ENISA today and in the future

Udo Helmbrecht

Executive Director

ENISA

Council Working Party
on Telecommunications and Information Society

Brussels, 20th September 2011

Check against delivery

Ladies and Gentlemen,

Thank you for the invitation to speak here today. I am very pleased that you have given me the opportunity to talk to you about ENISA's work and how it might evolve in the future to meet the needs of Europe.

Network and Information Security Today

ICT dependencies

Information and communication technologies (ICTs) are the backbone of today's global information society: for governments, for businesses and for citizens. Since 1995 the internet has become a vital medium of our economy and our social life: online-shopping, social networks, mobile communication, cloud computing are all examples of technologies that have come to play an important part in our daily lives.

Vice-President Commissioner Kroes has put forward the Digital Agenda for 2020, with the objective of improving the quality of life through, for example, better health care, safer and more efficient transport solutions, a cleaner environment, new media opportunities and easier access to public services and cultural content[1].

Threats & opportunities

Unfortunately, the significant benefits that ICTs afford us are accompanied by a number of new threats. These threats are not only due to vulnerabilities associated with new technological developments – they are also due to the fact that these technologies are being used to attack systems. ICT is increasingly used in cybercrime and politically motivated attacks.

Organised crime

In the recently released organised crime threat assessment from Europol, it is noted that the Internet is "a facilitator for organised crime". They note that "A new criminal landscape is emerging marked increasingly by highly mobile and flexible groups, operating in multiple jurisdictions and criminal sectors, and aided, in particular by widespread, illicit use of the Internet."[2]

Improving the capability for dealing with cyber-attacks is part of the objectives of the EU Internal Security Strategy, which states that, "Europe is a key target for

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

[2] http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA_2011.pdf

cybercrime because of its advanced Internet infrastructure, the high number of users, and its Internet-mediated economies and payment systems."[3]

ENISA acknowledges the importance of the fight against cybercrime as well as the need for a strong collaboration between Computer Emergency Response Teams (CERTs) and law enforcement. The role of ENISA in this area is to work together with the CERT and Law Enforcement communities and to ensure that the full potential of the CERT community is being used in the fight against cybercrime.

The evolving threat landscape

ICTs are vulnerable to threats which evolve as a result of technology and market developments. Such threats are global in nature and are not aligned with national boundaries. Therefore, as ICTs are global, interconnected and interdependent with infrastructures, their security and resilience cannot be secured by national approaches. There is a need for a comprehensive framework at the EU level that will enable us to stay ahead of the threats, or at least be up to speed, throughout Europe. Network and Information Security (NIS) is vitally important to modern communications, economic growth and development, and to social cohesion.

Of course it is not only threats that are evolving. The countermeasures to tackle them have also changed. These developments include improvements to networking best practices, more focused policies, regulations and directives, increased insight into multi-sector implications of security issues and the recognition of the importance of having a global perspective on NIS.

Ensuring a coherent pan-European approach

Any future approach to securing Europe's ICT systems must be coherent across geographical borders and communities and consistent in time. This is clearly not the case at the present time, where different approaches to securing information and systems are developed independently in different Member States and in different communities.

Even at a more technical level, there is evidence that the approaches we have defined to date need to be improved. As an example, it is clear that it makes little sense to separate the protection of infrastructure from the applications which run on top of it. Those who choose to attack systems do not make the distinction between the two – they simply exploit the weakest link. For example, with botnets[4] home

[3] http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf
[4] http://en.wikipedia.org/wiki/Botnet

users' computers can be infected with malicious software, such as a Trojan horse[5]. The computers can then be remotely controlled to attack governmental websites and online services. An example of this was seen in the 2007 cyber-attacks against Estonia.[6]

ENISA has developed a network of contacts across Europe that includes all Member States and that spans many different communities. ENISA will continue to strive for an approach to securing our systems and information that is coherent across all of these dimensions, and that is aligned with what is happening in other international communities.

Building on progress

In summary, whilst it is clear that threats will not cease to develop, each new development brings with it corresponding opportunities for improvement.

As I have already demonstrated, we are increasingly aware of how sensitive and how vulnerable to attack our infrastructures are. Unfortunately, we lack adequate information by which to be able to recognise and react to dangers in due time. Here, I see a real opportunity for Member States to use ENISA more effectively, by asking the Agency to collect and analyse data relating to information security in a cross-border context. Such an approach is likely to reveal trends that are not visible at present.

The communication on CIIP[7], from March this year, shows, that we have, on a pan-European level, already made several important first steps to improve our approach to cyber security and our ability to respond effectively to other forms of disruptive events. ENISA is playing a key role in facilitating much of this activity, and we expect to improve the impact of our activities even further with the strengthened role associated with the new mandate.

[5] http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29

[6] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

ENISA's work in 2010

ENISA's operational activities in 2010 are described in our general report.[8] Our work and deliverables were divided into the following five main areas:[9]

- Computer Emergency Response Teams (CERTs)
- Identity and Trust
- Resilience
- Risk Management
- Awareness Raising

The Agency interacted with a broad range of stakeholders across Europe and beyond, for example, by participating in the relevant working bodies of international organisations such as the OECD's Working Party on Information Security and Privacy (WPISP). ENISA also received two formal requests. One was from Romania to help set up a CERT, while the second was from the European Parliament and related to the establishment of an agency for the operational management of large-scale IT systems. Responding to requests is an activity where the current mandate limits the Agency considerably, and it is positive that there are recommendations to enhance the Agency's ability to accommodate requests made by Member States and other stakeholders. I will return to this point later on.

In addition, the first Permanent Stakeholder Group (PSG) to be appointed by me, as Executive Director of ENISA, took office on the 17th of February 2010.

Finally, a new process for developing future work programmes, based on stronger stakeholder involvement, was implemented.

ENISA's work in 2011

The 2011 work programme[10] is divided into three Work Streams:

- ENISA as a facilitator for improving cooperation
- ENISA as a competence centre for securing current and future technologies
- ENISA as a promoter of privacy and trust

[8] http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/TPAB11001ENC.pdf

[9] http://www.enisa.europa.eu/media/key-documents/enisa-work-programme-2010

[10] http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011

Together they contain thirteen work packages. It would be too ambitious to try to cover all of these in this speech. I will therefore give you a summary of some of the more important elements of the Work Programme.

The criteria used for the evaluation and selection of work packages was to evaluate whether they respond to specific regulatory and policy needs: whether they add a measurable value, on a European level, to NIS by anticipating demands and working together with European stakeholders; whether they contribute to both public and private sector objectives; whether they create impact that is clearly attributable to specific categories of stakeholders; and finally that they do have overlap with or duplicate on-going work.

ENISA as a facilitator for improving cooperation

Work Stream 1 is essentially dealing with two distinct areas: CIIP and the strengthening of CERTs in Europe. I will return to these activities later.

ENISA is also supporting the establishment of an EU institutional CERT and has Agency representatives both within the 'pre-configuration team'[11] and the Steering Committee.

ENISA as a competence centre for securing current and future technologies

In Work Stream 2, we are working with the public and private sectors to correctly secure new technologies and business models such as those arising from the adoption of cloud computing. Here, we are collaborating closely with other areas of the European Commission, notably DG INFSO Directorate F, where we will be involved in an advisory role in the next call for research projects under Framework Programme 7 (FP7).

ENISA as a promoter of privacy and trust

In Work Stream 3, ENISA is working with a number of other EU institutions and bodies (the Commission, the European Data Protection Supervisor and the Article 29 Working Group) in order to ensure that EU privacy laws can be implemented in a realistic and meaningful way on modern IT systems.

The work that ENISA is performing in Work Stream 1 is directly supporting the CIIP Action Plan, as laid down in the Commission Communication of March 2009 - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing

[11] The team is tasked with establishing the operational CERT for EU institutions within approximately one year.

preparedness, security and resilience".[12] It is therefore worthwhile to explain this work in a little more detail.

CERTs in Europe

Since 2005, ENISA has run a programme dedicated to reinforcing national and governmental CERTs. The goals of this programme are to support the EU Member States in establishing and developing their national and governmental CERTs according to an agreed baseline set of capabilities, and to generally support and reinforce CERT cooperation by making available good practice. Most Member States have already established official national/governmental CERTs. But there are still a few which either do not have such a team, or have one that is not yet fully operational. Besides this, there are national/governmental CERTs which participate in well-functioning networks. Finally, there are Member States which have national/governmental CERTs that are either not integrated in informal structures (TF-CSIRT[13] and FIRST[14]) or are unknown to CERTs in other Member States.

ENISA seeks to reinforce cooperation by analysing barriers for cross-border cooperation and proposing measures to tackle them. An example of how this is being achieved in practice is the development and further deployment of the activities around information sharing and the alerting of citizens in the Member States, such as the European Information Sharing and Alert System (EISAS).

The ultimate goal of these activities is to help CERTs to improve the effectiveness and the efficiency of their response mechanisms, particularly where cross-border incidents are concerned.

A recent development here is the work that ENISA is doing to facilitate dialogue between CERTs and other communities (notably the Law Enforcement community) in cyber security.

The EU institutional CERT

The Digital Agenda for Europe is a flagship initiative under the EU 2020 Strategy. Key Action 6 of the Agenda is to: "Present in 2010 measures aimed at a reinforced and high level Network and Information Security Policy." One of the measures identified is the implementation of a CERT for the EU institutions.

[12] http://eur-lex.europa.eu/Notice.do?checktexts=checkbox&val=493232:cs&pos=1&page=1&lang=en&pgs=10&nbl=1&list=493232:cs,&hwords=&action=GO&visu=

[13] Task Force – Computer Security Incident Response Teams http://www.terena.org/activities/tf-csirt/

[14] Forum of Incident Response and Security Teams http://www.first.org/

In August 2010, European Commission Vice-Presidents Neelie Kroes and Maroš Šefčovič established a "Rat der IT Weisen". This small group of high-level experts was asked to provide the Commission and the EU institutions with advice regarding the establishment of a CERT for EU institutions. This CERT will deliver strong value as it would inter alia increase protection against attacks and facilitate swifter reaction to threats, ensure efficiency through shared resources, protect EU competitiveness and be consistent with EU policy.

ENISA, in its position as an independent, experienced and – above all other things – trusted body in Europe is uniquely positioned to play a key role in the coordination of the incident response capabilities of the EU institutions. Experts from ENISA are established members of FIRST and TF-CSIRT, and maintain vital relationships with all other CERT communities around the globe. Furthermore, ENISA's experts have extensive experience in assisting CERTs in the provision and coordination of NIS incident response.

The Rat der IT Weisen's final report resulted in an action to take the first steps towards a CERT for EU institutions, by setting up a pre-configuration team. This started operations on June 1st of this year. ENISA is actively supporting the pre-configuration team that is implementing the first phase of the EU institutional CERT.

Cyber EU-Exercise

In 2010, ENISA facilitated the first pan-European cyber security exercise. This took place on 4th November 2010 and involved the participation of all 27 Member States and 3 EFTA countries (Switzerland, Norway and Iceland). Of these participants, 22 acted as players and eight as observers. One of the most important conclusions of this exercise was that procedures to handle cyber incidents do not yet exist on a pan-European level and that there is a need to improve response collaboration across Europe[15]. Following on from this work, in addition to preparing the next pan-European exercise (which is planned for 2012), ENISA has recently been asked to facilitate the planning of the first EU-US cyber security exercise, Cyber Atlantic, which will happen before the end of the year. This exercise represents an important development in international cooperation and we are happy that the Agency's expertise is being called upon to support this effort. Despite the fact that such a project is a great challenge for the Agency, we are confident that we can work together with the Member States in order to meet the deadline.

[15] http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report/view?searchterm=cyber+europe+report

ENISA's work in 2012

In putting together the work programme for 2012, ENISA has continued its efforts to concentrate on issues that are both strongly aligned with the European policy agenda and also considered as core areas of competency for the Agency. In line with our role of facilitating cooperation between the public and private sectors, we have also involved representatives of the private sector community in this process. For this reason, the development of the 2012 work programme has been carried out in a different way to the process used in previous years. The procedure followed this year was designed to ensure that the input from the Permanent Stakeholder Group (PSG) and from the Management Board (MB) was taken into account from the beginning of the work programme development process.

This process has resulted in a 2012 work programme that is structured into four streams of work. These work streams are:

- Identifying and Responding to the Evolving Threat Environment
- Improving Pan-European CIIP & Resilience
- Supporting the CERT and other Operational communities
- Security Economics & Governance

They cover the evolution of the global threat environment, the need to continue to improve Critical Information Infrastructure Protection (CIIP) across the EU, supporting the CERT and other operational communities and economic and governance aspects of NIS respectively.

Identifying & Responding to the Evolving Threat Environment

Information Security is about managing risks and threats linked to the security of information and information systems. These can be considered as being the key drivers in any approach to improve information security.

ENISA's objective in this work stream is to provide stakeholders with information on how risks and threats are evolving. More specifically, the aim is to link particular trends to particular stakeholder communities, thereby helping such communities to recognise and respond to changes in the threat landscape that are particularly relevant to their activities. In addition, we will propose suitable mitigation strategies and identify recommendations and implementation options for dealing with the identified risks. The emphasis will be on the provision of information regarding all the components of risks. The principle output of this work stream is a periodic report summarising and prioritising risks by stakeholder community.

Improving Pan-European CIIP & Resilience

This work stream seeks to improve the level of resilience and level of protection of Critical Information Infrastructure throughout Europe. This is essentially improving the level of preparedness of Member States to cope with large scale incidents affecting their ICT infrastructure.

Supporting the CERT and other Operational Communities

The objective of this work stream is to continue to assist Member States in improving their operational response capabilities in the face of an incident. This objective also includes assisting Member States in developing key concepts, such as Early Warning Systems, and ensuring that such systems are capable of operating across national boundaries, thereby improving the pan-European response capability

Securing the Digital Economy

The fourth work stream provides a stronger focus on contributing to the development of NIS policy and strategy at the EU level in order to support the objectives of the Digital Agenda and to ensure that the Digital Economy of the future is correctly secured. ENISA will support the Commission and the Member States in this area by looking at three different aspects of the Digital Economy; Economic drivers and barriers for security, governance aspects and issues related to the development of secure, interoperable services.

In this context, socio-economic aspects of security, as well as privacy and trust related issues will be taken into account. Moreover, existing EU initiatives related to Future Internet (FI) technologies and systems will also be considered as an important input to the work.

In addition, supporting work will continue in the form of stakeholder engagement activities and project support activities. Press and Communications will also be planned as a separate activity within the Agency, as in previous years.

Cooperation

Our tasks are made all the more difficult if barriers are set up to which our adversaries are not subject. It is important that on a European level we have a holistic approach to NIS – and that we pursue opportunities for international collaboration and dialogue. One of the biggest obstacles we face here is the fact that communication between different communities within Europe is far from being optimal. As an example of this, it is important to note that the public and private sectors are working actively in the area of Critical Information Infrastructure

Protection (CIIP), but lessons learnt are not being shared. By ensuring that these efforts are aligned, we can greatly increase the effectiveness of the overall approach.

This brings me on to the Lisbon Treaty, which gives us the opportunity to adopt a cross-community approach to NIS. The treaty is a second opportunity for ENISA, which is ideally placed to support the Member States and the EU institutions in improving the level of dialogue between these communities in the area of NIS. The Agency could sensibly be considered as an interface between different operational communities in general. The objective would be to ensure that the overall approach to improving information security throughout Europe is both coherent and efficient, by identifying synergies and eliminating duplication of work.

EP3R

Addressing threats and strengthening security in the digital society is a shared responsibility – of individuals as much as of private and public bodies, both nationally and globally. A good example of an initiative to build bridges between the public and private sector is EP3R (the European Public-Private Partnership for Resilience).[16] Since 2009 ENISA has facilitated and supported the activities of the EP3R working groups on security and resilience objectives, baseline requirements, and good policy practices and measures.

Three working groups have been established to discuss key issues and propose recommendations on:

1. Key assets, resources and functions for the continuous and secure provisioning of electronic communications across countries
2. Baseline requirements for the security and resilience of electronic communications
3. Coordination and cooperation needs and mechanisms to prepare for and respond to large-scale disruptions affecting electronic communications

International cooperation

The cross-border nature of threats and the associated mitigation mechanisms make it essential to focus on strong international cooperation. This requires major efforts at national level, at pan-European level and globally. There should be close cooperation with international partners to prevent and to respond to cyber incidents.

[16] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm

At the EU-US summit[17] in November 2010, held in Lisbon, it was agreed to set up a working group on cyber security and cybercrime to evaluate and coordinate opportunities for enhanced collaboration. One of the areas which this working group should focus on is cyber incident management to enhance collaboration between national and governmental computer security incident response teams in Europe and the US. Another is EU-US exercise as mentioned previously.

ENISA's role

As the technology and threat landscape has evolved, we have fortunately also improved our network and information security capabilities. In some ways we can more easily define the issues and what is at stake. However, we do not know what tomorrow brings. It is a constant race to keep up with new technologies and business models and the opportunities they create.

ENISA's role is to support the Commission and the Member States in advancing network and information security. I see it as one of our main tasks to perceive and understand the needs of the Member States and the strategic interests of the EU. On this basis we will promote extensive cooperation and facilitate efficient and effective collaboration to advance cyber security in Europe.

ENISA is in a unique position to be a focal point for NIS in the EU.

The Agency can achieve this in a number of different ways. By acting as a neutral European platform for information sharing - and for establishing and maintaining networks and communities - we promote dialogue and help Member States to align their approaches to specific issues. This role is also important in a more general context, where ENISA facilitates dialogue between European actors and their international counterparts.

The Agency also provides expertise and advice to a variety of stakeholders, particularly in the area of development and implementation of standards and best practices. As such, the Agency plays an important role in bridging the gap between policy and operational requirements. Finally, we are active in the area of risk assessment and management, particularly where emerging threats are concerned.

[17] MEMO/10/597 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/597

The future of ENISA

It is increasingly clear that information security is a global issue, requiring a global solution. Not only are approaches to security that are confined within national boundaries liable to failure, any European approach that does not take account of the international dimension will also not work. By acting as a focal point for Network and Information Security within Europe, ENISA assists Member States in aligning their approaches and, in close collaboration with the European Commission, in ensuring consistency with international developments.

At present, ENISA is the only public institution with a pan-European focus that is mandated to work closely with operational communities in order to respond effectively to the threats I have outlined above. Past experience teaches us that working closely with operational communities is critical to introducing significant improvements in this area and we have an opportunity to take this model one step further with the new mandate.

This need for coordination and alignment of approaches and responses are highlighted in the draft report[18] from the Rapporteur of the ITRE Committee, which calls on the Agency to assist in developing coherent responses to NIS incidents. The report also mentions the importance of the Agency's work and contribution in strengthening the CERT community, and suggests that this role is highlighted and clarified in the future mandate of the Agency.

Commission's proposal and our comments

In ENISA was established in 2004 by Regulation (EC) No 460/2004 of the European Parliament and of the Council. ENISA's mandate was extended in 2008 by Regulation (EC) No 1007/2008. In September 2009 Vice-President Neelie Kroes announced the Commission's proposal for the extension of ENISA's mandate[19]. To give adequate time to the legislative procedure to reform the Agency, ENISA's mandate was extended until 13th of September 2013 by Regulation (EC) No 1007/2008 on the 8th of June 2011.[20]

We very much appreciate the additional tasks, especially the fact that the proposal already takes steps towards overcoming the pillar structure by including a reference

[18] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-470.059+01+DOC+PDF+V0//EN&language=SL

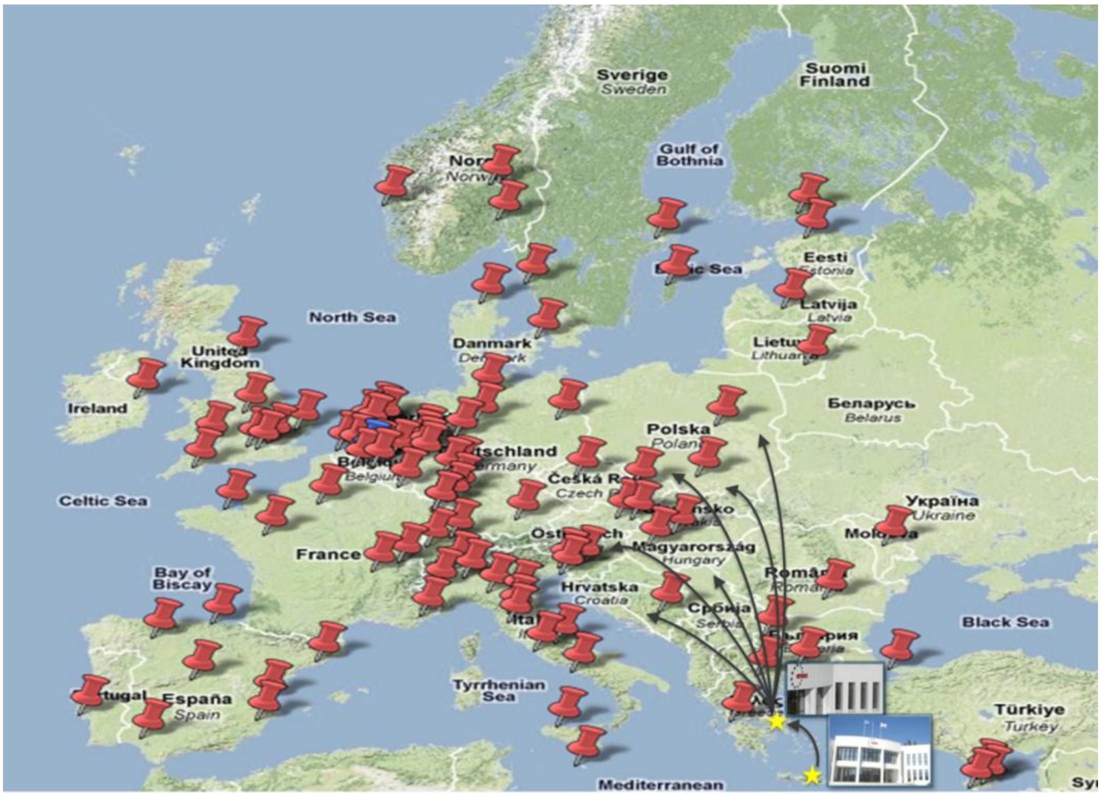
[19] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF

[20] http://www.enisa.europa.eu/about-enisa/regulatory-framework

to how ENISA can support other institutions in the fight against cybercrime by bringing forward the network and information security aspects thereof.

The Commission's proposal for the ENISA budget does not go beyond 2013. The budget will be presented by the Commission in the context of its proposal on the MAFF (Multiple Annual Financial Framework). As you have seen from the introduction on IT dependencies and threats, the budget of ENISA has to be aligned with the mandate's tasks lists. Therefore I am calling for your support in achieving this.

ENISA also needs more flexibility to face the current and future challenges in ICT. The modernised mandate of ENISA must have the necessary adaptability to respond to the challenges of the continuously evolving NIS environment.



Picture: The yellow stars show ENISA's seat in Heraklion on Crete and the Agency's branch office in Athens. The pins indicate ENISA's mission destinations across Europe.

The Agency must be enabled to fulfil the expectations and needs of our stakeholders, both today and in the future. It should be strengthened in its capacity and scope, as a centre for information sharing and exchange of best practices to achieve a pan-European approach to cross-border issues. In the Council meeting on the 27th of May, Vice-President Kroes expressed strong support for ENISA and has also since highlighted the need for the assistance which ENISA can offer to the Member States. Following this, ENISA sent out a letter offering expertise and support to Member States, which has resulted in the Agency receiving more than 10 requests in two months. These include seven requests from six different member states (Bulgaria, Denmark, Greece, Lithuania, Italy, Malta), one request from the European Parliament and two requests from the Commission, one request from the Council and an additional request from a European Agency. In order to respond to these requests effectively, whilst remaining within the scope of the existing mandate and respecting the agreed work-programme, a Mobile Assistance Team (MAT) has been established. The MAT operates on a mission basis from ENISA’s office in Athens.

Thus, we would like to see that the mandate of the Agency to respond to official requests is strengthened. In these ways, ENISA can assist in achieving a more coordinated and thereby more effective approach to cyber threats, as well as better cooperation on response to cyber-attacks in order to increase the overall level of cyber security to protect the European information society.

In a nutshell, ENISA is all about achieving stakeholder engagement. Our operating model is to maximise contact with stakeholders at all levels and to be present where the issues need to be resolved. Our previous work in this area has consistently shown that trust is built in small groups and that personal contact is a key factor in establishing groups that operate on the base of trust. We believe that this is particularly so where issues related to security are concerned. This is one of the few examples where the use of technology channels would not add a lot of value.

We know that this approach is supported by our stakeholder community, but we also recognise that being continually present throughout Europe is a significant operational challenge. In this respect, we would ask the Council to support the efforts of the Agency to improve the flexibility of its working environment and to create an operating model that allows the Agency to attract qualified staff as employees and to attract all relevant stakeholders.

Conclusion

ICT developments bring with them considerable benefits for modern society – they are a key economic driver and contribute to the competitiveness of the European economy. Such developments however are accompanied by associated risks, and controlling such risks is essential if we are to realise the true benefits.

ENISA already plays an important role in supporting the EU institutions and the Member States in securing the ICT infrastructure of the future. In particular, by acting as a neutral European platform for information sharing and for establishing and maintaining networks and communities, we promote dialogue and help Member States to align their approaches to specific issues. We also provide advice to stakeholders, bridging the gap between policy and operational requirements.

I have mentioned a number of areas where the tasks assigned to the Agency could sensibly be extended. Firstly, by asking the Agency to collect and analyse data relating to information security in a cross-border context, there is an opportunity to discover trends that are not visible at present. Secondly, I have noted that the coming into force of the Lisbon Treaty is a second opportunity for ENISA, which is ideally placed to support the Member States and the EU institutions in improving the level of dialogue between communities in the area of information security; and the Agency could sensibly be considered as an interface between different operational communities in general. I have also made extensive reference to the work that ENISA is doing in the area of resilience and CIIP, which is bringing valuable results to the community.

I have also mentioned the need to optimise the working environment of the Agency. Given that our operating model is to maximise contact with stakeholders at all levels and to be present where the issues need to be resolved, we would ask the Council to support the efforts of the Agency to improve full mobility and the flexibility of its working environment, and to ensure that we can place our resources where they are most efficiently mobilised throughout the EU – with the Member States.

Thank you.