European internet early warning system

Malte Hesse and Norbert Pohlmann

Institute for Internet Security – if (is),
University of Applied Sciences Gelsenkirchen,
Gelsenkirchen 45881, Germany
E-mail: Hesse@internet-sicherheit.de
E-mail: Pohlmann@internet-sicherheit.de

AU:
Please check the inserted Location and Zipcode in the Author affiliation.

Abstract: The internet is consisting of autonomous systems each managed by individual and mostly rival organisations. This situation makes it very difficult to capture the state of the internet as a whole. An individual internet situation awareness for various stakeholders can be accomplished by creating a common basis for private and public operators to monitor their networks, by offering them a common smart approach to monitor their network individually and the additional benefit of participating to establish a global view, which they can use as a reference for their local situation. This smart approach should utilise well-proven existing global statistics, best practices and existing technical sensors, which can be adapted to the overall common framework. From this, output for all relevant stakeholders can be generated to fulfil the individual needs. Once the internet situation awareness is accomplished, it can be used besides others for an European internet early warning system.

AU:
Please provide indication for corresponding author.

Keywords: critical infrastructure protection; global view; homeland security system; internet situation awareness.

Reference to this paper should be made as follows: Hesse, M. and Pohlmann, N. (xxxx) 'European internet early warning system', *Int. J. Electronic Security and Digital Forensics*, Vol. xx, No. xx, pp.xx–xx.

Biographical notes: Malte Hesse is a Research Associate at the Department of Computer Science of the University of Applied Sciences Gelsenkirchen. He is appointed to the Institute for Internet Security – if(is). His primary research in the area of security is focused on trusted computing, trusted network connect, mobile security, risk management and early warning systems.

Norbert Pohlmann is the Managing Director of the Institute for Internet Security – if (is) – of the University of Applied Sciences Gelsenkirchen and a Professor for Distributed Systems and Information Security at the Department of Computer Science. Furthermore, he is the Chairman of the board of the TeleTrusT association, Member of the Permanent Stakeholders' Group of ENISA and chairman of the ISSE program committee. He received his Doctoral degree in 2001 for his work on *Capabilities and Limitations of Firewall Systems*.

1 Introduction

The internet has become a large and complex system, which goes beyond all geographical, political, administrative and cultural borders, leaving a new and unusual

challenge to our society. Currently, society is undergoing fundamental changes cased by ever increasing connectivity and the penetration of the information society, in which the internet with its plethora of services plays an important role. Now, some parts of the internet have secretly emerged to be critical assets. Yet, the importance is growing, due to the convergence of fixed and mobile networks and evolving all-IP concepts. The internet is not regulated and consists of self-governed autonomous systems each managed by individual organisations mostly part of the private sector. Currently, there are more than 27,000 different autonomous systems advertised in the global routing table, information we have calculated with an if(is) tool called AiconViewer developed by Dierichs (2006) and available on our website. Private organisations are exposed to a high level of competition making an exchange of important management information between them impossible. The precise internal network structure, communication connections and topologies are often treated as being confidential by the network operators as Pohlmann and Proest (2006) experienced.

Besides the management of their own autonomous systems, the organisations also have to develop a strategy to exchange data with other autonomous systems. Based on statistics of the AiconViewer, there are about 60,000 logical connections between autonomous systems at the moment. Main factors for this routing of data are

1 the type of autonomous systems and the services it provides

2 (company) policies

3 more evident – financial aspects.

At the moment, no one can say how much inter-European traffic is routed unnecessarily through non-European networks like through Russia just for minor financial reasons, leaving security aspects out of perspective. Thus, economical necessities affect the organisation's proceedings, which yields to a reduction of redundancy and therefore to a destabilisation of the internet infrastructure.

Currently, there is a national discussion about the percentage of data traffic created by illegal downloads in comparison to the total traffic in Germany. Similar discussions are taking place in Europe and all around the world. This shows that the underlying structure of the internet is very complex and that nobody can offer a global view presenting adequate details. At the moment, every organisation operating as part of the internet simply has its own local view. Evaluation and analysis depends purely on the experience, resources and the used monitoring devices within each organisation. The internet exchange points for instance can only offer information on traffic that is exchanged between autonomous systems.

Internet service providers (ISP) earn money by transferring data, so they are not keen on providing evidence on how much money they make by routing illegal content. In addition, they can only offer their local view, which might differ from ISP to ISP, depending on their total number of end customers in relation to business customers.

To obtain a global perspective, there are a few challenges that have to be coped with:

1 communication data is relevant in principle to data protection (privacy)

2 the quantities of data are enormous

3 the data rates are sometimes so large, that they cannot always be analysed in real-time

4 while long-term storage of the communication data to observe long-term developments appears to be impossible.

Moreover, the question also arises of who feels responsible for creating a global perspective? This is easy to answer for a single corporate network, where due to corporate governance the responsibility for risk management is within the administration of a business. It is more difficult on an European level, where we can find an aggregation of different autonomous systems crossing various borders and administrative domains. A centralised operational body to monitor the European internet would have to be approved by most European member states, what is very unlikely, because the dealing with critical infrastructure is within the responsibility of each individual member state.

Nevertheless, the internet has developed into an omnipresent medium over the past few years, without which very large areas of the economy, research and private life would be unimaginable today. According to the European Network and Information Security Agency (ENISA) up to 30% of the global trade are 'digitally dependent' (LeClaire, 2008).

The constantly growing importance of the internet for our knowledge and information society makes it necessary to analyse and be acquainted with its status beyond the limits of the individual network operators. Only precise knowledge of the normal status makes it possible to detect anomalies, which influence the functionality of the internet.

2 Situation awareness

The term situation awareness comes from the area of air traffic control and military command and control. Generally, it is used when the understanding of an environment is critical for the process of decision making in a timely environment (Endsley, 1995b), which is a matter of life and death in the environment the term was explored for. Endsley (1995b) gives a generic definition for a wide variety of domains: situation awareness is "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future".

2.1 History and background of situation awareness

Coming from this critical background, a situation awareness is developed by a person (operator) using various sources, which can not only be sensors but also perceptions like the engine sound. The situation awareness is a representation of the state of an environment in the head of a person. It is used for the purpose of decision making and this decision finally leads to a certain action. Endsly emphasises that the different stages should be considered separately since it is up to the people to decide. So, incorrect decisions can still be made even with a perfect situation awareness and also perfect decisions can still be possible with an incomplete or wrong situation awareness. And furthermore, you might have perfect situation awareness, but due to personal abilities or a lack of experience, you might perform the actions in a lousy manner.

Endsly feels that "the problem with today's systems is not a lack of information, but finding what is needed when it is needed" (Endsley, 2000). This perception is based on the idea of an operator using a closed system, which is influenced by certain events like a pilot flying an airplane possibly in bad weather and not based on systems for the internet.

2.2 Situation awareness for the internet

The internet is a very complex system and there are lots of stakeholders involved each of which has the need for an individual situation awareness. So, it is not only the different stakeholders that require a different situation awareness, but also every individual member of each of these groups. One thing is almost certain, it will be impossible to capture the complete current state of the internet, like many mapping projects have already proven for a minor part of collecting information on the topology, but luckily this will not be necessary. We have to aim to provide the different stakeholders with individual information they need to fulfil their goals and decision tasks for their specific job or situation. For this, we have to work closely with the stakeholders in need of a situation awareness, since they need to phrase their demands.

Furthermore, we have to face the problem that we first have to retrieve the needed data of the internet, because so far this data is not gathered or at least it is not brought together to a global perspective. Then, we have to choose what is needed at what time for which stakeholder so that they can create a perfect situation awareness without being loaded with too much unneeded information. One should keep in mind, an important aspect stated by Endsly: "more data is not equal to more information". Therefore, it will be very important not to overstrain the stakeholders.

2.3 Process of situation assessment

In Endsly's model of situation awareness, he described in 1995 three sequent phases performed in the process of situation assessment by all people:

1 perception of elements in current situation

2 comprehension of current situation

3 projection of future status (Endsley, 1995b).

So, situation awareness is very commonly used in our everyday life, for example when driving a vehicle. The three sequent phases map to our efforts to generate a continuous internet situation awareness.

3 Input to gain situation awareness

To generate this situation awareness input from relevant and well selected, trustworthy sources; statistics, technical sensors and partners have to be used as part of the so called 'situation assessment' process. To make the idea manageable, the technical sensors must be able to comply with an overall framework, so that the data can be transformed to a common data format before it can be exchanged between various interested partners. It would also be an option, depending very much on the actual implementation and goals of such initiative, not to work with data but to exchange common incident reports.

These technical sensors can be divided into two main working zones:

1 network-based

2 host-based.

The sensors can either be active drones, initiating action by themselves or passive sensors, only analysing passing traffic or occurring incidents.

Besides input from technical sensors, there can also sources coming from an organisational background be used. This could range from portals, which can be used to report security incidents like social engineering attempts, to knowledge bases including information on zero day exploits, vulnerability, alerts, advisories, software updates, critical assets and technology trends.

For a complete situation awareness input, a number of sources can be used, such as from intrusion detection systems and netflow, also from sensor technology developed by scientists of the different member states. Examples for such sensor technology can be given by the means of two systems, which have been developed by our institute.

3.1 Internet analysis system

Our team has developed a passive sensor technology that can continuously collect statistical raw data with sensors, which are placed at selected spots of the internet communication infrastructure. At the moment, we have implemented sensors mainly in Germany to monitor the internal government network and the networks of universities and companies. In addition, we have found partners in Austria and Brazil, who also perform research with our technology. We are always interested in new cooperations and offer our technology to interested partners in economy and science.

The raw data is captured from header information of the passing network traffic by counting the occurrence of (currently) 870,000 different parameters. This processing is assuring that all sensitive header information, such as IP addresses and user data, are left out and therefore the data are not privacy-sensitive, avoiding ethical, privacy and legal challenges, that other data-collecting systems are plagued with.

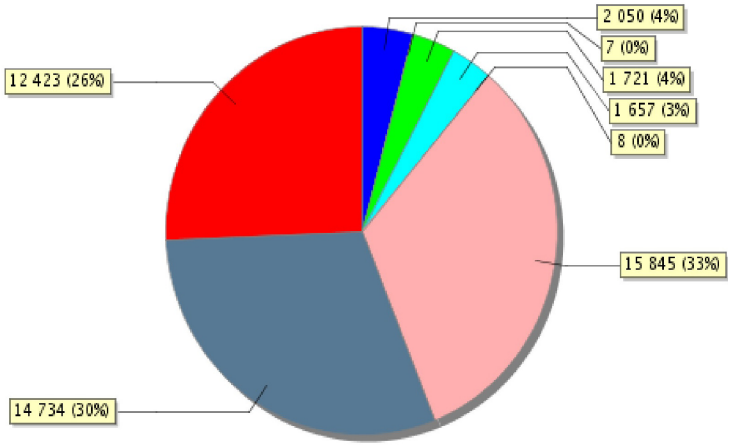
In addition, our processing is designed to have very high performance and it allows frequent transfers of the collected data to our centralised database using encryption. This enables us to collect and store data securely over a long period of time. The general approach is different form intrusion detection systems, which only collect information in case of a specific exception event and different from other monitoring systems, that store highly confidential content or IP addresses, which are privacy sensitive.

3.1.1 Some basic results of the internet analysis systems

Types of e-mail messages. Figure 1 shows the ability of the system to record the statistics of the headers of the e-mails sent via SMTP. The distribution can provide information on general communication behaviour as well as deviations from it. Figure 1 shows an example of normal behaviour in which the total number of messages without attachments represents 60% of all messages. These e-mails include messages with the text/plain (12,423), text/html (7) and multipart/alternative (14,734) content types. By rule, e-mails with attachments are provided with the multipart/mixed (15,845) content type. A mixed form is e-mails with the multipart/related (657) content type. Here, for example, images are integrated directly into the text. If these e-mails are included in the total count of e-mails, which are having an attachment, approximately 36% of all e-mails are sent with an attachment. The remaining 4% essentially consist of confirmations of reading with the multipart/report (2,050) content type. An abrupt change of these values in particular, may indicate a wave of spam affecting a company from the outside, or indicate that a computer is sending spam from within the company. It could also be an indication for an attack with malware attached to e-mails.

AU: Please provide the expansion for the acronyms ‘CERT, CERTS, DNS, DSL and SMTP’.

Figure 1 Distribution of e-mail content types (see online version for colours)



3.1.2 Transport layer security cipher suites really used for encryption

For the secure communication between clients and servers so called cipher suites have been pre-defined consisting of methods for the key exchange with authentication and algorithms for encryption as well as for data integrity. Which cipher suite is used for the communication is then negotiated between client and server depending on availability of algorithms and set preferences. If the browser is connecting the web server the browser offers the possible crypto suites to the server. Then, the web server decides which crypto suites should be used for the communication.

Since modern encryption is based on problems of the complexity and due to the fact that weaknesses in some methods have been identified, some cipher suites should no longer be used with growing performance of the available computer systems. But, sometimes the use of certain very insecure cipher suites is mandatory, due to questionable national laws, which are supposed to ensure legal interception especially in so called 'rogue regimes'.

The internet analysis system (IAS) can monitor from authentic network traffic, which cipher suites are really being used. This information is very interesting for all national representatives in charge for the monitoring of the infrastructure internet. So far, they have to base their decisions on very little available information. Most of the time, they are not aware of the actual situation.

In one of our monitored sub networks, we have recorded the following distribution (Figure 2): In 60% of all encrypted communication, the very common RSA_WITH_RC4_128_MD5 (5) cipher suite was used. In 33%, the improved and more secure DHE_RSA_AES_256_CBC_SHA (1) cipher suite and in about 6% the RSA_WITH_AES_128_CBC_SHA (3) cipher suite was used which is from the perspective of security. Also fine But, we have detected some profiles, that should not be used, like in 0.1% of all encrypted communication in form of the RSA_EXPORT_WITH_RC4_40_MD5 cipher suite, which only offers a 40 bit key length or in the case of 0.01% of the encrypted communication in form of the

RSA_WITH_NULL_SHA cipher suite, actually offering no encryption at all. From this information, national representative can disseminate guidelines for a secure use of the internet for agencies, companies and citizens.

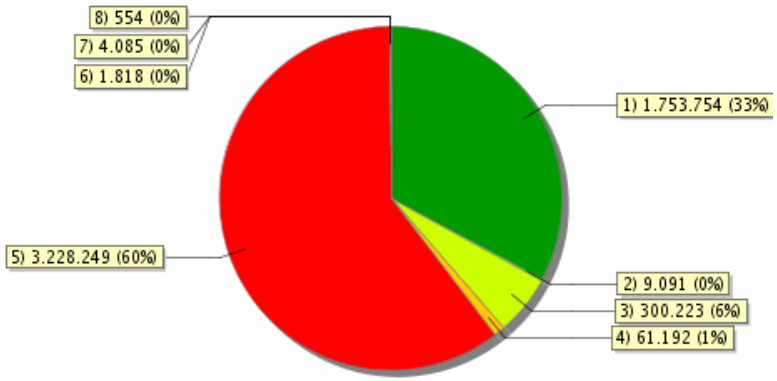
3.2 Internet availability system

The internet availability system (IVS) monitors the quality of the most important internet services and the infrastructure seen from a users view and visualises the results. Service specific evaluation methods are used to monitor the functionalities. Referring to the protocols in use, the system to be monitored is connected and the service is used. The response times are logged and later used as a basis for evaluation systems. Unlike other systems, we try to create various visualisations of the internet from different users' point of view. ISPs are able to monitor the functionality, but they are not able to see how accessible their systems are for users.

They need an internet connection, a DNS system and depend on the work of autonomous system routers. Due to these facts, the availability system is designed to collect data from different locations to recognise fluctuations within its own connection in comparison to other locations.

The IVS can be used to determine what should be considered as being the 'European internet'. Using the access connections of a representative number of users and enterprises to access those services, which are most important to the users, enterprises and governments, we can draw an undirected graph of active network components as nodes and their connections as edges by using the availability system. This would be a very applied and manageable approach to determine the scope of the European internet. Of course for the governments, the focus will be more on critical infrastructure protection. These important services would need to be determined by means of surveys or rankings based on hits.

Figure 2 Distribution of cipher suits used (see online version for colours)



3.3 Global view

As illustrated, the IAS can be used to generate a local view of IP-based networks. The IVS can be used in addition to generate additional data by actively probing certain systems and services from the perspective of different users. The monitored networks come along with very different characteristics, like obviously the total number of packets passing the sensor. The local view already helps the operator to monitor his own network, but a global view is even a lot more valuable (Tschöltsch, 2008). It can be used to compare the local situation with an authentic global view to detect abnormalities, which might help to confirm or dismiss the detection of local attacks or events. The global view is valuable to a number of other relevant stakeholders as well, like for national assessment centres.

To generate this global view, partners using the IAS and/or IVS are invited to join by frequently sending a summary of their local view to a centralised evaluation system (Figure 3). From this authentic data, the common global view is generated and transferred back to the participating partners. Due to the structure of the internet, this can only be accomplished with the support of the partners. So far, nobody can offer this kind of global view, so one cannot just buy it from someplace.

In Figure 4, an example of the possible confirmation of an attack with malware attached to e-mails is given by the use of the global view. The local view shows our partner, that the number of e-mails with a zip-attachment has abruptly increased, which is an indication for an abnormality and possibly for an attack. To verify whether this is a local phenomenon, which would be speaking for a directed attack towards the local partner, the event can be compared to the global view.

Doing this, we can find out that only a few partners have recorded this phenomenon at this specific time. Therefore, the event could be a directed attack against a selected group, for example banks or insurance companies. Other partners, who have no problem at this particular moment, can use this information to protect their organisations in advance. The centrally management evaluation system will also be able to detect cyber war activities.

Figure 3 Collaboration for a global view (see online version for colours)

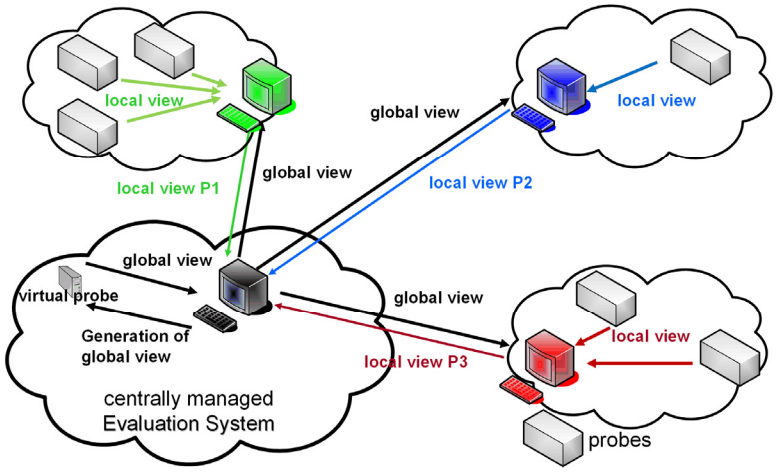
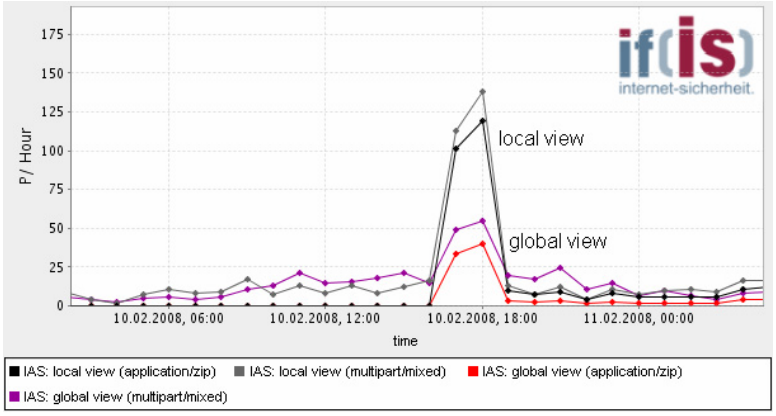


Figure 4 Example of malware detection (see online version for colours)



A further challenge will be to deal with the different natures of networks that can be monitored with the sensor technology. The traffic passing the sensor is characteristic for the types of services, which are provided by this different kind of network. Therefore, a content provider has a different profile of traffic as a university. To improve the outcome of the global view for these partners, they could be grouped in logical units. Each group can have their individual global view, which can be combined to the common global view of the internet. The challenge is that not all networks can be grouped that easily, due to their diversity and multiply business cases.

The selection of network operators as partners should of course be done due to scientific evaluations (rectangular distribution). For the future, once the technology has reached a wider level of acceptance, this will leave some unsolved complex statistical challenges for selecting the right amount and location of partners, which we have to face once this opportunity arises.

In addition, we have to deal with different time zones and inconsequent daylight saving time regulations all over the world. We cannot just agree on a global time for the distributed system of sensors, because the local time reflects in the usage of services and therefore in the collected raw data. The traffic passing the sensor consists roughly of human and machine initiated communication. The human part is highly affected by the different time zones, as people tend to sleep during night and work during day time. The human part is also affected by cultural issues (sociological aspects) like the long lunch break in Spain (Siesta), due to the hotter climate. We have to face the additional problem that no existing real-time sensor can decide for sure by analysing the passing communication data, if the connection was originally initiated by a human or a machine. It is not like we could build on the work of Turing, trying to test whether the communication partner is a machine or a human. The sensor is only monitoring passing traffic in real-time, which, in a lot of cases, are only fragments of packets of the different applications. At this point, further analysis is necessary.

We have a strong feeling based on the results of a diploma thesis conducted by Ricci (2008), that a limited but well chosen selection of parameters might already be sufficient to compare the local situation with the global overview to detect possible events. This is the great advantage of this system colleting statistical raw data, enabling the utilisation of findings of this mathematical discipline. In the long run, we can further extent the

selected parameters, if this should become necessary. At the moment, we are working on selecting and roughly splitting up the parameters. From there, we can build a global view, which considers the relevant time changes for each parameter of each sensor.

4 Idea for an European internet early warning system

Early warning systems (EWSs) have been installed in various working domains and they are a major part of an effective risk management in enterprises. In addition, they are part of the national homeland security systems, which protect a national territory from all sorts of natural and man-made hazards. The general idea is quite common in all working fields: monitor the environment, detect and forecast incidents and disseminate warnings.

The domain of hazards might vary from financial crises in enterprises environment to natural hazards like earthquakes. The existing EWSs save lives and reduce damage in various domains. Those at risk are humans at first and then of course the economy and welfare of the society. Usually, EWSs for natural hazards have four very important elements:

1 risk knowledge

2 monitoring and warning service

3 dissemination and communication

4 response capabilities.

4.1 Early warning process

The following section explains the early warning process containing of

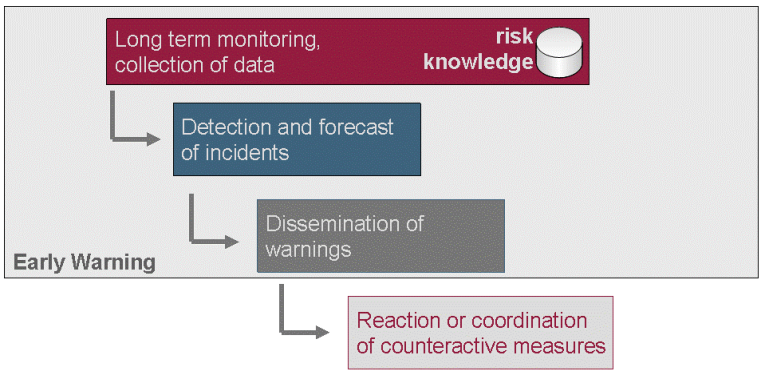
1 long-term monitoring, collection of data (measurement of precursors)

2 detection and forecast of incidents

3 dissemination of warnings. Some EWSs go beyond the warning aspects

4 support for reaction or coordination of counteractive measures as demonstrated in Figure 5.

Figure 5 Early warning process (see online version for colours)



4.1.1 Long-term monitoring, collection of data (measurement of precursors)

Scientists, working for EWSs for natural hazards use sensors and other sources as well to detect possible hazards and precursors occurring before the hazards strike, like minor earthquakes or shock waves. So, the main tasks of this phase are to develop sensors, setup a network of these sensors and operate this network.

An internet EWS will require a number of sensors (different sensor networks) and additional input data like from statistics or user feedback. In addition, the environment where the sensors are placed have to be well selected and have to be within the scope of the European internet. The information content presented should be the relevant aggregation of the actual information content so that the monitoring can please all stakeholders' needs.

4.1.2 Detection and forecast of incidents

In the area of natural hazards, the cruising radius is pretty much set and limited to a selection of mostly massive destructive forces. The scientists might not be able to forecast a seaquake, but they can detect the effects with their sensor networks. This is why the term 'measurement of the precursors' is used in the domain of early warning research for the monitoring. With this data and their knowledge base, they can forecast certain events with a certain probability, like the occurrence of a tsunami.

The internet EWS needs without question to be able to detect known attacks and threats, which can be identified by the means of the risk knowledge. On top of this, it is necessary that developing threats can be forecasted to a certain extend automatically or by the help of an operator. This can be done by thresholds, recognition of known situations, pattern matching and other methods, like from the area of data mining and artificial intelligence.

4.1.3 Dissemination of warnings

One of the most important aspects of an EWS is that the affected people, enterprises or governments are warned before the incident strikes and are provided with meaningful directives. Therefore, the group of affected and the response capabilities must be known and there must be a reliable way to notify them. All this is not trivial for instance if the incident takes place at night, or if the medium concerned – like the internet – was planed to be used to broadcast the warnings.

One example for

> "a web-based platform that combines existing web-based disaster information management systems with the aim to alert the international community in case of major sudden-onset disasters and to facilitate the coordination of international response during the relief phase of the disaster" is the global disaster alert and coordination system (GDACS) website (GDACS, 2008). This website can be used by everyone to register with their current location, preferred warnings and ways for communication (like SMS, e-mail or fax). The website also gives information on the current status of different hazards around the world. "GDACS will be activated in major natural, technological and environmental disasters, which overwhelm the affected country's response capacity and require international assistance".

So far, the focus is on natural hazards like earthquakes, tropical cyclones, floods and volcanoes.

EWS have to face multi-jurisdictional challenges. And since the project is funded by the United Nations and the European Commission, they cannot ignore the affected country's competence, which means that they have to be tolerated by the affected country's administration, especially if they go beyond the warning aspect by offering coordination and support services.

We feel that the GDACS portal must have a hard time to keep the contact data, including location and emergency phone number, up to date. Minor drawbacks of the GDACS website are for example problems with the transmission of SMS messages in certain mobile phone networks and of e-mail messages over the internet since "some email domains and some mobile phone companies do not allow GDACS messages for various reasons", as they are marked as spam. These problems are relevant to the objectives behind this document as well, since reaching the person at risk cannot entirely rely on the infrastructure at risk (the internet), which might be unavailable or unsafe to use when needed for a dissemination of warnings.

Incidents in the information technology sector do not cost many lives, an aspect which is very different from area of natural hazards. Of course, one could find examples in which lives are put at risk if computer networks and components break down, like in case of power plants, hospitals and maybe airplanes. But, most of the time backup solutions can cope without the support of computers for a certain time or the system is designed to shut down automatically if that situation occurs. Nevertheless, the damage caused by hazards to the information technology is enormous and can be reduced or avoided by the means of an EWS. Since most incidents in the world of information technology affect machines before humans, an approach that automatically initiates counteractive measures, would be interesting to have and could also be possible in a closed operational environment. First of all, this requires the knowledge of risks and response capabilities as well as the cooperation amongst various players. Therefore, Public–Private-Partnership (PPP) is an essential keyword.

The internet EWS would need to address the affected or other organisations that could further distribute the warnings correctly, that could be besides others the home user, an administrator in an enterprise, a service provider, the CERT community and government assessment centres. The GDACS website can address some of them. Other ways of dissemination would still have to be setup.

4.1.4 Reaction or coordination of counteractive measures

The reaction or coordination of counteractive measures does not have to be within the scope of an EWS. EWS for natural hazards for instance most of the time only warn and give advice. The response has to come from the community at risk.

4.2 Overview on the process of an European internet early warning system

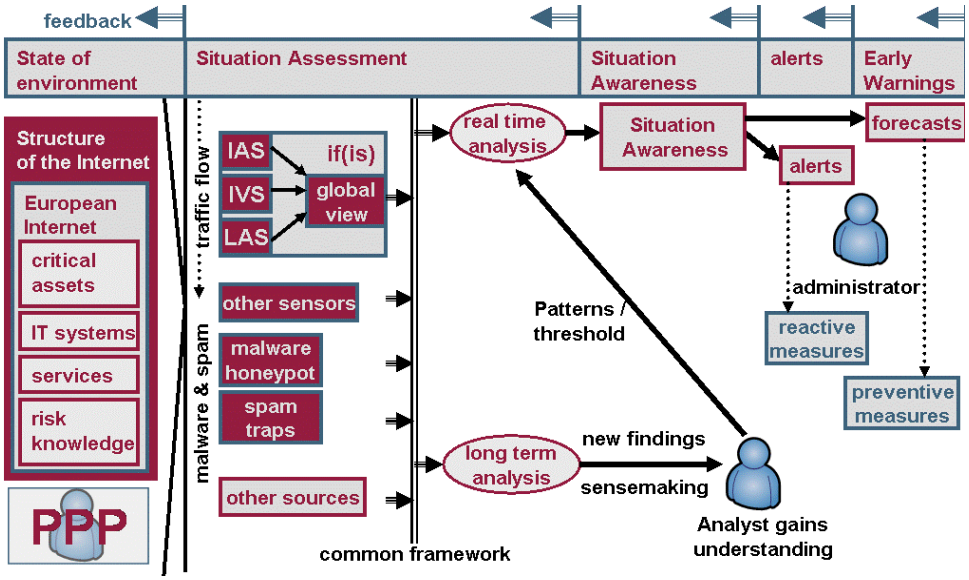
Figure 6 shows the project idea for a continuous internet situation awareness and EWS. First of all, the state of the environment needs to be addressed by analysing the structure of the European internet. Together with risk knowledge, we can identify critical assets, information technology systems and services. To be able to capture the state of the environment, a PPP needs to be setup and we need to find ways to comfort all partners by

offering them an added value for participation. The added value can range for instance from access to raw data up to individual reports on technology trends but is an essential requirement.

Once we have an understanding of the state of the environment, we can start the measurement of the precursors. Therefore, we need to take a look at available sensor systems to monitor IP networks. On top of this, additional information like statistics might be necessary in the situation assessment process of the operator of an assessment centre for instance to identify the total number of DSL connections in Europe. A common framework should be used by all developers to bring the data of various sources or the identified incidents in a common format. The common framework needs to be worked out in a PPP, acknowledging the fact, that a centralised operational united would lack acceptance by the European CERTS and national assessment centres. Ideas are presented in an ENISA feasibility study for an information sharing and alert system (2007).

The data can then be used for real-time analysis. The result of the real-time analysis is a situation awareness of the European internet of a person working for the assessment centre. The assessment centre knows the needs and available response capabilities of the different stakeholders. It will probably be required for the stakeholders to register information about their infrastructure and response capabilities. Once, attacks or other events are detected or reported by other EWSs. This could include notifications from EWSs warning about a storm or other natural disasters, which could create potential damage to the information technology infrastructure. Concerned stakeholders can be identified and then notified with alerts. Linked to a knowledge base, the alerts can be turned into multilingual advisories with concrete actions for the stakeholders addressing their response capabilities. Especially, the community at risk consisting of home users should be addressed in their native language. This was one very important demand of the referenced ENISA feasibility study (ENISA feasibility study, 2007).

Figure 6 Idea for a continuous internet situation awareness and early warning system (see online version for colours)



At this stage, a regular EWS is done with the scope of its work, because it is the stakeholders, who can then take reactive measures. But, it would also be possible in the long run that the internet EWS could go beyond the warning aspect by offering coordination and support services or by actively performing reactive measures, like the blocking of ports on all internet routers of the participating group of trusted partners.

An ENISA feasibility study (ENISA feasibility study, 2007) strongly encourages always to 'start small, but think big'. Therefore, the internet EWS should start with alerts first, extending those to multilingual advisories after a while and gaining trust and acceptance by the stakeholders before going towards automation. By the means of patterns, thresholds, experience of the operator and so on, the assessment centre can also forecast certain known events and those similar to the known events. Notifying the possibly concerned stakeholders before the event might strike, will allow taking preventive measures and therefore avoiding damage.

Besides the real-time analysis, the personnel of the assessment centre can also use the common data to do long-term analysis. This will allow making new findings and will support sense making, which helps the analyst to gain understanding of the situation, which he can use to adjust thresholds or define new patterns for the real-time analysis.

4.3 Organisational structure and possible funding

First of all, due to the structure of the internet all early warning activities will require a PPP. We can state that we also have to choose whether the system should be centralised or decentralised, which depends on how the two initial phases

1 monitoring

2 forecasting are provided.

At this point, we want to remind of one of the main demands of the ENSIA feasibility study for a different European system, which is meant to share information and alerts: "A newly built, centralized, co-coordinating body with operative tasks is less likely to be accepted by the relevant stakeholders from the area of CERTs and assessment centers." (ENISA feasibility study, 2007)

Therefore, the correct approach would be a decentralised one, building on existing structures of the domain of technological hazards for monitoring and forecast and in addition on an existing system for dissemination to share alerts in form of incidents reports and advisories like the GDACS for the community of the home users preferably in the user's native language. The GDACS can be used for the registration of potentially concerned and dissemination of warnings to emphasise the multi-hazard approach. In addition to the GDACS, we will need other systems for the dissemination of warnings and alerts to other communities and for the exchange of raw data and information.

Funding has to be provided mainly by public sources in combination with income which can be generated through added value for the private partners.

5 Conclusions

The existing EWSs save lives and reduce damage in various domains. The internet has become critical in some parts by now, but we are lacking the global monitoring and

controlling of this distributed infrastructure like it is common in other infrastructures. Stakeholders belonging to various communities need to be able to develop their individual situation awareness when using the internet, just like people are used to do it from driving a vehicle or performing other tasks. When using the internet, they have to trust that everything will be fine. Unfortunately, this trust has to be brought in this relationship by the user and has not been earned by the infrastructure. In addition, this trust has been known to be shattered by crimes arranged by individuals hiding in the anonymity of the internet and by malfunctions of the infrastructure.

The internet is more or less like a black box to the users and it does not offer any transparency, which hinders the user from developing an understanding of the state of the environment. Even the operators of the independent pieces of the internet only have an inside of differential quality to their own little piece. Situation awareness is essential not only for the home user to strengthen the trust in using the internet, but also for representatives of the government to make strategies for the further development or for enterprises planning to use the internet as a reliable platform for business.

With an availability system, in a first step, we can determine which parts of the internet are important in an European context by tracing the active network components along the routes from a number of important access providers to the most important service providers. With this information, we can identify and monitor critical elements. The gathered information can be published continuously on a website to help educate the users and published in a more detailed manner to offer an added value for supporters. The availability system will also deliver data about the status of various services to different interested assessment centres.

Besides the availability system, it is necessary to get the information what is being transferred at certain key points of the internet. The IAS will help to gather general statistics about the distribution of services, usage of technology and the overall development. This information could as well be published and offered to the supporters. The IAS will be able to detect known attacks and those showing similar behaviour to the known once. This can be used to generate warnings and alerts. It will also be possible to detect some unknown attacks that result in deflections from the previously as normal behaviour recorded representation of the network.

In addition, the raw data collected by the various sensors can be offered to other assessment centres, to emphasise the decentralised approach for an EWS.

This decentralised approach is necessary to gain the needed acceptance, but unfortunately it does not help to bundle the limited available resources. With an assessment centre in every member state involved in the EWS, we could at least face the challenge to address the users in their native language. For the long run, it would improve the entire process by far, if the different organisations would grow together to one operational body while working together closely in this constellation.

For the dissemination of the warnings, we could build on the GDACS system to inform the home users. For other communities, we will need additional methods for dissemination of alerts and advisories. In the long run, it would be a good aim to add some automation to the process within a closed environment of cooperating partners. Once an attack has been identified, routers could block ports and/or IP addresses to protect others from additional damage.

We face a challenging way to establish a working internet situation awareness, which can be used for national or international internet early warning activities. The internet situation awareness will help to:

1 improve the stability and trustworthiness of the internet

2 raise awareness for critical processes or components of the internet

3 find out more about the internet and its users in order to better cater to their needs and service demands.

We need to utilise new methods and techniques, algorithms and automated processing, before the open and self-governed structure of the internet degrades and possibly breaks down. The cooperation of companies, organisations and governments is important to create a global view of the internet. By that we will be able to detect attacks in time and answer interesting research questions on the 'living creature' internet.

We believe that we have to start to get experience, so that we will be able to have European internet EWS in the near future.

References

Dierichs, S. (2006) 'Eine strukturelle analyse des internets (a structural analysis of the internet)', *Diploma Thesis*, University of Applied Sciences Gelsenkirchen.

Dierichs, S. and Pohlmann, N. (2005) 'Netz-Deutschland (German internet infrastructure)', *iX – Magazin für professionelle Informationstechnik*. Hanover, Germany: Heise-Verlag.

Dong, G. and Li, J. (1997) *Interestingness of Discovered Association Rules in Terms of Neighborhood – Based Unexpectedness*, The University of Melbourne.

ENISA (2007) *EISAS – European Information Sharing and Alert System*, A Feasibility Study.

Endsley, M.R. (1995a) 'Measurement of situation awareness in dynamic systems', *Human Factors*, Vol. 37, pp.65–84.

Endsley, M.R. (1995b) 'Toward a theory of situation awareness in dynamic systems', *Human Factors*, Vol. 37, pp.32–64.

Endsley, M.R. (2000) 'Theoretical underpinnings of situation awareness: a critical review', in M.R. Edsley and D.J. Garland (Eds), *Situation Awareness Analysis and Measurement*. Mahwah, NJ: Lawrence Erlbaum Associates.

EWC III (2006) 'Developing early warning systems: a checklist', *Third International Conference on Early Warning*, March, Bonn, Germany, pp.27–29.

GDACS (2008) Available at: http://www.gdacs.org/.

de León, J.C.V., Bogardi, J., Dannemann, S. and Basher, R. (2006) 'Early warning systems in the context of disaster risk management', *Entwicklung and Ländlicher Raum*, pp.23–25.

LeClaire, J. (2008) 'Cyber terrorism threat growing, EU agency says', *CIO Today*, Available at: http://www.cio-today.com/story.xhtml?story_id=1230048OPVML&nl=5, 05/27/08.

Pastor-Satorras, R. and Vespignani, A. (2004) *Evolution and Structure of the Internet, A Statistical Physics Approach*. Cambridge, UK: Cambridge University Press.

Pohlmann, N. (2005) ''Internetstatistik' (statistics of the internet)', Paper presented in the Proceedings of the *CIP Europe*, B.M. Hämmerli.

Pohlmann, N. (2007) 'Probe-based internet early warning system', *ENISA Quarterly*, Vol. 3, January–March.

Pohlmann, N. and Proest, M. (2006) 'Internet early warning system: the global view', *Securing Electronic Business Processes – Highlights of the Information Security Solutions Europe 2006 Conference*, S. Paulus, N. Pohlmann, H. Reimer, Vieweg-Verlag, Wiesbaden.

AU: References 'Dong and Li (1997), Pastor-Satorras and Vespignani (2004), Dierichs and Pohlmann (2005), de León et al. (2006), EWC III (2006), Pohlmann (2007) United Nations, General Assembly (2007)' have been provided in the list, but not cited in the text. Please check.

Ricci, G. (2008) 'Betrachtung der vom IAS gesammelten kommunikationsparameter auf relevanz zur anomalie und angriffserkennung (evaluation of the relevance for the detection of abnormalities and attacks of the communication parameters collected by the internet analysis system)', *Diploma Thesis*, University of Applied Sciences Gelsenkirchen.

Tschöltsch, S. (2008) 'Konzeption und realisierung einer globalen sichtweise auf das internet zur bewertung der eigenen sicherheit (concept and realization of a global view of the internet for a better evaluation of the local security situation)', *Diploma Thesis*, University of Applied Sciences Gelsenkirchen.

United Nations, General Assembly (2007) 'Global survey of early warning systems', *Report of the Secretary-General*, 14 September.