization/executive-director.

*Commission and Member States ask for our support, e.g. like CERT trainings, via the so called Art. 14 procedure of our regulation.*

3) Regarding Cyber Law, one of the countless challenges facing the security of information and networks still consists in the fact that most of the Member States have their own interpretation of the legal framework that should be established at national and European level for that purpose. Even now, after facing the recent Digital Single Market's initiatives announcement, many of the Member States still insist on maintaining different priorities and taking opposite approaches. Moreover, the fact that the legal landscape in that area is so fragmented, since it touches so many topics (and controversial topics), such as privacy, criminal law, trade secrets and national security, makes it difficult to find a common ground.

Do you think that one major step towards a joint European cybersecurity commitment is a unified vision of the legal framework that should be established at an European level? Shouldn't it be the priority? If you agree that it should, what would be, from your point of view, the best way to keep Member States on the same page, in what concerns cybersecurity?

*Cyber security is a key priority for most EU Member States, 23 countries have already adopted a national cyber security strategy - the key policy document providing the actions to take place to enhance cyber security in a national level. However the approach each country takes on the topic is diverse and according to their national requirements, i.e. some countries have developed specific action plans drawn by legislation, some others have created working groups per critical sector to focus on tackling the cyber security issues, others include cyber security in the mandate of the body responsible of national cyber security, etc.. These approaches depend on the national assets that need to be protected and on the culture of the country.*

*Harmonized implementation of legislation creates a level playing field and makes it easier for asset owners and users to operate across different EU countries. ENISA plays a key role in encouraging the harmonised implementation of security requirements by stimulating the dialogue amongst various stakeholders across Europe and maintaining a number of technical experts' communities. The article 13a (security and integrity in*

*electronic communication networks, Directive 2002/21/EC) and NCSS (National Cyber Security Strategies) working groups are typical examples of such communities maintained by ENISA.*

4) Last March, at «*Technologist*», again, you've noticed that «*We're missing a vertical approach to escalating decision-making – taking the problem from a technical level up to a politic level*». You emphasized the problem of not having one «*well-established escalation procedure*[2]». Do you see ENISA filling that gap, setting out an escalation procedure and becoming, in the near future, the Network and Information Security European Regulator?

*It is the approach of ENISA to situate its work in between the high level policy initiatives and the low level technical work supporting the Member States in implementing the provisions of EU policy initiatives. Having said this, the decision on whether an EU European Regulator on Information Security is required is entirely up to the National Authorities.*

5) The nature of the Internet and other computer networks gets in the way of dealing with cybersecurity matters. As you noticed before, «*When you talk today about the Internet, it is the "Wild West*[3]*"*». Does that anarchy, that still characterises the Internet and other computer networks – and that is one of its key attractive features – should be limited or even put to an end by an appropriate control?

*As you rightly note this 'anarchy' that characterises the Internet is one of its key attractive features.*

*Perhaps the best answer to this question is that the 'anarchy' should be limited where necessary in order to protect citizens and provide an environment from which all communities can benefit. The challenge for the policy maker and an Agency like ENISA is to come up with the best balance in terms of appropriate controls. I do admit that this*

2 See text available at http://www.technologist.eu/europes-cyberdefence/ .
3 Text available at http://www.euractiv.com/sections/infosociety/cyber-security-directive-held-face-wild-west-internet-313431.

*is not an easy task. For example, you may recall the recent discussion at Members States as well as the European Parliament on allowing or not the use of encryption technologies for public communications.*

6) It's no overstatement to say that much of the growth and richness of the *Internet* itself and other computer networks and information technologies thrived through that singular human feature: «Confidence»(*Trust*).

Latterly, with all those ablaze «*mass surveillance*» cases *affecting* European citizens; with all those cyberatacks that have been reported in major European organisations, with the disclosure of sensitive personal data of millions of customers; and recently, with the CJEU *striking down*, on October 6th 2015, the Safe Harbour data transfer agreement (on the grounds of insufficient guarantees that the companies would comply with the European data protection rules), do you believe that we should continue to "trust in and through" *this necessary and additive technology*? And if we do, is there any way to *counteract* attacks on confidence? Are we still able to entice the trust of 500 million consumers for the Digital Single Market (DSM)?

*In my view the pervasiveness and richness of the content of Internet contributed to its amazing growth. Having said this I agree with you that especially due to recent developments, issues such as Confidence and Trust are becoming of great importance. ENISA is convinced that the area of 'online trust and confidence' is an opportunity for European ICT industry!!! Moreover, the pervasive nature of the Internet and its services forces both industry and policy and policy makers to do their outmost in order to ensure that confidence on the network and its services is set at high levels.*

7) Again, «*Trust*». Is there any way we could establish a based trust-system, from private to public partners, if the temptation of one «mandatory reporting duty» is on the edge of the planned European cybersecurity legislation?

Assuming «Trust» as the kernel of the business relationship (let's think, for instance, Finance, Bank, Stock-exchange, Health, along with many other sectors), isn't a «mandatory report duty» a kind of *assault* to that kernel (private or even public)? As we

know, many of the organizations don't disclose the fact that they have been attacked, serving to lessen the overall perception of risk, so, isn't that «mandatory report» seen as a kind of disincentive to the higher level of resilience intended to create?

*An example for trust building that works well and also scales for larger groups is set by operational communities, especially the CSIRTs. This mechanism makes use of a "trusted introducer" process, where capabilities and other issues are checked by other teams. In more sensitive environments, where sensitive information needs to be shared, there are vouching mechanisms in place, where for example at least two other already introduced teams need to vouch for a newcomer. This kind of trust building works quite well in everyday business, and could be adopted in other environments as well.*

8) Lets take the singular case of Portugal. Most of its business structure depends on SME's (small and medium enterprises) which operate with very strict budgets. Most of the times, these organizations, eventually yield its cyberprotection to those off-the-shelf programs. Moreover, we see that *Security, [it] is being added on carelessly, and, worse, afterthought rather than a design priority*, as William Saito[4] unerringly noticed. This is normally due to budget constraints.

We need to think broad, and start looking for ways of incentive. The cybersecurity task is immense. Why not start by discussing tax incentives to those SME's organizations when implementing cybersecurity measures?

*The fact that higher security comes at an increasing cost is becoming more and more obvious to many decision-makers; therefore tolerance of some level of insecurity is necessary for economic reasons. From an economic perspective, the key question is whether the costs and benefits perceived by market players are aligned with the social costs and benefits of an activity.*

*As the Internet itself can be seen as a public good, it is likely that ICT security shows public good characteristics as well. The consumption of public goods is not affected by rivalries in the domain or by excluding interested parties from involvement.*

4 See text available at http://www.huffingtonpost.com/william-saito/why-internet-security-mat_b_6527104.html.

*Total security is neither achievable nor desirable. Hence, each actor will carefully make a trade-off between costs and benefits associated with ICT security investments. Some level of ICT security is, however, a prerequisite for the globally interconnected economy to work. This is also true for the Internet's services to function. Basically a secure ICT infrastructure resembles a functioning banking sector, which is essential for doing business. Malevolent or careless users can cause harm to other users. Further incentives to invest in security are often misaligned as parties do not have to bear the costs of their behaviour entirely, if at all.*

*Due to these effects, ICT security can be regarded as a public good. If the existence of a public good is desired by society, its provision has to be safeguarded by means of regulatory intervention from some superseding level of governance. To these means pertain, e.g. legislation (such as liability laws), taxes, requirements, bans and rules and quotas, often designed to fight external effects.*

9) Much of ENISA's software resources are based upon open source products. In a different way, critical infrastructures and Industrial Control Systems (ICS) products are mostly based on standard embedded systems platforms which often use commercial *off-the-shelf* software. The reduction of costs and improved ease of use can be taking place at the cost of cybersecurity and this might open the door to computer network-based attacks. Is it possible to create a capability that allows us to test and evaluate our software? Are we able to rate the security of our software? And what should be the form of control when we deal with the continuous and *gushing* migration to cloud computing, transferring to third parties the decision on the software to use?

*Although the industry is moving in the direction of developing security through the use of standards, recommendations and guidelines established by certification bodies and/or public–private initiatives, there are still several areas where there is room for improvement: poor software development practices, fast testing and objective measuring, official security certifications, current status of new security standards development, etc. All these needs could be addressed by a common test bed framework, which allows for testing ICT, processes and components against specific security requirements.*

*Security testing certification needs a holistic and human-centric approach and as a result security cannot be rated with absolute numbers. Security-certified ICT systems and components need to be operated by competent organisations and personnel. Security testing and certifications of components and organisations and key personnel set the minimum accepted level and can be further elaborated with a "Competence Bonus" to motivate incident reporting and problem solving.*

10) Looking at the cybersecurity chain, we recognize that its weakest link is the «human factor». From social engineering, to lack of skills or knowledge, to unsafe behaviours, all of us concede that it is far difficult to modify existing routine actions. And all the cyberattackers know it also.

Peter Warren Singer have one interesting proposal on «*how to save the Internet*[5]». He compares the effect of CDC (Control Disease Centre) in 1940/50's for the human physical health with a similar approach to the informational and cyberhealth in the present time. Do you believe that we might have one chance to build our cybersecurity centres' based on that Singers' singular proposal[6]?

*Your example has similarities to the approach followed by ENISA namely to situate its work in between the high level policy initiatives and the low level technical work supporting the Member States in implementing the provisions of EU policy initiatives. Having said this, such decisions on the exact role of National and/or a European cyber security centre rests entirely up to the EU Member States.*

5 See article available at http://www.wired.com/2014/08/save-the-net-peter-singer/

6 Lets, for instance, assume that the CDC, serves as a *fusion centre*, where the public and private poles can merge their interests: on the one hand, the State accepts its *natural* obligation of (cyber)scientific research (since the cost associated with scientific research is of high provision) and its further dissemination of knowledge; and, on the other hand, the private sector, noting the independence and impartiality of the centre itself, walks toward it in a voluntary basis in a lightly way, devoid of that burden of the mandatory report. Could this help on creating and promoting the much-vaunted and needed cyberawareness?

11) In the past, in 2013[7], at *Deutsche Welle*, when asked about all the possibilities, technical or legal, linked to the «*right to be forgotten*», you've noticed that *«Ultimately, it comes down to the realization that the Internet never forgets!»*.

Viktor Mayer-Schonberger, for instance, seems to have one, even *hypothechnical*, solution to this particular subject. Why not the use of «*Expiry dates*[8]» (maybe, digital time stamps) attached to our digital footprint? Would you subscribe that solution?

*The idea of 'ephemeral messaging' or simpler 'disappearing messages' has been investigated by researchers as a possible solution towards establishing trust online. At this moment in time we are still at a phase in Europe where we recognise the need to deploy Privacy Enhancing Technologies (PETS) in order to safeguard EU citizen privacy as well as the position of EU industry. This is also reflected in the General Data Protection Review.*

*The next challenge for Europe for the coming years would be to translate this into a set of technologies that when combined could enhance online trust. Which are these technologies is still not clear. A number of candidates exist like the one you describe. It is clear however that one technology will not suffice and a combination of techniques would be required. ENISA has been working for a number of year in assessing the maturity and potential of privacy enhancing technologies especially in view of the upcoming General Data Protection Review. In this respect, I believe that we are very well positioned in providing support to Member States in implementing the provisions General Data Protection Review.*

12) Finally, how do you envision the development of research centres for cyber and related matters? What role do you think they could play in the near future and, possibly, in connection with ENISA?

---

7 See article available at http://www.dw.com/en/the-internet-never-forgets/a-16996942.

8 At the *NJ.com*, in 2009, *Mayer-Schonberger* pointed out the following: «*Expiry dates is just a piece of meta information that we would enter when we store a file or a document in our computer and we would be prompted by our computer not just to enter the file name and the location where we want to store it, but also a expiry date. When that date is reached our computer would automatically purge that file or that image from our system. Of course, we would be perfectly free to change the expiry date anytime we want if we change our mind if we think we want to preserve an image for longer or delete it much faster*» (available at http://blog.nj.com/njv_kelly_heyboer/2009/11/will_the_internet_let_us_forge.html).

We consider research in the cyber security area as very important, where we can we offer our support for institutions and researchers, but sadly we can do this only on a best effort basis, due to our small size and lack of resources. So as much as we consider this important, we cannot engage in research ourselves. But we are open for formal and informal agreements, or maybe staff exchange in limited, well-chosen cases.

13) Do you have some final words to our Cyber Law Research Centre[9], Professor Udo?

*I would like to welcome your initiative and your Cyber Law Research Centre that are the kind of initiatives that we can bring an important added value for our society. The cyber space is growing and developing so fast and changing the way people and society interact. The impact is not only in business but also in the private life of all of us and the legal challenges are increasing to keep the balance between technology and supported development and fundamental rights. All this in line with the vision that is expressed in the Lisbon Treaty for all Europeans. ENISA will continue to work towards the citizens' through the Member States via Industry, Academia and all other related stakeholders that play a crucial part in the development as your Cyber Law Research Centre. Congratulations for the initiative and for the help on Building a Secure Cyber Space in Europe.*

[9] This interview, conducted by Nuno Teixeira Castro - on behalf of CIJIC - was only possible due to the unsurpassed support of ENISA's staff, namely, Sofia Andrioti and Paulo Empadinhas.