National Cyber Crime and Online Threat Analyses Centres

A study into national and international cooperation

De Natris Consult

Leiderdorp, 17 september 2012

Index

1. Introduction

This report follows up on the results of a survey titled "National Cyber Crime and Online Threats Reporting Centres", we held in April of 2012. Recipients are different national entities responsible in their own way for establishing cyber security and/or fighting and preventing online threats. Having a law enforcement background myself, I have seen the difficulties these different entities have to find each other and exchange valuable, let alone actionable data at first hand. The discussion for the need to cooperate in a more structured way is not new. It does seem to have gathered up steam in the last months of 2011.

The idea for the survey specifically developed from two different occasions. Signal Spam expressed the need to expand its original function of a spam reporting centre towards a national botnet mitigation centre. It also expressed a distinct need to be able to share data at a larger scale than just France. It also became clear that several countries were discussing establishing a national centre for botnet mitigation or cyber crime reporting and analyses. Hence two questions arose: What is the actual present status quo in Europe and who is cooperating, sharing data with who?

This led to more questions. The result was a survey by De Natris Consult sponsored by Microsoft's Digital Crimes Unit. The main questions of this survey focussed on obtaining the following information:

- the present level of information sharing;
- the state of development of national centres in the selected countries;
- the (level of) participation of the respective participants;
- the level of cooperation between different partners involved in mitigating online threats;
- thoughts on international cooperation and coordination;
- suggestions for breakthrough topics towards (inter)national cooperation.

The answers lead to several insights and recommendations that need to be faced by those responsible for setting up and/or coordinating (inter)national cooperation concerning cyber crime and online threats. Some fundamental shortcomings will be presented on in this report. First though, we take a look at the background of this survey, with the premise up front that, as agreed, the individual answers of the participants remain anonymous[1]. We have the distinct impression that this led to more candid comments.

[1] Entities from the following countries we invited to participate: Austria, Belgium, Bulgaria, Denmark, Estonia, Finland, France, Germany, Greece, Italy, Luxemburg, Netherlands, Norway, Poland, Portugal, Romania, Spain, Switzerland, Sweden, UK and Turkey.

Of course this report does not pretend to be complete. For this the scope is too small. For a full overview more relevant entities in (more than the) 21 approached countries should have been approached and responded. However, because of the selection of countries and organisations, we do claim that the results of this survey point at fundamental issues and concerns the responding organisations (hence: the respondents) face in establishing cyber security and/or enforcing cyber crime (hence in the general sense: online threats). The candidness with which answers were given shows that most participants have very clear views of the situation they face. Although from different backgrounds, all have a specific task and responsibility in this field. In most countries we selected there is (a debate on) a national centre and/or strategy in some form. We thus selected enforcement agencies that have an established track record of enforcement actions and added other relevant organisations in those countries. In the survey we primarily try to establish how the entities receive and analyse data, secondarily we looked into how data is shared between entities. Thirdly we've tried to establish their involvement in national and international cooperation. With these questions we go beyond just the national centre (to be) in order to establish the present level of cooperation, coordination and efficiency in the fight against online threats. The results of this survey give cause for concern in all three fields of inquiry.

A draft of the report was sent to several entities with the request to deliver a statement on the report[2]. All those that responded, clearly gave off the signal that it is important to cooperate. That without the ability to share (actionable) data and information cooperation can not succeed. This report could be the beginning of new forms of cooperation between different actors who complement each other's competencies.

As the results to the survey are presented completely anonymous, I can not thank the respondents in person here. I extend my gratitude for your time in participating in the survey. For those who also accepted my invitation to do an interview[3], thank you kindly for the time allowed to me in your busy daily schedules and for the often invaluable information and frankness you provided. You all know, individually, who you are.

[2] You find the statements in full in annex 3.
[3] The results of the interviews are not shown in the graphics below, unless an answer was provided that was not in the survey response. The interviews are used as examples to underscore a point made and in the many examples for action and recommendations mentioned below.

2. Executive summary

Discussions on closer cooperation between public entities themselves and with industry on cyber crime and online threats are on agendas for several years. However, in the final months of 2011 several different initiatives in EU countries on botnet mitigation centres and/or ideas for a national cyber security centres seemed to intensify to another level of urgency. The more De Natris Consult delved into this topic, the more initiatives became apparent. At the same time several questions arose. Having discussed these initiatives with various experts from the European Commission, national authorities and industry, we developed the idea to hold a survey among very different entities, each responsible for the prevention and/or enforcement of, different forms of, online threats.

The questions that arose focus on cooperation, coordination and the sharing of data between these entities. So we decided to focus on a National Cyber Crime and Online Threats Reporting Centres that is to be read within the context of the survey, so for the gathering, analysing and sharing of data on "botnet related crimes and fraud, such as spam and/or, spam directing or causing people to load unsolicited malware, online account abuse and credential theft, and online advertisements distributing malware". Added to the definition was that several, different entities needed to cooperate within this centre.

After discussing my ideas with Microsoft's Digital Crimes Unit it accepted to sponsor a survey by De Natris Consult on National Cyber Crime and Online Threats Reporting Centres. The results of this survey are presented in this report.

2.1 The participants

This report is not exhaustive nor complete. For such the size and scope of the survey is too small and the set of questions too selective. However, it can claim to prove solid information that can help shape future national and European strategies on the prevention and enforcement of online threats. It also presents several recommendations that are based on comments, either in the survey or in the interviews held with participants, made by European entities which are closely involved in cyber security or enforce online threats. The participants to the survey are Law Enforcement Agencies, both police, government and regulatory bodies, telecommunication companies, CERTs, and NGOs, some of which are at the forefront in terms of expertise within Europe.[4]

The title of the survey suggests that it focusses on the relevance of national centres to understand and combat cyber threats. You will find it addresses more broadly the cyber security landscape and

[4] All invited universities did not respond.

its various threat vectors, from mass spam to targeted attacks. Most importantly, it focuses on what is most valuable to enforcers, the data and how they are collected, processed and whether this data is shared nationally and internationally.

2.2 Lessons and recommendations

The answers to the survey highlight the current challenges faced by European countries but also help shape possible next steps to improve building capacity against cybercrime.

Some of the most noteworthy conclusions from the survey are:

- Data collection is still done manually to a large extent (e-mail, fax, letter, phone);
- Both threat intelligence and complaint data is collected;
- Most entities do not think that they have an accurate real-time picture of the threat landscape;
- It is arguable that many incidents are not followed up on most likely due to the lack of automated means to do so in combination with a lack of resources;
- Information is not shared effectively between different stakeholders;
- International cases are exceptions;
- There is a great lack of coordination, hence great inefficiency in the way resources are put to use;
- There is no coordinative body where all can meet;
- There is no level playing field in the way national entities can operate inside and outside the respective countries. The following reasons were mentioned:
    - Different levels of technical development, skills, resources and focus;
    - Different implementation of EU Directives;
    - Other priorities;
    - International agreed upon standards are missing;
    - Reciprocal cooperation with police agencies is almost non-existent;
    - Beyond the EU it becomes even harder to cooperate.

These conclusions give rise to concern. Although the comment must be made first that we saw true commitment to the topic of fighting online threats. The people we spoke to, show the determination

to change the present course of online threats and clearly see where improvements are necessary. Most respondents know what should change to have more success. Some are very hesitant to go that way due to reasons that will be explained below.

It is clear that there are initiatives in place or under preparation for 9 national centres in 8 countries. However, this survey shows that these centres are specialised centres only, in which cooperation and the sharing of data with, let alone active participation by, other entities than the own (community)[5] is not standard procedure. If we go deeper, one finds that of the 16 entities which responded to the survey, only two take part in a truly national initiative as meant in the addition to the definition given above: "that several, different entities needed to cooperate within this centre". At present most other entities are not invited to participate in a national centre, sometimes share data with this centre, but usually do not receive data in return.

A culture of cross-disciplinary work is close to non-existent. Putting aside the two initiatives which can qualify as national, all other initiatives that the respondents participate in or allude to, are aimed at one specific topic, such as cyber crime, botnet mitigation, CERT function/cyber security. This strongly suggests that solutions are presently sought within the same discipline (e.g. criminal law, civil law) or area of expertise[6].

Most would expect that due to legal restrictions, respondents do not share privacy sensitive data with other types of entities. But legal restrictions are not the sole justification for the lack of sharing intelligence between them. Clearly the differences in culture and the traditional separation between these worlds play a notable role, and if a connection is established, it is more due to the personal commitment and initiative of individuals than to an established strategy by the agency or the authority, let alone the national government. Also the perceived lack of profit in sharing data with less equipped entities prevents cooperation.

What the survey responses clearly show, is that while the Internet is borderless as are the Internet crimes and online threats, responses to these crimes are not. Effective and impactful cooperation on international cases is hardly mentioned by the participants of this survey [7]. Most cases and efforts remain at national level, which leads to inefficiencies as intelligence is not shared. As a regulator annex botnet mitigation centre representative said: "There is nowhere we can all meet". Most who shared their ideas on international cooperation alluded to the Europol model as a starting point. Perhaps not so much in the form of seconded officers within a central organisation, but more as an

[5] More than one entity can participate in the "natural" community, as e.g. in a botnet mitigation centre.
[6] There are at least three initiatives known to us that did not respond to the survey of which two are aimed at botnet mitigation and one at cyber security.
[7] This does not mean they do not exist, but they are exceptional.

organisation that brings the different entities together and works on education, protocols and coordination so efficiency levels are raised and a level playing field created.

2.3 The way forward

Participating entities gave several clear recommendations on how to proceed, from centralised training sessions to coordination at case level. Despite the fact that some entities have very specific concerns, e.g. 44% of the respondents need to deal with each complaint individually, which stands in the way of wanting to receive complaints in a more efficient, automated way, in general it is possible to state that there is a clear need for:

- a higher quality of data which are gathered and analysed automatically;
- coordinated ways of gathering and sharing data and intelligence;
- international guidance to create a level playing field both at the national and international level.

This survey shows that cooperation between CERTs and/or botnet mitigation centres, including industry, on online threat incidents is established best. Cooperation among different sort of law enforcement agencies and in general with industry and academia is less well established. Looking at the survey results, we see a clear possibility for industry to play a more defining role through sharing high quality data with LEAs and academia in the same way as a few present, successful examples in the survey show for CERTs and botnet mitigation. We conclude that strengthened cooperation between all entities, which at present is underdeveloped, could lead to even higher standards of data and case solving. The results of which will lead to higher levels of protection for all. Further research into this topic is called for as standards and protocols need to be provided.

Another overall conclusion that shines through the results, is that the topic of fighting cyber crime, in its many different guises, let alone prevent it, at present is too large and overwhelming for most individual organisations. The CERT community, followed by botnet mitigation centres, copes best and at the same time shows the most ambition to better itself. The true reason for this does not show in this survey's results. Some differences in ambition clearly stem from national implementation of EU directives and the level of priority given to fighting online threats by entities themselves and/or national governments. For all goes that working cross border and this can be read as establishing cooperation between the different entities at national level as well, is hard to achieve in a structural way and too overwhelming for an individual entity to achieve. New approaches are recommended by most, which are presented at the end of this report. There is a distinct need for more efficiency, including a call for guidance at a central level. Both national and international.

3. The selected participants and the respondents

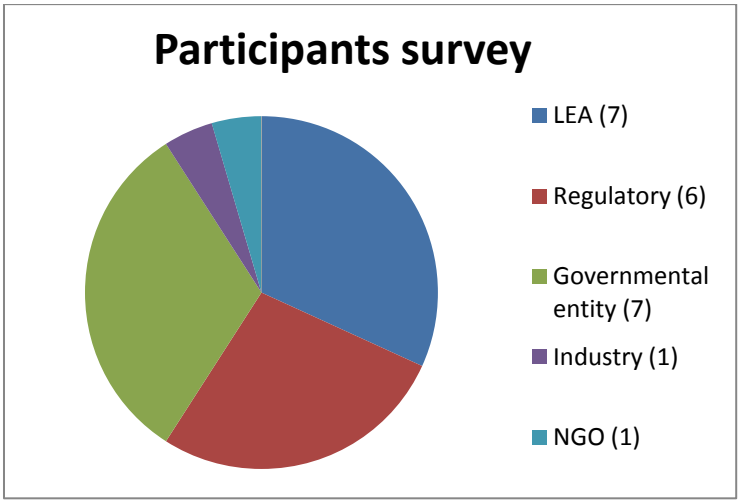
In the following we first look at the entities that were invited to participate in general. After that we take a look at who participated, but not without reporting on those who did not and their reasons, if given, for not participating, as these are also relevant to the result of this survey.

3.1 The invited participants

In total 41 parties were approached to participate in the survey. 33 originally elected by us, two later additions and 7 referrals (of which one was to an already selected participant). Two recipients opted for referral, but never followed up with who to refer to[8]. Two others referred, but decided to participate after receiving more information on why their contribution would be valuable. The selected participants come from 21 countries of which 3 are non-EU. The selected participants come from different backgrounds: police forces, governments, different administrative or civil regulatory bodies, CERTs, telecommunication companies, NGOs and universities.

3.2 The respondents

16 of the approached parties responded to the survey of which 5 were additionally interviewed. The respondents come from a total of 13 countries, two of which are non-EU. The background



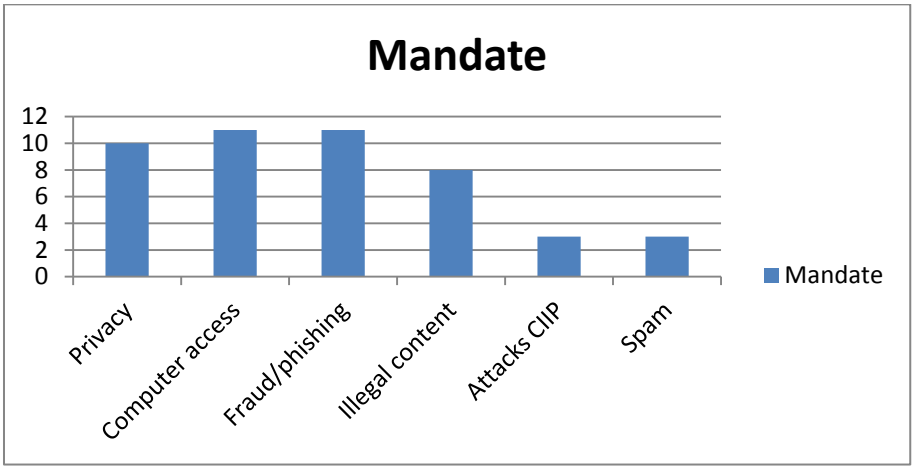
Graph 1, question 4 your organisation is a

of respondents show the diversity of the selected parties. From all backgrounds, with the exception of the universities, at least one organisation responded. Of course this total does not allow us to claim completeness. However, the opinions from very diverse entities as well as the reasons given for

[8] These two referrals are not included in the scores as there was never an introduction or name provided.

not participating, do point to fairly clear patterns as we will show. Graph 1 shows the score for participating entities.

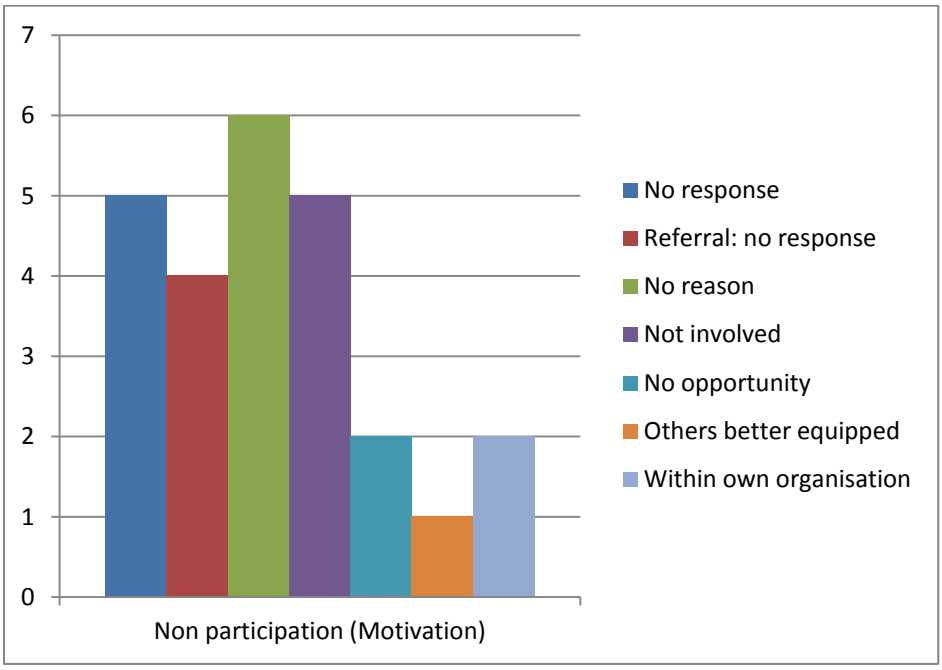
Between them the participants are mandated for the following online threats (graph 2).



Graph 2, question 5.3 online threats your organisation is mandated for

3.3 The non-participants

Not all organisations participated. Is there a lesson to be learned from the reasons for not participating? There is to some extent. As one consumer and anti-spam regulator voiced it: "We are not invited to participate (*in a national centre, dNC*) in any form, so I will not make time available to participate in this survey". With this answer the entity provided the main answer for this whole survey: 'Are you in any way involved in a national centre?' This answer is of great interest for this survey. A total of 5 entities motivate non-participation by stating that they are not involved in this topic, while 2 others state that others are better equipped to participate. Mind, all were eligible for both of the two main reasons for selection: involvement in one or more specific aspects of online threats and the news on plans of a national centre in their respective countries. Interesting to note here also, is that two entities participated anyway, after claiming non-involvement, when we explained the value of their participation to them. In as far as non-participation was motivated, it is shown in graph 3.



Graph 3 Motivation for non-participation (if given)

The motivated response for non-participation underscore some of the outcomes of this study and come back later in this report.

4. A short evaluation of the survey itself

There are three quick lessons. The first seems that the layered structured of question 6 was too complex as many respondents appear not to have filled it in correctly or did not fill it in at all, despite certain choices that could be made. The second lesson is that putting energy into follow up of referrals is hardly worth the effort if a good introduction is not provided for. Most simply did not respond unless the referral came with a recommendation. Even then it led to only two additional respondents. Both were very well introduced. These organisations approached me directly. The third is that personal relations worked best.

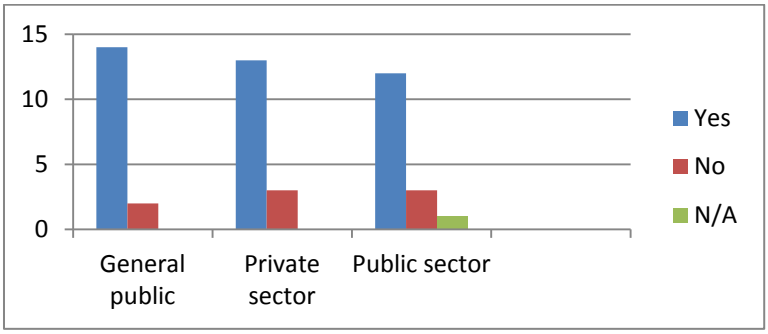
The interviews held with roughly 1/3 of the respondents led to very relevant insights and were an asset to the outcome of the survey. The reasons given behind certain answers or additions that did not show up at all in the answers were of great value as will be shown e.g. in the suggestions for change and the recommendations later in the survey.

5. The answers

In this chapter the results are shown in different sections, mostly following the order of the survey.

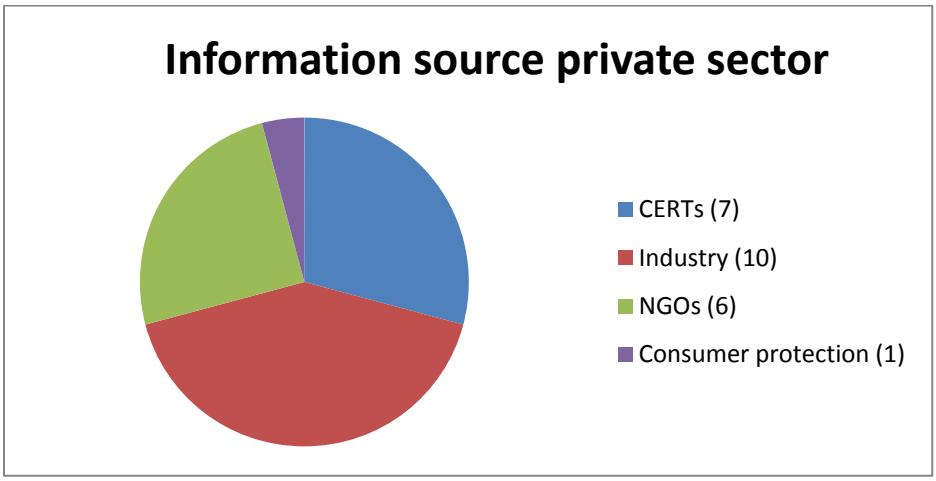
5.1 The receiving of data

The first cluster of questions focusses on the receiving of data. Graph 4 shows from which sectors the entities receive information on online threats.

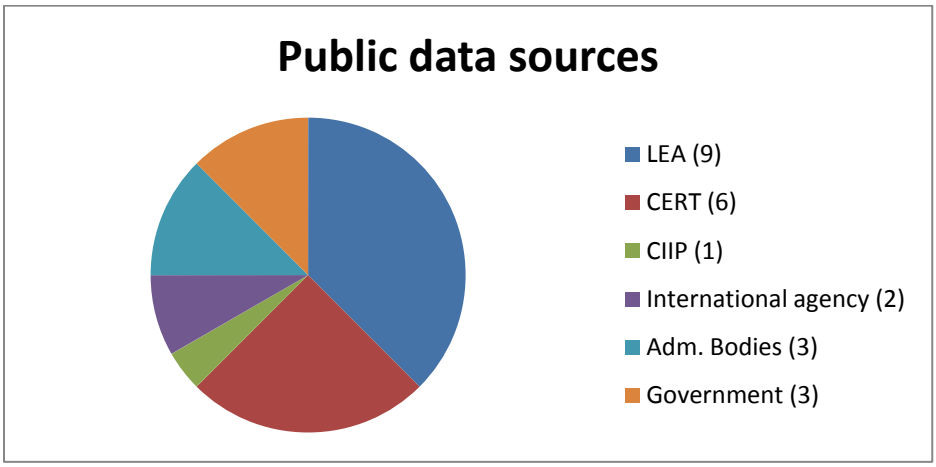


Graph 4, questions 5.1.1 to 5.1.3 does your organisation receive information on online threats from

If we specify this question to the private sector (graph 5) respectively public sector (graph 6) the results show the following.



Graph 5, question 5.1.2 selected contributors form private sector specified

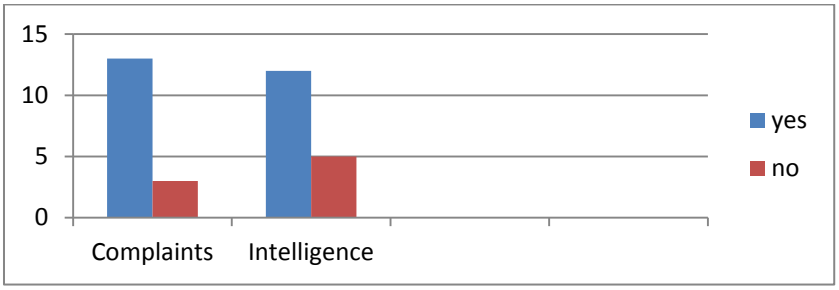


Graph 6, question 5.1.3 selected contributors form public sector specified

The overview presented in graphs 4, 5 and 6 seem a good result. Many sources lead to the overview the different entities get on threat levels. In how far these, public and private, sources are used on a regular basis, is not included in this survey. If we take into account the questions on quality of data and the wish to have (better) automated analyses systems below in section 5.2, into account, there is some reason for concern for several participating entities. Further research may be necessary to form a better opinion on this topic.

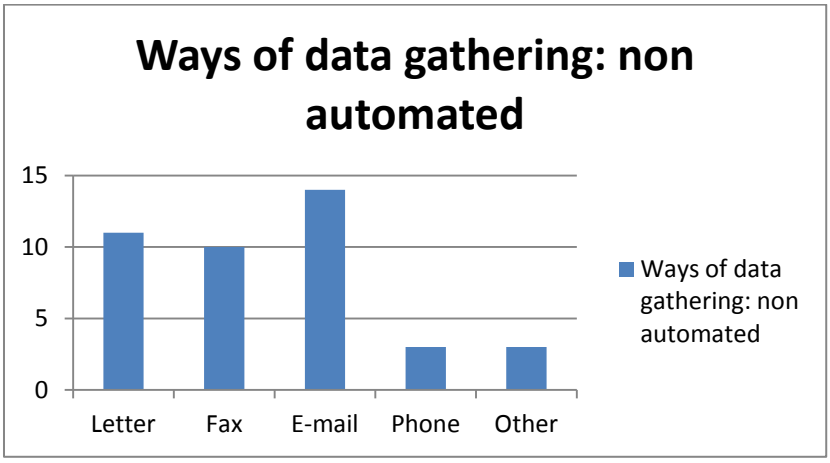
Remaining question: How often do entities receive data or intelligence from different sources and what is the spread in quality of received data?

When asked how the information received should be categorized, there is an almost as high answer for complaints as intelligence. This can lead to the conclusion that most organisations use multiple resources to gather data as is shown in graph 7.

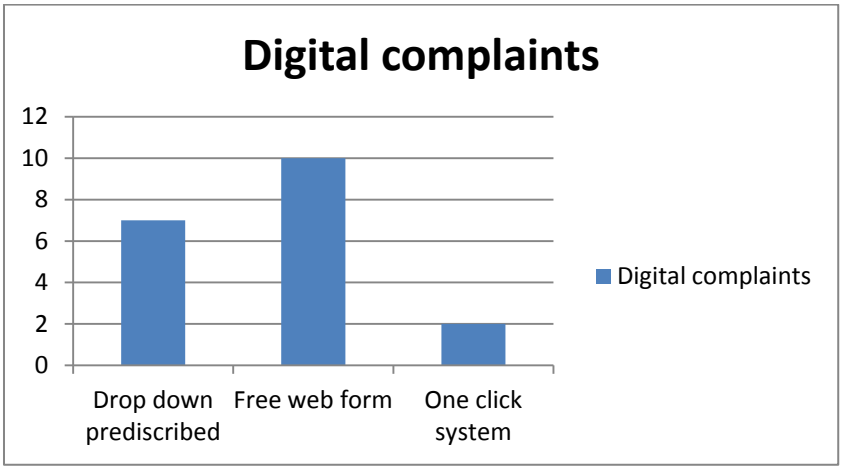


Graph 7. Questions 5.2.1 and 5.2.2 Legal status of information

The next graphs, 8 and 9, look into the way data is gathered. We asked about offline and online forms of data gathering.



Graph 8, question 5.4.1 Citizens or users can provide detailed reports by non-automated systems



Graph 9, question 5.4.2 Citizens or users can provide reports through automated systems

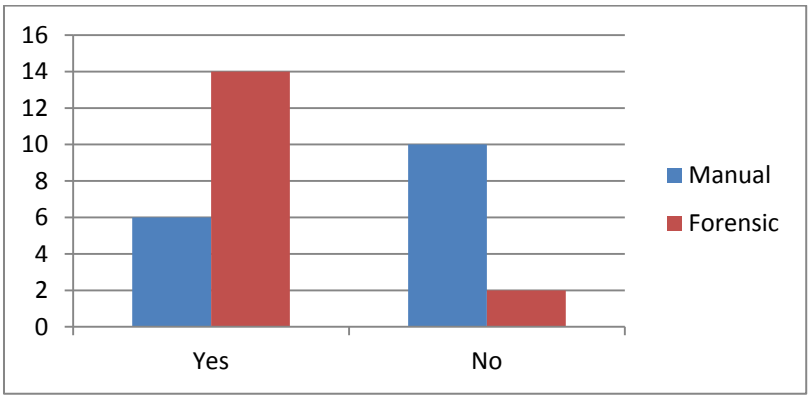
Graphs 8 and 9 show the answers given in a quite telling way. The conclusion we can draw from these graphs is that most organisation still rely on old-fashioned ways of data/complaint gathering. Highly automated forms of reporting, like the one click button, is used only in two instances. This result is reflected in the answers about the perceived quality of the data below.

13 out of 16 participants receive anonymous data. Almost all unconditionally. Two do not and one organisation does not work complaint based (question 5.4.3).

5.2 The (perceived) quality of data

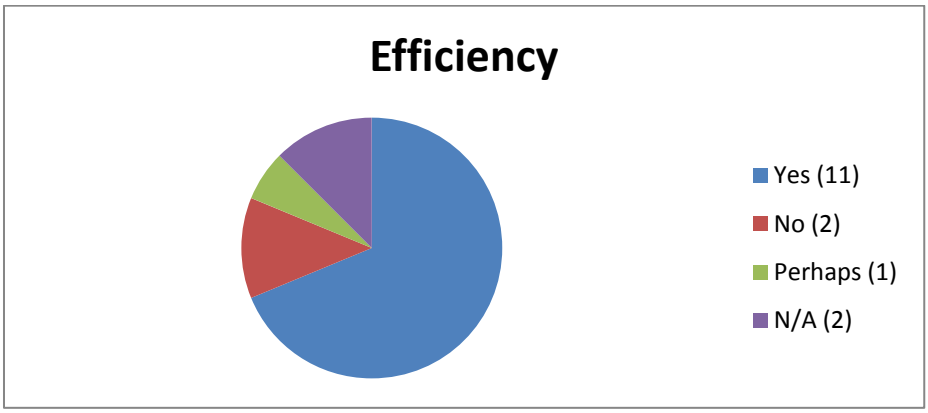
Questions 5.5.1 to 5.5.7 asked respondents about the quality of the data they received and the way they process the data. Here major differences between participants start to show, which do not directly show up in the previous graphs. It is also from these questions that the first comments were made in the interviews or given voluntarily in the survey. The reasons for these discrepancies are the first signs that organisations work from a different background. This however does not allow for all differences, nor for all the comments. Let us look at the graphs first.

Graph 10 shows the way data is handled by the respondents. There is cause to think that the first question was misread as an and/and option. The choice was "Through manual review **only** Y/N" and "through forensic tools or database management systems Y/N"? The score to both questions should have matched, but did not. Hence the two columns instead of one, which then are consistent.

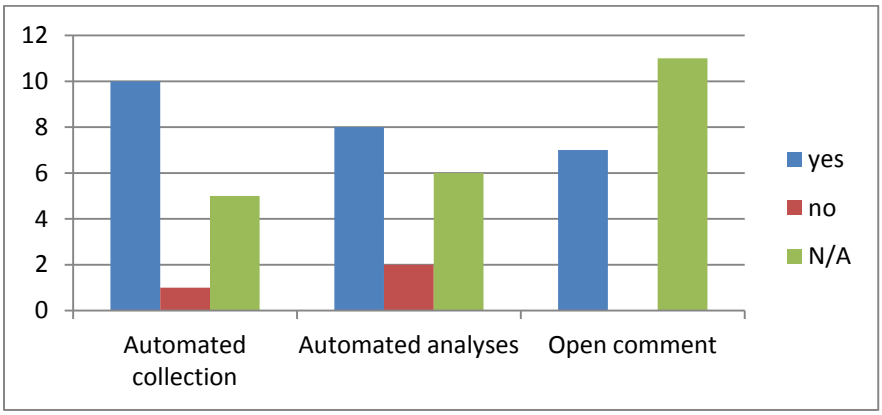


Graph 10, question 5.5.3 does your organisation analyse and evaluate the data you receive

My conclusion is that at least 4 (25%) out of 16 still handle analyses of data manually, as it seems next to forensic tools, while 2 (12,5%) exclusively handle complaints in a manual way. This conclusion is supported by graph 11 which shows that most participants have cause to declare that they can better the way they operate at present. Even the most advanced say so. Not surprisingly, they also seem the most ambitious to better themselves. (Graph 11)



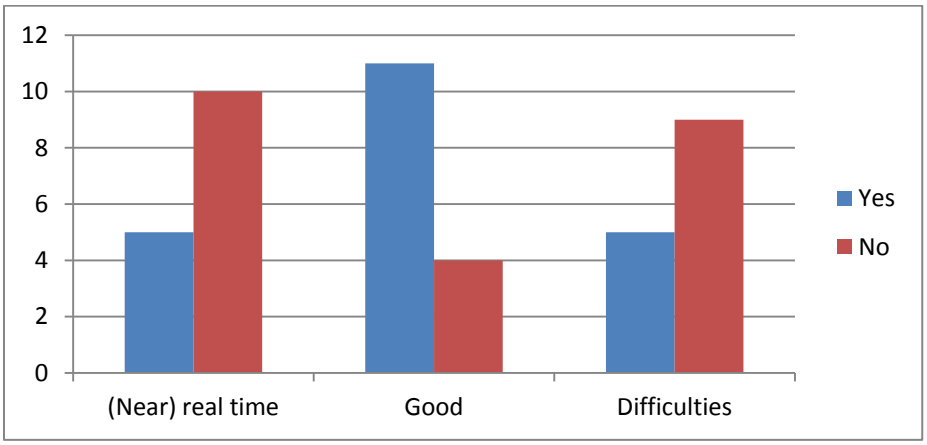
Graph 11, question 5.5.4 Do you think the process to collect and analyse complaints/information could be made more efficient



Graph 12, question 5.5.5 If yes, how (can data collection and analyses become more efficient?)

Graph 12 shows that ca. 60% of the respondents expect to better themselves through receiving complaints automatically and 50% through automated analyses. (One organisation does not operate on individual complaints.) The note must be made here that most entities as a standard allow non-automated complaints. Results show that where information was not gathered automatically, often the quality of data was very poor and led to inefficiency for the entity involved (often combined with the obligation to act upon this incomplete complaint).

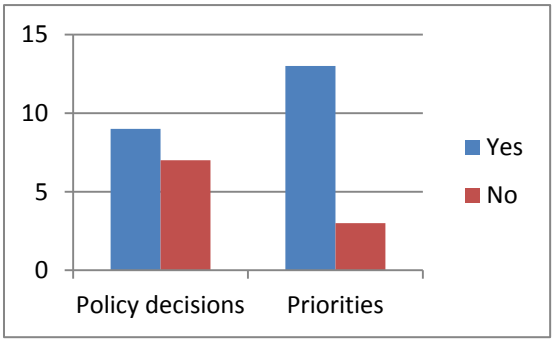
From the situation that most organisations see ways forward to improve their operation, it is not surprising that most do not think they have a (near) real time overview of the threat landscape as graph 13 shows.



Graph 13, question 5.5.6 does your organisation have a proper overview on the national online threat landscape?

Although graph 13 shows that it is hard to really score this particular question as some respondents gave more than one answer, it is clear that 11 entities declare that they do not have an accurate view on the threat landscape, while five are struggling with the ability to perform their task. It may however be a fair comment that not all organisations need a near real time insight to perform well. There is a distinct difference between (public and private) CERTs and enforcement agencies. The discussion about the (near) real time availability is a different one than the discussion about better quality data, from more diverse sources and the way it is analysed. Still, there could be reason for concern on the basis of these answers, especially those for that struggle. Further research is called for.

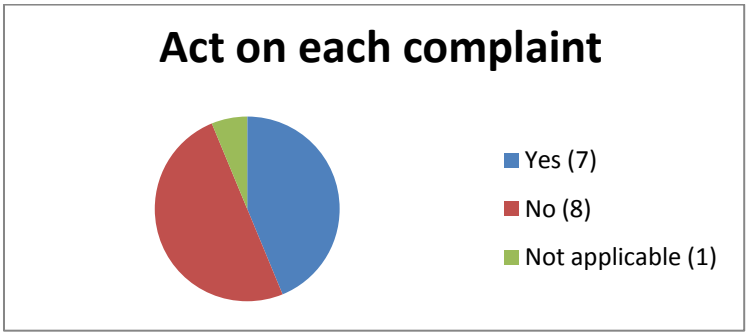
Remaining question: What organisations would perform better with near real time data and do those that need it actually have access to this data?



Graph 14, question 5.5.7 does the data you collect enable your organisation to make policy decisions and set priorities?

Graph 14 looks into whether the participants are able to make policy discussions and set priorities on the basis of the data they receive. Just over half of the respondents are able to make policy on the basis of the present level of received and processed data. Most are able to set priorities.

Graph 15 shows how some of the differences can be explained.



Graph 15, question 5.5.1 does your organisation act upon each complaint/information you receive?

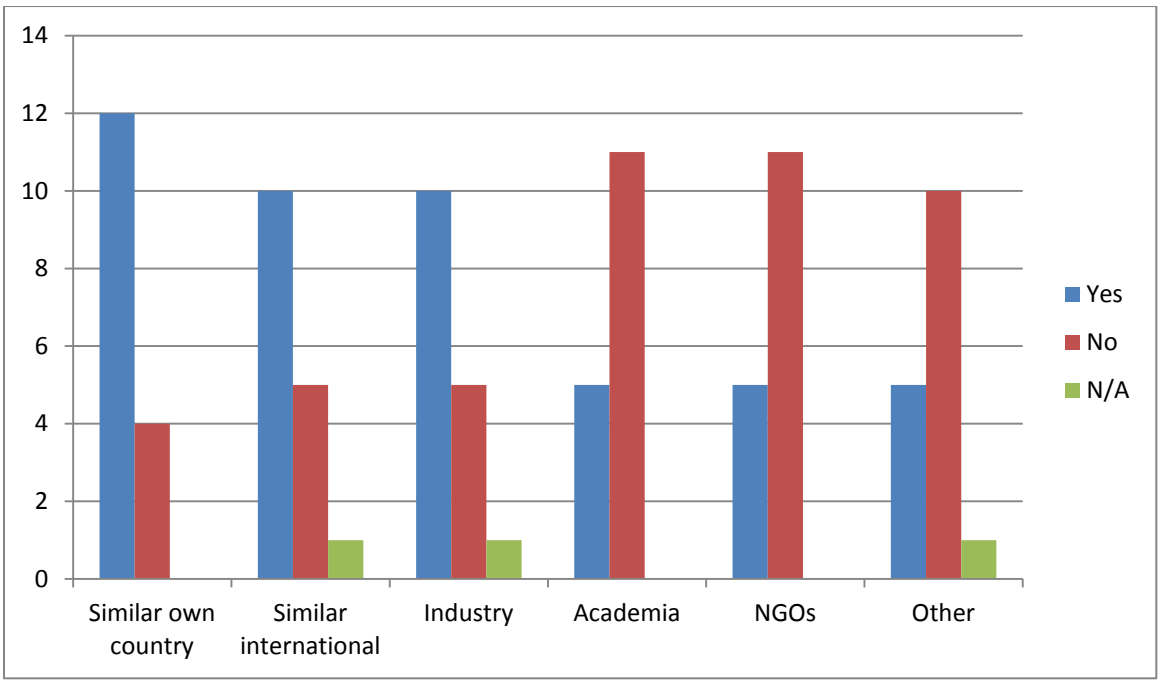
The obligation to act on each complaint means that the 7 entities shown in graph 15 cannot create a policy on complaint handling leading to prioritising and efficiency. In the case of law enforcement this lack of flexibility leads to sub-optimal results and a(n explicitly expressed) wish not to receive more complaints than are at present received. In other words the implementation of the local law seems to hinder a more efficient case handling and impede on true successes for the local enforcement agencies. It is necessary for governments to realise that e.g. spam and the crimes ensuing from spam is sent by the millions. If all would complain, the obligation to act on each complaint would swamp the enforcement agency. This explains, at least partially, the low level of presence of this entity and the wish to keep complaints low. Next to that, individual complaints run the greatest risk of not being correct complaints, false positives, with all the implications towards the efficiency of the authority and public money spent. Also the true extent of violations of the law may never become clear due to lack of numbers. This gives cause for concern and is advised on to discuss with national governments.

5.3 Data retention

Where the retention of data is concerned, question 5.5.2, most participants noted yes, we do and for the time the law allows. A minority stated that data was not stored before selecting the reports for relevance. Another, very small, minority answered never to have looked into the law on data storage and answered maybe we should be doing that.

5.4 The sharing of data and information

So far we have gathered a relatively good overview of data and intelligence received by the different entities. Now we can have a look at the way this data is shared. Do participants actually share data that could be of use to other entities in the online threats chain? We asked whether organisations cross-reference their data with other entities and if yes with whom. The results are shown in graph 16.



Graph 16, question 5.6.1 to 5.6.6 does your organisation at present cross-reference data with other organisations?

Graph 16 gives a very good impression. I am afraid we will take away from it below in the remaining part of the survey, but in general data is shared. Not taken into account in the survey is how often data is shared and with whom or which country specifically. Nor are differences clear whether certain entities in general are able to share data more easily than others, nor do (reasons for) differences between individual countries show through. It could be of interest to study this further. Following up on recommendations presented on below, however, may be more effective.

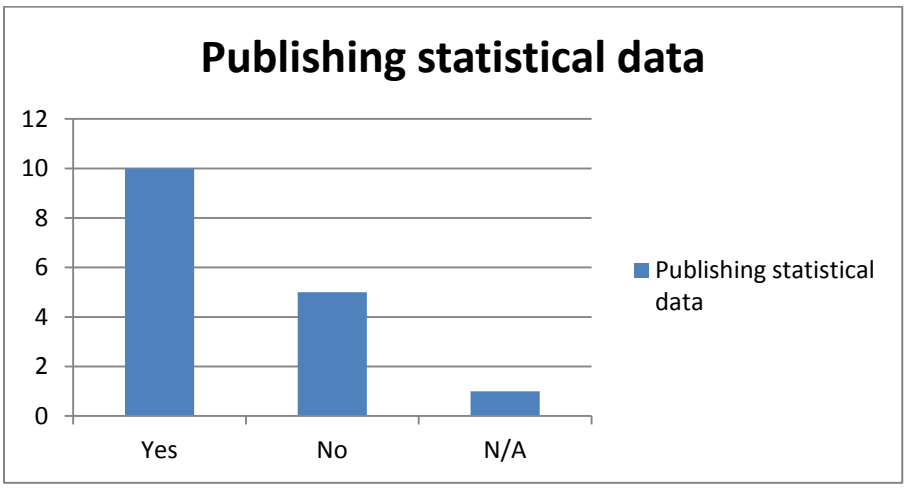
Remaining question: What are the true numbers on shared data, the quality, effectiveness and results of the data shared?

The next comment that needs to be made, is that "others" in the last column of graph 16 are all critical infrastructure partners that data is cross-referenced with, mainly by CERTs and botnet mitigation centres. This is telling as will be shown below.

Despite the figures in graph 16, it becomes clear that for over 67% of the respondents it is a-typical to work outside of the own category, with the exception of working with industry. 25% (see column one) and 37,5% (see column two) do not cooperate even within the own category nationally respective internationally. The fact that this potential of enhancing data and intelligence remains unused, is one of the main lessons of this survey. As one of the participants from a regulatory and botnet mitigation background formulated it: "there is nowhere where we can all meet". Of course the modest scope of this survey does not allow for more in-depth conclusions. It is definitely a cause for concern and calls for further study as some that commented are at the top of their field of fighting online threats.

Remaining question: How can data and intelligence sharing become more natural for entities to engage in?

Another comment that is important to notice, is that all that made a comment and those interviewed all confirm that cross-referencing data with police organisations is hard to come by. They also, without exception, state that this needs to start happening as they would (both!) be able to work more efficient and have better data. The police organisations in general do not seem used to work with other governmental agencies involved in fighting online threats , which is also confirmed by this survey. We observe that this leads to a division between cyber security and enforcement of other forms of online threats on the one hand and the enforcement of cyber crime on the other. This most likely leads to sub-optimal results in both sectors, for several reasons. E.g. sub-optimal use of potential, incomplete or a lack of data, sub-optimal use of different enforcement tools and powers, etc..



Graph 17, question 5.5.2 do you keep each complaint/information you receive in your records?

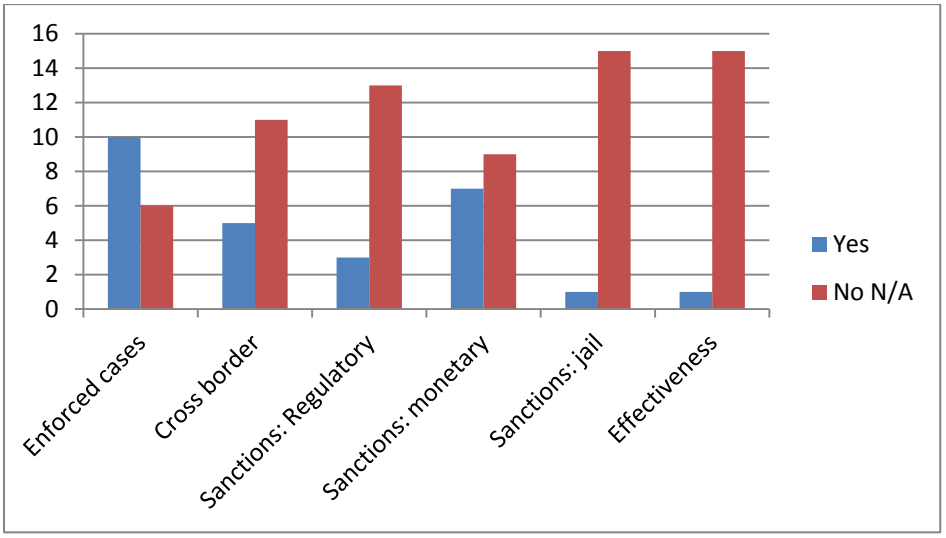
5.5 The publishing of statistical data

More than half of the participants publish (some) statistics, graph 17. The websites referred to are not mentioned here as they give away the identity of responding entities.

5.6 Statistics on enforcement

The response to question 5.8 on statistics on enforcement led to very diverse answers. The reason is that not all respondents enforce, e.g. telecommunication company and two law enforcement organisations that hardly do cases themselves, but assist at the national level and hand over intelligence to local LEAs. Monetary sanctions are exceptions in numbers, the notable exception being 171 monetary sanctions given by one entity in 2011 alone (and paid!). Regulatory sanctions are more numerous. E.g. botnet mitigation centres give warnings on infections of computers to ISPs. They run into the thousands per annum. CERTs take action against breaches of security. Graph 18 shows the scored results in a yes/no fashion.

A note to make at graph 18, is that in an environment -and this is a fact everybody agrees on- which is without borders, only 30% of the participants have actually dealt with a cross border case in the



Graph 18, questions 5.8.1 to 5.8.4 statistics on enforcement

past two years. The survey does not explain this fully. Neither does it show the impact of these cases. Below some reasons will be shown, either from comments in the responses or through the

conducted interviews. We state here that this answer clearly takes away from the quality of the responses above under graph 16, that participants cross reference data internationally. The small number of cases, 1 or 2, show the exceptionality of international cooperation at case level for the participants. We observe that this also takes away some value from the perceived positive value of cooperation in the respective international cooperation bodies towards international cases, see graph 27 below. Perhaps this is the case for national cases that the network provides additional value in several ways, but this is not specified in this survey.

Remaining question: What are true figures of international cases on online threats, who participate and can results of international cooperation be measured?

Remaining question: In how far do entities actually cooperate on a cross border cases or is information or a case referred to a colleague entity without further involvement?

Another note is, that only one organisation claimed that 100% of the monetary sanctions were actually paid. One claimed confidentiality. The rest could not or would not answer. The true effectiveness of sanctions is not clear.

Remaining question: What is the level of effectiveness reached by law enforcement and regulatory agencies in cases and how does this compare with (the quality of) data received by them?

5.7 The present state of national centres

In general you will see several categories of answers:

a. There is no centre as described at the beginning of this report;
b. Yes, there is a national centre (and my organisation is it);
c. There is a form of national centre and I participate, am the centre;
d. There is a form of national centre, but we do not participate.

a. There is no centre as described at the beginning of this report

14 of 16 respondents noted that there is no national centre as such meant in the survey[9], but that there are initiatives that come close to a national reporting or analyses function, but usually isolated within one organisation.

[9] The definition is given in the first and second section of this report.

b. Yes, there is a national centre (and my organisation is it)

There were two organisations answering "yes, I am the centre" of which one was part of a national strategy. In case of the other centre an entity that responded from the same country, did not name the centre as such in his response and mentioned another initiative. This gave rise to us to (also) mention this entity in sub c below.

c. There is a form of national centre and I participate, am the centre

Five of the respondents are (part of or participate in) a national centre of which four are a government agency that have a predesigned task given by the national government. One of the centres is part of a national strategy. Two of these centres come from one country. The fifth is an NGO.

d. There is a form of national centre, but we do not participate

In the other countries where a centre with a national function was mentioned, the respective organisations did not participate in this centre nor receive data from it, with one exception, a telecommunication company, who cooperates fully to its satisfaction.

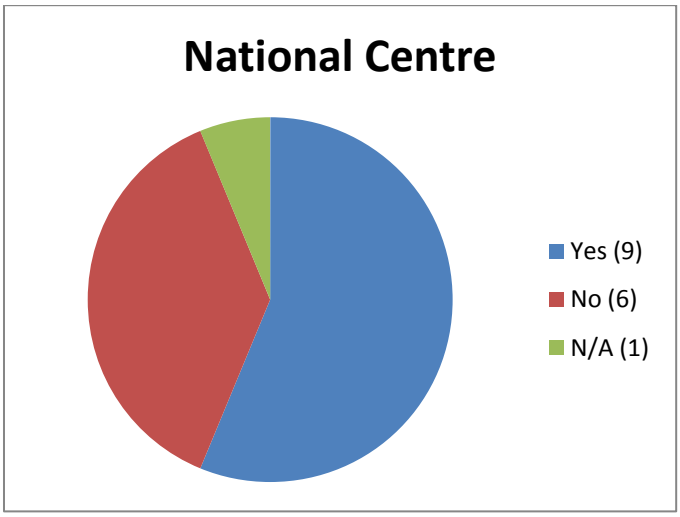
In general the picture is very diffuse. Eight organisations pointed to another organisation in their respective countries, among who two organisation coming from the same country. One entity answered it would be part of and be leading this centre, should it come. Only two agencies that were referred to participated in the survey. It happens both come from the same country.

All respondents who referred in this way, state that it is a centre coming close to a national centre. They stated without exception that they did not participate in the centre, while most do not cooperated with it. For most, to share data with this centre is hard. Receiving data was a clear exception. There are a few initiatives mentioned that made it clear that at least two countries have a botnet mitigation centre in place[10].

These are the national centres mentioned by respondents (question 6.1): CERT-FI; Action Fraud (UK); Signal Spam and Internet-signalement (Fr); CIRCL & GovCert (Lux); Nitec (Dn); Cybercrime and Competence Centre (A); CNAIPIC (It); Computer Crime Analyses Unit (It); Melani (Sw); CYCO (Sw).

[10] There are two other national initiatives known to us that have not responded to the survey

The following information is available around national centres. Graph 19 shows the responses towards the presence of a national centre. Again we point that these centres do not qualify as to the definition we gave for a national centre (with one already mentioned exception). Most mentioned centres appear to have a national function embedded within one organisation and the resulting data is meant for this organisation or at most shared with similar organisations or natural partners[11].



Graph 19, question 6 does your country have a national centre …?

Comments made show this. " I am the national centre but only for security breached/only for cyber crime". Another comment says: "There is a national centre for cyber crime, but we do not participate, nor were we asked. We should participate on spam, phishing and data breaches'. Someone else commented that they could not participate in the centre for cyber crime because there "is no direct connection between spam fighting … and "real" cyber crime activities".

A final comment is that a small minority of respondents do not want or are hesitant to participate in a national centre for fear of losing its independence. Still, they both claimed participation in sharing data with the centre would be an improvement towards their work.

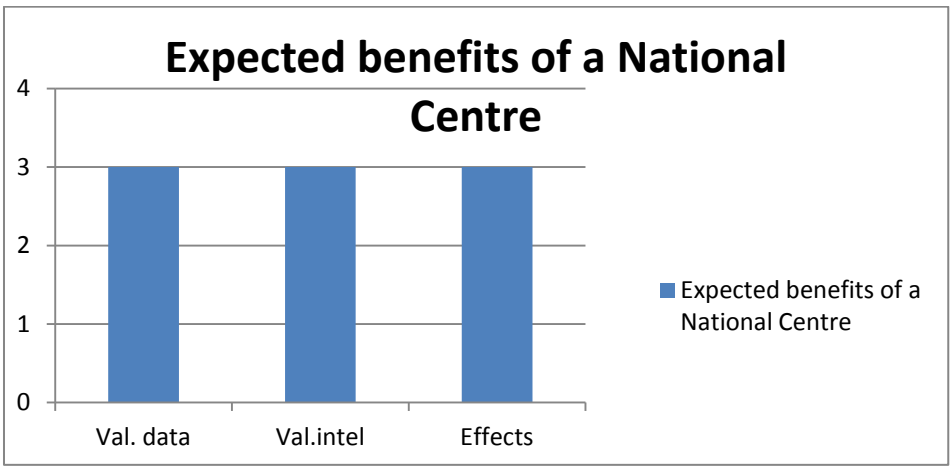
There were two national centres mentioned, but not participated in by the respective respondents, that are part of a national strategy, question 6.1.3. Here are the links:

http://www.cabinetoffice.gov.uk/news/protecting-and-promoting-uk-digital-wolrd

http://www/mediacom.public.lu/cybersecurity/CSB_Strat_Gie_final_20111122_.pdf

[11] There are notable exceptions. E.g. when the respondent is protecting national infrastructure, involved in botnet mitigation or cooperation on spam fighting. Still all state that that the sharing of data and cooperation needs to be bettered.

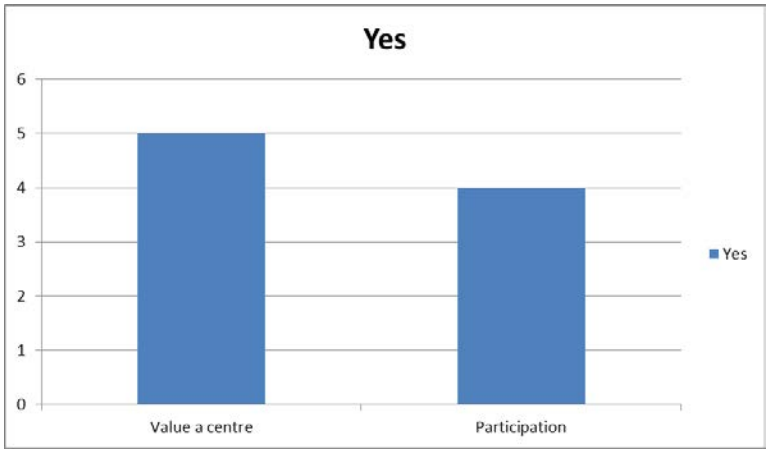
6 participants responded to the question whether they participate in discussions around a future national centre in their country. 4 Answered yes, 2 answered no. 3 of the 4 answered the follow up question what they expect the benefits of a national centre to be for their organisation.



Graph 20, questions 6.1.2 Are you a member of this centre (answer no)

There were only two respondents to the question 'yes, there is a discussion on a national centre, but we do not participate'. We asked whether they wanted to participate if possible. One answered: We would be an integral part of such a centre. Another pointed towards an on-going reorganisation at national level, but it was not clear to us whether a centre would rise from these reorganisations. The answers show in graph 21.

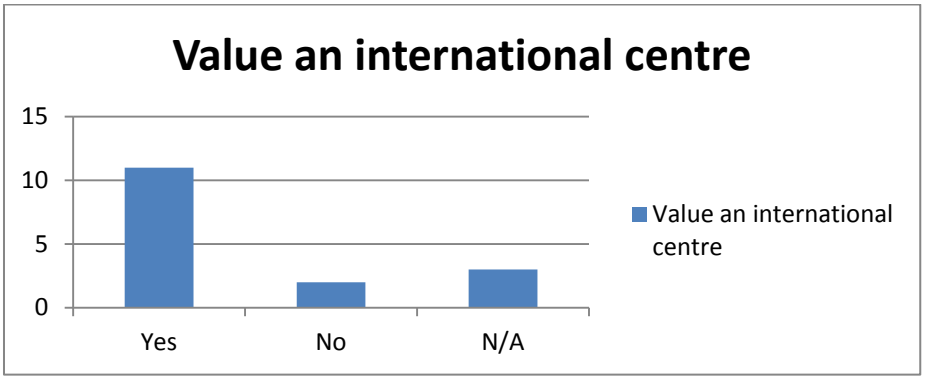
In the remaining option on this topic, we asked those in whose country there is no centre nor preliminary discussions, whether they would value a centre in general and if so whether they would participate in such a centre. Graph 21 shows how those remaining answered. One regulator did not want to participate in fear of losing its independence.



Graph 21, question 6.3 and 6.2.2.(1) Would your organisation value a centre in general and would you like to participate in a national centre once it is instated?

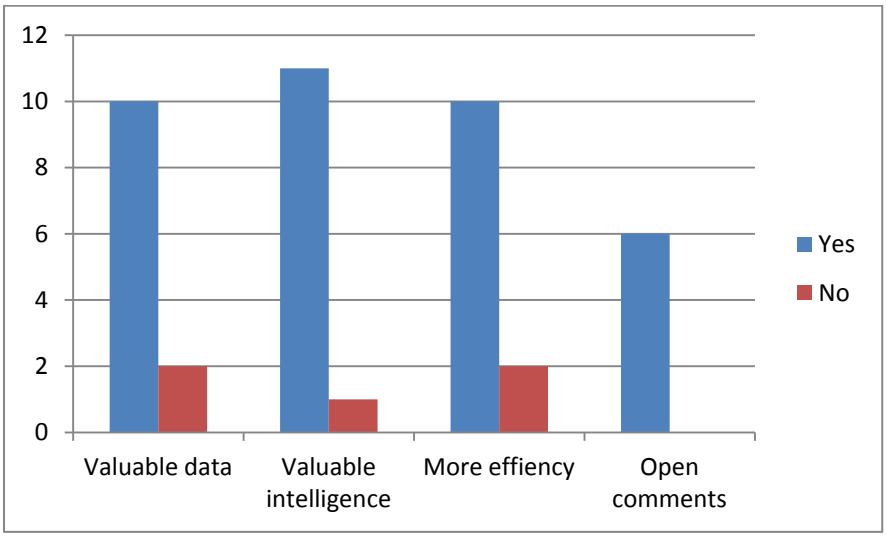
5.8 An international centre for online threats

As a contrast we asked respondents to show their opinion on the concept of an international centre in which online threat reporting and analyses takes place. Such a centre at present does not exist. What is their perceived value of such a centre? We also took the concept one step further and asked whether this centre should also have coordinative powers. We start however in a general way. Would the participants value an international centre as meant to be a form of extension of the national centre as described in the introduction to the survey?



Graph 22, question 7 does your organisation wish to be involved should an international centre be created?

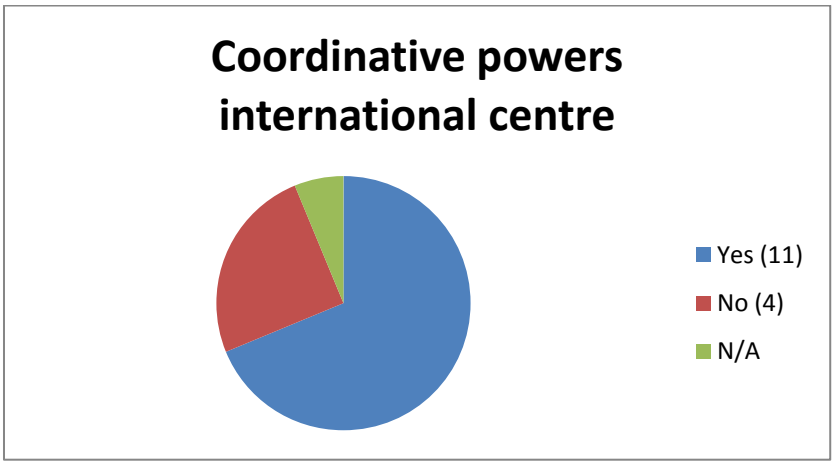
So we know that roughly 2/3 of the respondents would value an international centre. The next question referenced what the participants would expect this international centre to do, graph 23.



Graph 23, question 7.1 what would you expect an international centre to do?

Next the survey gave the respondents the possibility to fill in open comments. These are very diverse. They range from coordination between entities, setting best practices and receiving and analysing data, to mere coordination without technical tasks. One respondent said that the international centre would only mean more reporting with no additional value and for that reason did not want one. Below on page 28 this subject is discussed in more detail when we look at motivation and suggestions supplied by the respondents.

As said, we built the question up, see graph 24. Would those that value an international centre also want it to have coordinative powers between the different entities on cross border enforcement cases?



Graph 24, question 7.2 would you want the international centre to have any form of coordinative powers on cross border enforcement cases?

We also asked participants, to specify their concerns towards coordination at an international centre. An important note to make, is that these entities answered yes in general. This led to the following concerns, of which one was positive anyway:

- Fear for loss of independence through coordination from abroad on activities and decision making;
- Difficult to clarify respective scope of action;
- We do not need new centres, but need to work on existing problems;
- It would be more useful offering support for a coordination body/initiative/structure;
- For information security each topic is an individual matter. A centre makes no sense;
- Everybody who wants to can already share. No additional value to such centre;
- Those who don't have data, cry for a centre;
- Yes: Coordinative and administrative support for joint investigations.

In the interviews it was possible to go more in-depth into the concerns. From a police organisation's point of view it's important that a new centre should not duplicate what Europol already does. When I asked deeper, the suggestion was given that perhaps this centre could coordinate between LEAs (police) and NGOs and industry. When I followed up with "what about other LEAs (regulatory bodies)?", the reply given was that this had never been contemplated, but could be an interesting option.

The regulators provided a broader range of views. To show the different thoughts I include them all, because it clearly shows the needs of the enforcement agencies that are not police.

- Coordination and bringing the best people together.
- International coordination is welcome on predefined topics like tools, training and standardization of cooperation, e.g. through setting up international protocols on data sharing. Provide measures on reporting of data breaches.
- A turning point for coordination on intelligence in international cases.
- ENISA already has a role like this, but can only become an international centre with a coordinating role when LEAs (can) participate actively.
- Fear for loss of autonomy (both national and international).

- Europol could play its present role for all LEAs. It already has the expertise to coordinate on case level. Active sharing of data and intelligence between all can be added to the present role.

- To create efficiency. To prevent double work for everyone involved in an internet investigation. More at Interpol than at Europol level, but perhaps different regimes can be provided for. From light regimes of cooperation, as e.g. is this a violation of your law?, to full cooperation between EU member states. Where the Europol model is the example.

Respondents who answered no to question 7.1, see graph 23, were offered to motivate their choice. They had great concerns over an international centre for the following reasons:

- Legal issues with data protection in the different jurisdictions might impair success;

- The national DPA decides what can be shared with whom. So an international centre up front is impossible;

- The ones who share the most data run a risk of the highest penalties (*from a DPA, addition by DNC)*;

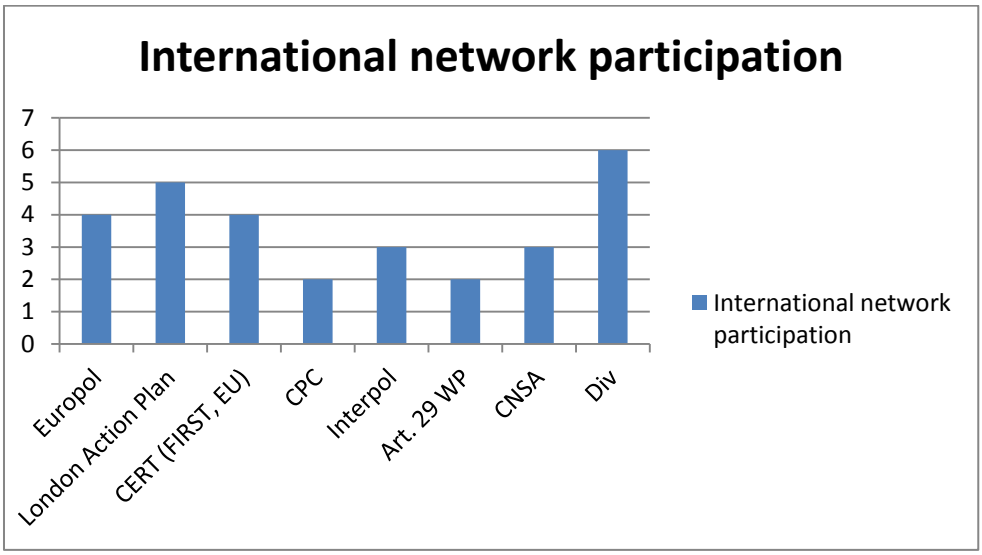
- It will not provide me with valuable data and expertise.

This is the first time in the survey that data protection issues were mentioned by respondents of standing in the way of cooperation. Hence, the suggestion of some to provide EU wide protocols on data sharing, so that a level playing field between countries and entities on this topic is created.

5.9 Participation in an international network group

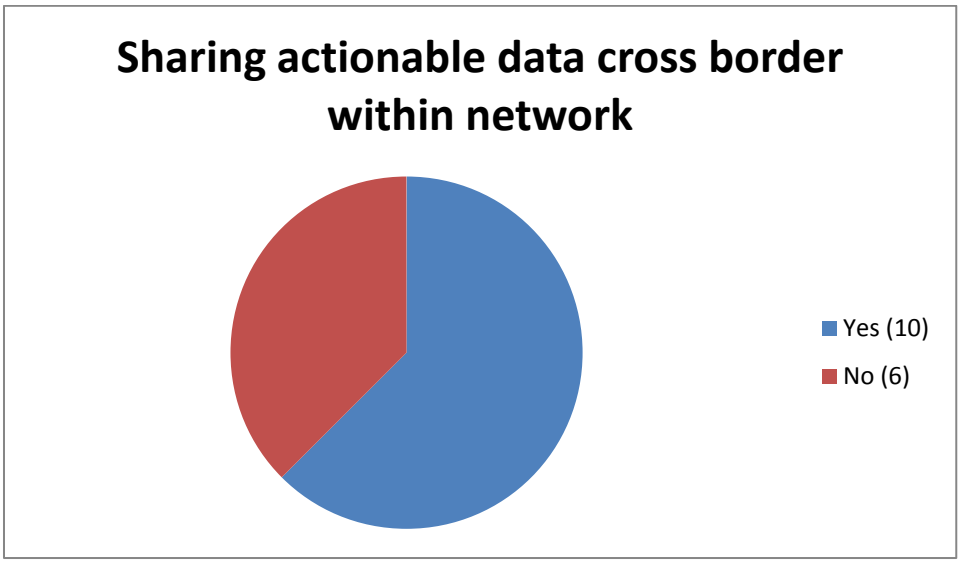
We also asked the participants whether they presently participate in international network groups. All but one answered that they participate in one or more networks (question 8.1). To delve deeper we also asked them to give their opinion on the value of this participation. Graph 25 shows the specified answer as to participation.

One regulator mentions that the CNSA, the EU's anti-spam enforcement community, has not been active over two years .



Graph 25, question 8.1 and 8.2 does your organisation participate in an international network group?

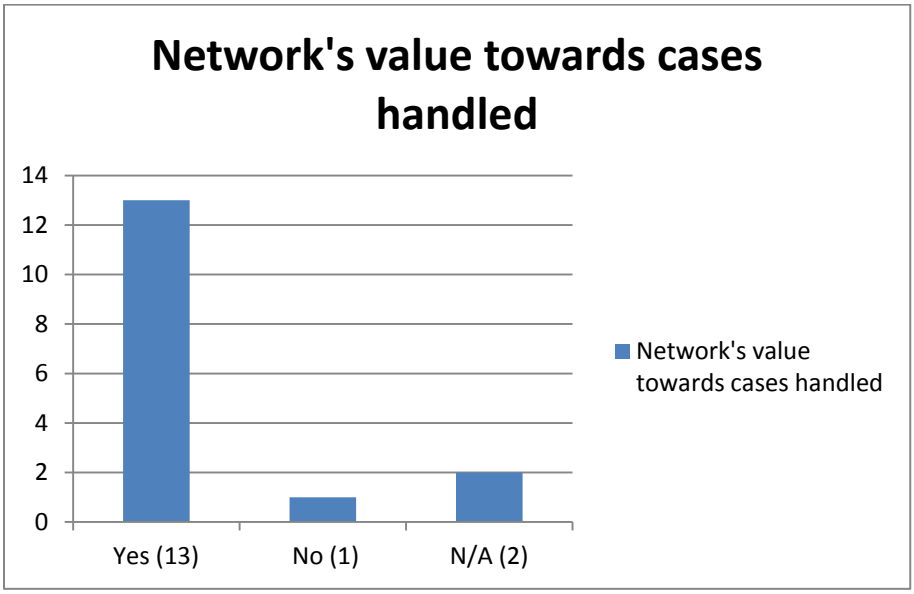
Next we asked whether the participants share actionable data within these networks. This may seem as a repetition of an earlier question, but is more focussed within the context of a network. Graph 26 shows the results.



Graph 26, question 8.3 do you share actionable data on cross-border cases within the network?

This means that over 1/3 of the respondents do not share actionable data with entities within their own international network(s). If we combine the answers of question 8.3 with question 5.8, we see that for most answering yes in 8.3 sharing data at the international level is an exception to the rule.

Most entities work on national cases. A conclusion we derive at from this data is that major international cases or cooperation outside police entities are an exception.

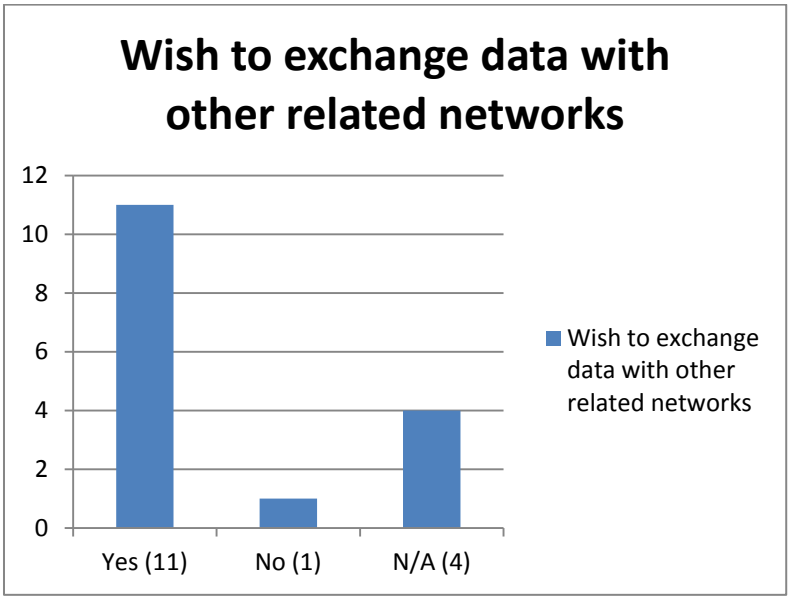


Graph 27, question 8.4 is the network of additional value to you concerning the cases you handle?

In order to be able to say something about international cooperation we asked whether the international network is of additional value concerning the cases that are handled by the participants. Graph 27 shows the responses. It seems to be in sharp contrast with the number of cases actually handled in cross border cooperation. A conclusion here is that more entities value the network concerning cases handled then actually share cross-border data related to cases. As said before more research is called for to find out the true value or effect of international networks. It is safe to state that this survey does not reflect the true nature behind the provided answers. E.g. did provided training or shared expertise helped solve national cases or informal exchanges, etc.? and is the network not of so much of value for cross-border cooperation cases? Some comments in relation to other questions like those in section 9 of the questionnaire can shed more light on the perceived value of the international networks.

One of the comments made in the interviews is the following from a regulator. “The greatest obstacle in international cooperation is that there is no level playing field in the sense of the way local laws allow investigations into cyber criminality and security, the way priorities within countries and organisations are set, the level of skills at colleague organisations and in the way privacy laws are implemented. Without a level playing field it hardly makes sense to try for international cooperation. This is the case even within the EU. Outside of the EU the challenge only becomes greater. There is no standardisation for cooperation. The development of tools and the (standardised) training of organisations could improve this. There is no Europol for spam that standardises and coordinates”.

These freely transposed quotes reflect the comments made above and below when we look at possible future topics to follow this survey up with.

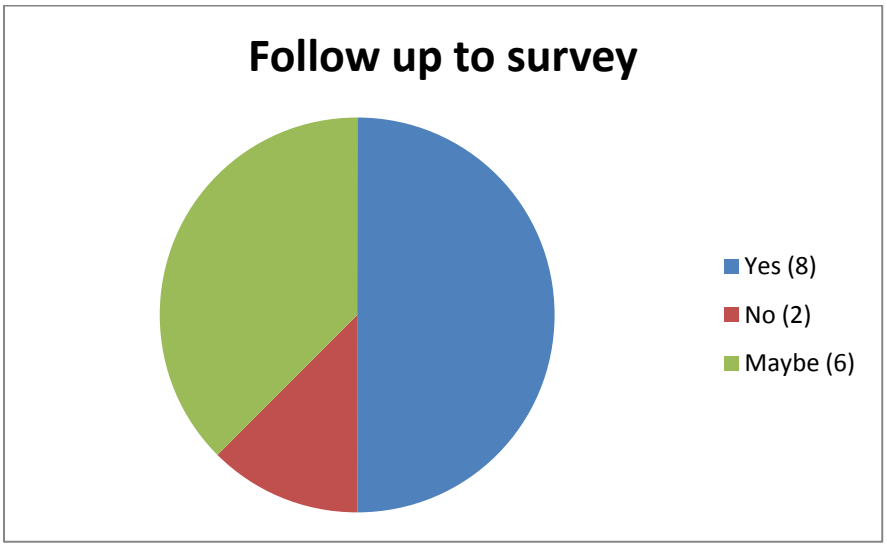


Graph 28, question 8.5 would you want to exchange relevant data from similar, related networks?

Next we asked the participants whether they would want to exchange data with entities outside of their own international network that participate in similar, related networks. Something they presently do not all do. Graph 28 shows their answers. 2/3 of the respondents to the survey express the wish to share date with different entities outside of their networks. Also it's clear that 25% has not answered the question, while each of these respondents has a function in making the internet safer. These respondents were not asked to specify their respective answers, but it may well have to do with not wanting to receive more data, because of the legal obligation to handle each complaint or each piece of intelligence individually, as was mentioned in an interview.

5.10 Second phase of the survey.

After asking the respondents about their everyday reality as well as their concerns and wishes, we gave them an explicit platform to stage their wishes. This way the survey gave them a chance to formulate their concerns in a positive manner. So, as a last question, we asked the participants: if there is to be a second phase to the survey, would you be interested to participate and followed this up with the question what topics should be on the agenda of this second phase. The results are, if only due to the diverse background of the respondents, inherently different, but some clearly point in directions that could be of interest to all respondents and beyond. We translated these into recommendations. But let's first look at graph 30 that shows the wish to participate and note that only two say no, an NGO and a CERT.



Graph 29, question 9.1 should there be a second phase after this survey, would you be interested to participate?

As said, in the last question of the survey, the participants could freely answer on topics that they think important for the future. This is a very diverse range of topics, most likely coloured by the individual backgrounds as well as the present level of sophistication an entity is at. If anything, the results show a multitude of topics that could be addressed in the near future, topics that can take national and international cooperation to a higher and more efficient level.

Suggestions come from most participants, including the ones answering 'maybe'.

- Division of tasks between different players to get more efficiency between countries.
- Set goals for an international centre for online threats.
- Set goals for competence of participating members.
- Concentrate on current positions and what it is we miss and try to fix that.
- Only if it does not double with other present initiatives.
- Two mentioned make sharing of data possible.
- Two mentioned making a personal data policy.
- Determine first who is to host this *(an international centre, DNC)*.
- Determine who takes part.
- Discuss how data is shared at the national and regional level.

- Information sharing.
- National clearing house.
- We have a lack of manpower, but would value information about on-going activities.
- Study into why Spot Spam failed and what needs to be changed to make such an initiative a success in the future.
- Direct reporting of citizens into an international reporting centre, including analyses and coordination from the Commission to address national NRAs.

The interviews added to these topics in a more elaborate way.

- Cooperation and the sharing of data between entities needs to be made compulsory by law. Including rules on a safe way of sharing data. Approved encryption rates set and create standardization through all these efforts.
- The ideal picture would be one organisation for all online threats. This leads to more data on the development of online threats. This way we may be able to predict what's coming next. Cases with a high threat level could be dealt with immediately.
- We have built a forensic lab. Others do not have this level of expertise. It is necessary to create a level playing field between regulators. All must have the same knowledge and tools.
- Organise trainings, webinars, so all can develop at the same speed.
- By meeting more frequently knowledge is spread at the same level. Knowledge can be shared. At the same time coordination of necessary data can be taken care off.
- There needs to be a common standard for exchanging data. It needs to be of the right quality, i.e. complete.
- A central spam database. Spam messages and data are centrally gathered and accessible through a forensic program. Through the database data is shared, efficiency is reached and the doubling of efforts prevented. The results are made available on a national level.
- Create a national centre. What can we achieve if we truly cooperated? Joint forces, operating from close proximity. It would straighten out processes, ease personal contact. Also a joint EU international centre, whatever and wherever, would be able to facilitate these processes.

- The law of my country says we can share data with each country, unasked even. So data is shipped across borders.

6. Interpreting the results

This survey has as main focus the state of implementation of National Cyber Crime and Online Threats Reporting Centres in Europe. For this survey the meaning of "a national centre" was strictly defined. The recipients were selected for reasons explained above. Interpreting the results, it is important to understand that only two initiatives claim to become a national centre in which more than one topic is dealt with and more, i.e. different, organisations (will) participate[12]. This report has shown that there are several initiatives referred to in the survey that are a national centre that fall outside of the definition, because they specialise in one form of online threat, e.g. fraud, botnet mitigation, security breaches or, a somewhat more general term, cyber crime. Almost all respondents allude to challenges and concerns to their tasks and several have provided valuable recommendations as they come from people working with these challenges every day. These are presented in the following two chapters.

6.1 The challenges of national and international cooperation

6.1.a. Cooperation outside the own category

Where data is shared outside the own category, most commonly by CERTs and botnet mitigation centres, it is usually followed by the comment that it is not a common practise to receive intelligence in return from non-involved entities. Some of the CERTs and botnet mitigation centres stated to actively share data with the police. An important observation that was made, is the following: there is no expertise available in the centres – at least in those that responded- to coordinate on any form of action beyond their own category. They do not have the (legal) power, hence any experience, to do so. This makes coordination at national level between different entities hard if not impossible.

It must however be noted here that on the other hand it seems hard for entities to share data, even if they wanted to, as several organisations are not willing or equipped to receive data. The comment that a few entities sort of gave up, is disconcerting in a so all-encompassing topic as online threats is. This creates to a situation that everything outside of the own category and country is dismissed and left to, yes to whom? At present the perpetrator himself, who can go about his business unhindered.

Another observation that presents itself, is that all participants that are not police agencies who commented on national cooperation state that reciprocal cooperation with police agencies is almost impossible. Several share data with the police but hardly ever something comes back in return. A comment from one police organisation that it had 'never thought about cooperation with other LEAs', is quite telling. Still, several other, non-police, entities point to the Europol/INTERPOL model for international cooperation as an example for how it could or should be organised for their

[12] The survey does not render enough data on these two initiatives to substantiate the claim beyond doubt.

category. Some take it one step further: we should all be in Europol or something like it, in which we all participate.

The main conclusion has to be that cooperation between the different categories fighting online threats is uncommon at national level. This is the same internationally.

6.1.b. Cooperation within the own category

International cooperation is organised the best in two categories[13]: police in Europol[14] and CERTs in CERT-EU and FIRST. Even this is hard as we were made to understand from the delivered comments. As one police organisation states: "due to the borderless nature of cyber crime and the timeliness with which information is received from abroad (particularly jurisdictions where there is no relationship with …[15] law enforcement) … my organisation is experiencing difficulties to have an accurate view on the threat landscape". We have to add that this entity answered to have near real time overview in general.

Several regulators, of different background, introduce the term level playing field. It is hard to share data and coordinate actions when there is a lack of sufficient skills, tools, resources or the same priorities with the receiving organisation. This often leads, so they say, to put a stop to or severely hinders cooperation and sharing data. Some claim that there is no use to attempt cooperation.

6.1.c. International coordination

Roughly 2/3 of the participants state, some hesitatingly, that international coordination is necessary in one form or another. The survey results show that several organisations state to be very efficient and have a view of how to mitigate the challenges they face. These organisations point to the lack of knowledge in other, not mentioned, countries. Others point to their own inability to fully cope with the online threats faced, due to several reasons as shown above.

However, in general the participants give off a call for guidance, while several plead for more (centralized) efficiency through more national and international cooperation. The most ambitious promote centralizing the way data is gathered and analysed in order to be able work more efficiently, as doubling work at the national level would be prevented. If this were to be organised this way, we add that at the same time it becomes clear to all involved which entities actually need to cooperate in a case. Cooperation is set out at the start of an investigation. Several respondents expect that

[13] Within botnet mitigation centres cooperation stems from agreements made between the participating entities, public and/or private.
[14] and INTERPOL, but this entity lies outside the scope of the survey, which was aimed at Eu(ropean) countries.
[15] Country name deleted by De Natris Consult due to assured anonymity.

through coordinated efforts more success can be gained. This does not take away anything from the expressed concerns around this topic that need to be addressed and are found in the recommendations.

In general the suggestions go from regular meetings where knowledge is exchanged, to firmly directed trainings, onwards to coordination on cases at the EU level after centralised gathering and analysing online threat data took place. If there are to be initiatives towards a more international approach to answer the challenges posed by the respondents, it is these topics they want addressed first.

6.2 What is the actual level of international cooperation?

The relevant agencies that answered the question on international cases show that delivering a case across a border or cooperate together to solve an international case is a major exception. (One police entity providing data mentioned to have shipped 50 cases across the border.) We safely conclude that the focus of all respondents is primarily on national cases. This is only logical as this is their main task. The true value of (the level of) international cooperation does not show from this survey. Neither does it show concrete figures of successful international cooperation between entities. As said this calls for further study.

We state that the following conclusion can be drawn from this survey. Where online threats are discussed and seen as a major international concern, national enforcement agencies are not prioritising these cases, due to the reasons shown above. Botnet mitigation centres deal with (the results of) online threats primarily at national level and struggle, due to unknown reasons, as they did not show up in the survey, to get enforcement agencies involved.

We also conclude that it is hard for most entities to share data internationally. Although most participants value being a member of an international network vis-à-vis international cases, we have to conclude that most do not work on such cases or as an exception only. Hence it appears that there is no focus on the foremost international threats on the Internet, except in the fire department like approach at national level at CERTs and a few noticeable police cases.

The survey hints at the fact that the topic of online threats in combination with national or international cooperation is too large, too overwhelming to cope with for an individual, national entity. Especially when there is no well-functioning national and/or international body assisting in cooperation. As said this needs further study, but the provided answer by a national botnet centre who stated “to have no powers to be able to coordinate beyond the own category” tells all. Results in mitigating online threats will always remain sub-optimal if this does not improve.

6.3 National law hindering successful enforcement

Seen from an individual entity's point of view the obligation to deal with each individual complaint is a major obstacle to successful enforcement. The legal obligation to formally respond to individual complaints is a legal task that is not suited to the online environment where threats like spam, phishing, fraud and worse are sent by the millions. It seems that the agencies that are allowed to prioritise are, though less productive in pure volume of output, more efficient in gathering and analysing data and intelligence as well in general have a better overview of the threat landscape. An explanation is that entities having to deal with every individual complaint do not prioritise on receiving complaints (in an automated way).

6.4 The quality of data

31% of the participants claim to have a, near real time, overview of the threat landscape. Of these most state that they could do better, but that this can only be achieved by fully automated receiving and analyses of data. Most respondents agree that non-automation leads to poorer quality, as it often leads to incomplete data and complaints. Some organisations state that the lack of resources and/or being understaffed stand in the way of bettering themselves. The (perverse) incentive mentioned in chapter 6.3 also stands in the way of receiving more and higher quality data.

Cooperation starts with an entity that is comfortable within its own working situation and has the resources and enforcement/investigative tools to do so. It appears that a significant part of the respondents are, in different degrees, not comfortable within their own role in securing cyber safety and security. Most claim that they could do better where their view on the threat landscape is concerned. Some need to become better. There is a task here for national governments to look into the possibilities and prioritise towards raising the levels of fighting cyber crime and ensuring cyber security in their respective countries. They go hand in hand and can't be viewed as two different subjects. To do so is to ultimately fail.

7. Recommendations

There are several recommendations to be made from the results of this survey. What shines out most is that in general there is a need for more coordination at the national and international level. With the exception of the police organisations and two others all plead for changes in the way online threats are dealt with. The background of respondents explains that wished for solutions may vary, but still a pattern is quite clear. We come to the following recommendations.

a. Level playing field

According to participants, from different background, there is no level playing field in the EU (and even less beyond) where fighting online threats is concerned. There are several suggestions all aiming for forms of standardisation as mentioned above. It is recommended that these suggestions are taken up at a central level, so that true needs, e.g. protocols, training, assisting the national level, that could create a level playing field are dealt with. By providing for these steps an efficient and meaningful level of cooperation against different forms of online threats can be set up.

As most organisations stated that they want or need to have a better view on the threat landscape, part of creating a level playing field lies in providing in the right (analyses) tools and educated people at entities. To achieve said level playing field national governments most likely need to look into the way fighting online threats is prioritised at the national level and who exactly has or could have which role in achieving an acceptable online safety and security.

b. Coordination on intelligence and enforcement powers

The idea that efficiency can be obtained by making sure that actions are not duplicated or worse, is a valuable one. Online threats are often aimed at more countries at the same time and perhaps involve many different agencies not knowing they are working on the same intelligence. Coordination on analysed intelligence could mean a significant step forward in mitigating online threats at the national and international level as it brings entities together that, once actually working together, could solve an online threat.

Knowing who (potential) partners in another country are and understanding what enforcement tools or disruptive measures they can bring to a case, means that an online threat can be mitigated from the best possible angles. Calling for the participation of entities in this way, assures the highest chances of a positive outcome.

c. Share data at the national level

National governments can assist in creating laws or clearly defined rules, that allow data sharing at the national level and create a body in which different entities involved in dealing with online crimes meet regularly and thus build a relationship. Governments can look into ways in which a national body could coordinate between the different national entities and become a point of reference for international entities as well.

d. Share data on the international level

National governments can assist in creating laws or define clear rules, that allow data sharing at the international level. See further ad c above for possible initiatives at the EU and global level.

e. Sharing data between the different categories, public and private

To be able to work with high level and accurate data and/or intelligence is a prerequisite to fight online threats. Providing prior conditions that allow entities, specifically between public and private entities and vice versa, to exchange data are obviously called for. Industry as a standard has great quantities of (actionable) data in their possession. It is not common practice that this data find its way to law enforcement. This has to change as close public – private cooperation is needed to deal with online threats. Through laws or clearly defined regulation governments can make this possible.

f. Look into the creation of an EU online cyber threat/coordination centre

The EU can assist national entities by actively taking the lead in which way and to what extent coordination at the EU (and global) level could be provided for. It is clear that national entities will not achieve the needed level of cooperation between categories that allow for tackling online threats on their own accord. Potential topics have been discussed above. There is not much use in losing more time.

g. Proactively assist countries in developing their online threat skills

This survey shows that the differences between Member States, and entities within Member States, are huge. The EU could look into (training) programs that assist entities at the national level to become more effective. From assessments of the implementations of relevant EU Directives, to training programs and perhaps financial aid. Centralized training also provides for the necessary contact between the experts of entities; the start of any cooperation. The past years have made clear that online threats are not solely national problems. The weakest link in the chain could and usually does provide near unconquerable problems for the (entities in) other countries. This needs attention and mitigation.

h. Study into the effect of sharing (actionable) data at present

Most entities state they receive and share (actionable) data in some form. This survey does insufficiently show the following:

a) the impact of data shared;
b) how often data is shared;
c) whether this leads to priority changes at the receiving end;
d) actual cooperation between different entities on cases and
e) diversify these question at national and international level.

This is of great interest as only the sharing of data and intelligence in combination with actual cooperation on cross border cases can make a difference in the end, where the main international online threats are concerned.

i. A meeting place

There is a need for different agencies to meet and discuss, in order to build trust and to create an atmosphere in which information and data is shared, actions coordinated and enforcement powers or disruptive tools used in the most efficient and effective way. Where they can formulate concerns and recommendations on behalf of the EU and national governments. It is recommended that such an institution is created. Several entities hint at the Europol model for all involved agencies. We wonder whether the European Cyber Crime Centre could provide such a role?

8. Conclusion

This survey shows beyond doubt that there is a lot left to be desired by entities involved in online threats. Steps are necessary at the national and international level that ensure better cooperation in the form of the sharing and cross referencing of data. There is a distinct need for more efficiency and a call for guidance at a central level. Some prefer only a very basic level of guidance, where others would prefer full coordination and analyses of data at the EU level.

Most national governments from countries involved in this survey as well as the European Commission presently prioritize in mitigating online threats in some form or another. The Commission allocates millions of Euros to prevent cyber crime and enhance cyber security. Those involved in this allocation may well do good to read the recommendations of this survey, as the entities involved in dealing with (the results of) online threats have distinct needs that have to be taken into account in order to have a chance at successfully mitigating online threats. Most participants made it clear they could do with (a form of) guidance on these topics. Even the ones most advanced. In short: to create a level playing field, to set up protocols, collective trainings and systems for sharing data and intelligence between all categories that participated in the survey and thus create a higher level of efficiency through (inter)national coordination.

Only when individual entities receive assistance and guidance in the field of national and international cooperation, will chances at a successful enforcement, (economic) disruption and the mitigation of direct threats in the online environment, change for the better and true successes be reached. Perhaps even by the combined effort of all just mentioned.

Annex 1 Remaining questions

How often do entities receive data or intelligence from different sources and what is the spread in quality of received data?

What organisations would perform better with near real time data and do those that need it actually have access to this data?

What are the true numbers on shared data and the quality, effectiveness of the data shared?

How can data and intelligence sharing become more natural for entities to engage in?

What are true figures of international cases on online threats, who participate and can results of international cooperation be measured?

In how far do entities actually cooperate on a cross border cases or is information or a case referred to a colleague entity without further involvement?

What is the level of effectiveness reached by law enforcement and regulatory agencies in cases and how does this compare with (the quality of) data received by them?

This survey did not allow for statements on the main differences in outcome per category, as this was not on objective of this study. This takes a more elaborate effort with many more participants. The question how different entities hold up compared to each other and an explanation for the reasons behind potential differences is an interesting one, deserving further in-depth research.

Annex 2. Bio Wout de Natris, consultant and trainer/owner, De Natris Consult

Wout de Natris started De Natris Consult in 2011 after seven years in national and international cooperation on spam enforcement and cybercrime. Wout has experience as a spam investigator at OPTA, chair and coordinator of several national and international cooperation bodies and in anti-spam and awareness training. He has worked extensively in and presented regularly at international forums on spam and cybercrime, also in relation to IP resources and cooperation between industry and law enforcement. He is currently chair of the Cyber Crime Working Party with RIPE NCC. Wout is author of several articles on (inter)national cooperation involving online threats

Recently he did projects for ECP in the Netherlands on mobile security and a the introduction of a botnet mitigation centre. Provided an anti-spam training for three enforcement agencies in Canada. He developed a survey concerning national cyber threat incident reporting and analyses centres, sponsored by Microsoft.

At present he assists in organising two workshops at the upcoming Internet Governance Forum on international cooperation in combination with privacy and the lack of a level playing field. He is also involved in an international project for the roll out of botnet mitigation centres, assist the London Action Plan in organising the upcoming workshop and participates and works in a project on raising awareness in cyber security for SMEs.

As we humans are often the weakest link in cyber security, raising awareness is just as important as investing in security and may be a lot cheaper.

Wout blogs regularly on spam, cybercrime and cyber security. You can visit his blog at http://woutdenatris.wordpress.com/author/woutdenatris/ and www.circleid.com.

Annex 3. Statements

The following organisation kindly responded to our request to deliver a statement after having been sent a draft of the report for referencing.

The Cybercrime Coordination Unit Switzerland (CYCO)

“The study clearly shows where the deficiency in both national and international cooperation is. This detailed statement, and the numerous valuable recommendations will definitely be useful in improving the practice”.

Eric Freyssinet as chairman of the European Expert Group of Interpol on IT Crime

"Sharing should be the weapon of choice for a modern fight against cybercrime. Sharing experience, information as well as brain or calculation power. To avoid duplication of efforts, but also to create together a richer and more accurate picture of the situations. It is also about making decisions together on the most efficient solutions and coordinating action. Of course such efforts must take into account the need to always protect personal data, keep in mind the objective of protecting the victims and bringing the suspects to the courts. The secret for success is to be able to associate all actors - should it be in a variety of roles and implications and create an environment of trust between all of them : victims, industry, law enforcement and justice, public and private research."

FICORA

FICORA recognises that “a proper response to security threats requires on one hand actionable, reliable data on reported incidents and threats from partners across the globe on other hand reliable action on countries where we report threats observed to be originating from respective areas. Internet security requires global cooperation”.

Hellenic DPA

“The HDPA agrees with many of the recommendations provided in the final report. More specifically, as e-crime perpetrators become more sophisticated each day and the threat environment evolves, it becomes evident that EU needs to be able to combine its forces and handle e-crime in a unified manner through exchange of information and technical expertise. Some ideas towards this direction, as outlined in the report, could be the establishment of a unified international centre for online

threats, the development and adoption of data exchange standards and rapid communication channels, online or offline training in matters of handling online threats (ex. investigating spam cases), exchange of actionable data, and central incident / spam databases, etc. The HDPA notes that the protection of personal data and privacy of all relevant stakeholders should be central in any cybercrime handling approach and, to this end, would encourage any further proposals and/or actions regarding this issue in the future.

Concerning future debates on the report, the HDPA would be interested to be informed and/or participate, especially on issues related to data protection and privacy (e.g. exchange or information and/or personal data breaches), as well as the establishment of the EU Cyber Crime Center. We suggest that these issues are already taken into account in your workshop proposal for the upcoming IGF in Baku."

OPTA

"OPTA supports the recommendations in the report that sharing data across borders is of great importance to be able to effectively deal with online threats. Legal and operational arrangements need to be in place to exchange data on both threats and threatening parties in a timely manner. The most important factor in the willingness to exchange data however is trust between the exchanging parties".

Signal Spam

"A necessary step towards better involvement of each local player in a more comprehensive frame has been taken with this survey. We now have a clearer picture of the state of the art regarding intelligence gathering and data sharing (as well as mitigation) on cybercrime threats in many countries, and we need to build on this excellent work and the knowledge it brought to us. The conclusions and recommendations exposed in this survey should help us achieve that!"