DYŻURNET.PL Team Activity Report 2010

DYŻURNET.PL Team Activity Report 2010

A Member of INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES INHOPE

NASK

saferinternet.pl

dyżurnet.pl

European Commission
Information Society and Media

Warsaw, 2011

Dear Readers,

This report presents the 2010 activities of Dyżurnet.pl, the Polish Hotline, which has been committed to enhancing the safety of Internet users already for 6 years. We pursue this goal as part of the Polish Safer Internet Centre formed by NASK and the Nobody's Children Foundation. We focus on responding to information about illegal content on the Web and having it removed. Nevertheless, our work is not limited to handling reports from Internet users - we take up numerous initiatives in that area which are addressed to children, young people and professionals. The experience of our team is recognised by experts from many countries: in 2010, we played host to many representatives of countries where hotlines had been opened or were planned.

In this report you will find both detailed data on analysed incidents, and a general description of trends and phenomena observed over the year. The specific nature of the content that the team works with allows for observations and conclusions that take into account the most current threats in the virtual world.

The year 2010 was important to our work due to an amendment of the Criminal Code which introduced new crimes that have appeared or intensified simultaneously with the growth of the Internet. The Dyżurnet.pl team had previously signalled the need to adjust Polish regulations to the dynamically changing environment and to increase the safety of children and young people who use the Internet. The amendment concerns child grooming and propagating paedophiliac behaviours. Currently we want to draw your attention to enhancing the privacy of Web users, and especially the youngest ones.

Our activities would not have been possible without cooperation with the Police Headquarters, members of the Advisory Board and many parties interested in improving safety on the Internet. We wish to extend our thanks to them and to website administrators who are quick and cooperative in responding to our reports about abuse on their sites. We must also emphasize the role of the international INHOPE association of which Dyżurnet.pl is a member. Our cooperation with other response teams allows us to intervene efficiently also when servers hosting objectionable content are outside of Poland.
We hope you find the information useful.

Dyżurnet.pl Team

Dyżurnet.pl

Dyżurnet.pl is a team whose main responsibility is to respond to anonymous reports about illegal content on the Internet. The team's mission is to remove any illegal web content produced with the involvement of children or intended as a threat to their safety, or promoting racism and xenophobia. The Dyżurnet.pl team also analyses content reported by users, produces technical documentation, forwards information to the Police, ICPs and ISPs or international INHOPE hotlines. Dyżurnet.pl operations are based on national legal regulations and international cooperation within INHOPE. Apart from its core activity, the team takes part in projects that aim at raising the awareness of young Internet users with regard to Internet safety.

The hotline has been operating since 2005 in association with the Research and Academic Computer Network (NASK), initially as part of the Computer Emergency Response Team (CERT) Polska, and since 2010 within the NASK Academy. It is also a part of the Polish Safer Internet Centre.

For more information please visit
www.dyzurnet.pl

The Polish Safer Internet Centre

The Polish Safer Internet Centre was established in 2005 as part of the European Commission's "Safer Internet" programme. It is run by the Research and Academic Computer Network (NASK) and the Nobody's Children Foundation (FDN). The Centre has undertaken a number of comprehensive initiatives aimed at improving the safety of children and young people who use the Internet and new technologies. The Centre offers educational programmes (Saferinternet.pl), provides phone and online help in situations where children and young people on the Web are in danger (Helpline.org.pl), and acts on reports about illegal content on the Internet (Dyżurnet.pl).

For more information please visit
www.saferinternet.pl
www.helpline.org.pl

The Research and Academic Computer Network

The Research and Academic Computer Network (Naukowa i Akademicka Sieć Komputerowa, NASK) is an institute that focuses on research and implementation. In 1991, NASK connected Poland to the worldwide Internet. Today, it carries out projects centred on the quality of ICT services and IT system security, and in particular on biometric identification methods.

Operating for 15 years as part of NASK has been CERT Polska — Poland's first Computer Emergency Response Team that cooperates closely with other such teams worldwide. In 2010, NASK and the Internal Security Agency (ABW) were awarded the "Teraz Polska" badge of quality for the ARAKIS-GOV detection and early warning system for government networks.

NASK maintains the national internet domain name registry for the .pl domain. A partnership programme launched in 2003 now allows registering domain names with over 140 companies.

NASK is also a data network operator and offers Internet access and security services to business, government and academic clients.

The NASK Academy is a NASK division responsible for creating and implementing training, educational and awareness programmes. In developing the curricula and conducting training courses NASK uses its own know-how and cooperates with partners. The Academy comprises two teams: Dyżurnet.pl and the Training and Education Team.

Among other things, the Academy conducts non-profit activities as part of the European Commission's "Safer Internet" programme. The free educational offering is addressed to many audiences from various age groups: children, young people and adults, including educators, members of associations that work for children, representatives of universities, government institutions, the Police and the judiciary.

The NASK Training and Education Team also offers specialised training courses for business, public administration and academic institutions. The training topics include e.g. ICT system security, ICT network modelling, optimisation, control and management, Internet domain registry maintenance, as well as biometric authentication and identification methods. The training offering is tailored to the needs and level of the audiences, and the scope can be extended with new topics.

For more information please visit
www.nask.pl
www.cert.pl
www.akademia.nask.pl

The International Association of Internet Hotlines—INHOPE

The mission of the Association is to support and enhance the performance of Internet Hotlines around the World; ensuring swift action is taken in responding to reports of illegal content making the internet a safer place.

The international cooperation dates back to 1997, when, on the initiative of the British Childnet International, the idea was conceived to establish a forum for the international exchange of experience among national Hotlines. Initially, the forum operated as part of the European Commission's "Daphne" programme. In 1999, the Forum transformed into the INHOPE Association, which was still supported by the European Commission, but now as part of the "Safer Internet" programme.

Currently, there are almost 40 INHOPE member teams in Europe, Asia, North America, Africa and Australia. The Association has been developing a set of guidelines ("Best Practices") to be implemented by all the teams. During internship or expert training sessions, team members can also learn in detail about the procedures, law and specific issues found in other countries. The main benefit from the international cooperation within the network of trusted hotlines is swift response to reports about illegal content hosted on servers outside of a hotline's country.

The INHOPE association also offers assistance to new response teams with regard to work organisation, cooperation with partners and employee training.

For more information please visit
www.inhope.org

Komitet Konsultacyjny

Representatives of government agencies, the law enforcement and judiciary, universities, business and NGO's sit on the project Advisory Board. The responsibilities of the Board include support, assistance, knowledge sharing and active involvement in the activities of the Polish Safer Internet Centre.

The Advisory Board comprises representatives of:

- **The Ministry of Science and Higher Education**
- **The Ministry of Interior and Administration**
- **The Ministry of Justice**
- **The Ministry of Infrastructure**
- **The Ministry of National Education**
- **The Polish Police Headquarters**
- **The Office of Electronic Communications**
- **The Office of Competition and Consumer Protection**
- **The Polish Chamber of Information Technology and Telecommunications**
- **The Office of the Ombudsman for Children**
- **The Polish Society of the Phonographic Industry**
- **The Polish UNESCO Committee**
- **The Orange Foundation**
- **The Warsaw School of Social Sciences and Humanities**
- **The Centre for Citizenship Education**
- **The National In-Service Teacher Training Centre**
- **Pixelate Ventures Sp. z o.o.**

The Coalition for Children's Safety on the Internet

The Coalition for Children's Safety on the Internet (Porozumienie na rzecz Bezpieczeństwa Dzieci i Młodzieży w Internecie) is a voluntary initiative established in 2009 by leading ICT companies, NGO's specialising in network security, and public institutions working in that area. The main objective of the Coalition is ensuring safety for children on the Internet, and especially combating illegal content defined as illegal pornography as well as incitement to violence and hatred on national, ethnic, racial or religious grounds. The Coalition has currently 20 signatories, but the initiative is still open to new members.

For more information, please visit
http://bezpieczniewinternecie.pl

The core activity of Dyżurnet.pl is comprehensive handling of reports on potentially illegal content submitted by anonymous Internet users. Since 2005, the team has analysed over 16 thousand incidents (Fig. 1). Most users fill in the web form on www.dyzurnet.pl (over 4,500 reports in 2010). A minority use the dedicated email address (over 300 reports), and the automated telephone hotline is used sporadically (fewer than 10 reports).

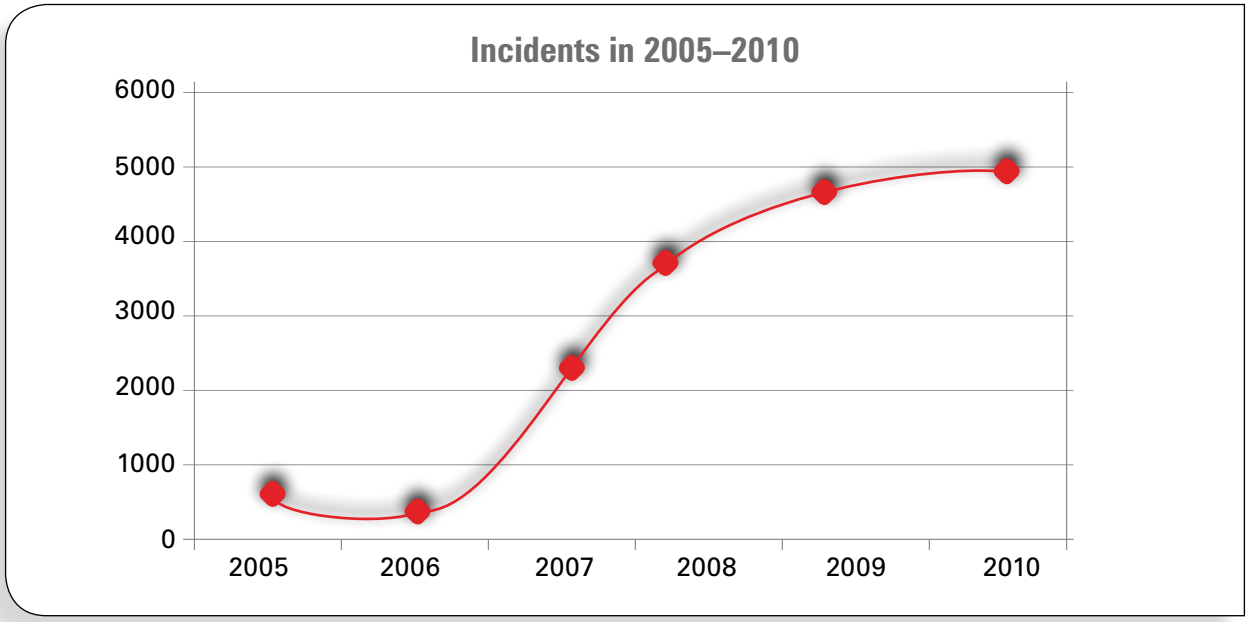


Fig. 1. The number of incidents analysed by Dyżurnet.pl in 2005–2010

In 2010, the Dyżurnet.pl team processed over 400 reports monthly on average (Fig. 2). The growth was significant compared with the previous years, especially as no promotional campaigns were carried out during that period.

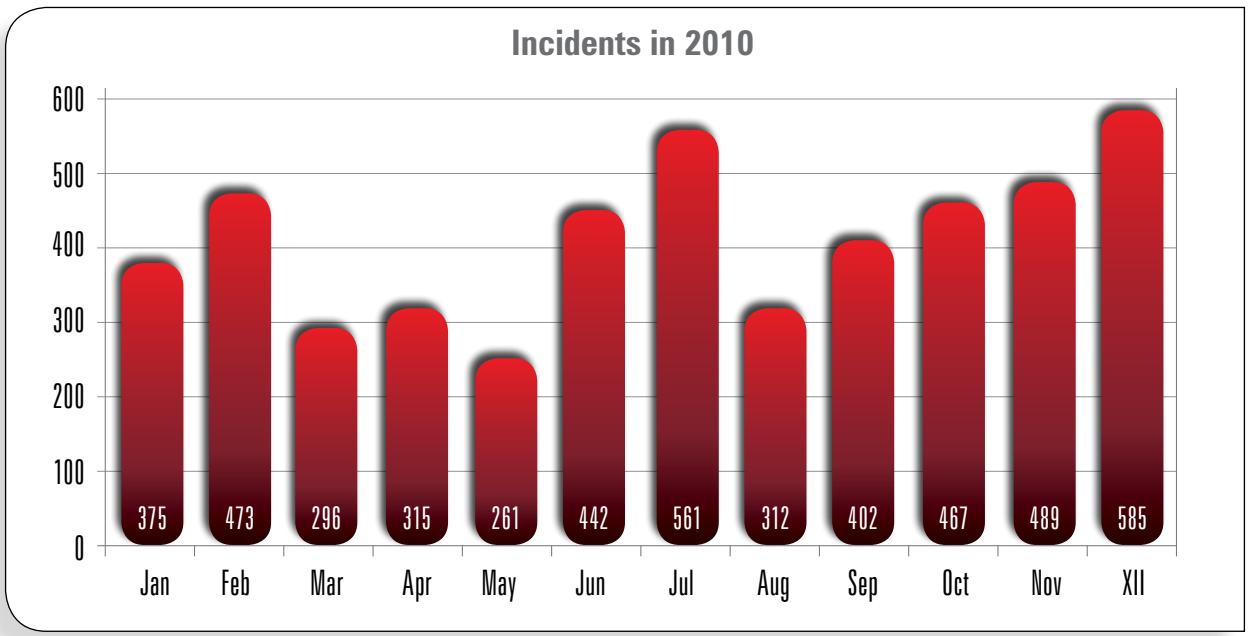


Fig. 2. The number of incidents in 2010

According to European Commission guidelines, since early October 2010, national hotlines are required to monitor the effectiveness of their actions against websites where child pornography was published. In the light of new procedures and the analysis of collected data, most such pages are quickly removed (Fig. 3). Currently, we are unable to determine whether such content is removed due to actions taken by response teams in countries where servers with illegal content are located. The monitoring procedure still requires some improvement and alignment with INHOPE guidelines.

The Dyżurnet.pl team receives reports about potentially illegal content on the Internet. Apart from notifications about dramatic child abuse and related pornography, the team also responds to information about other harmful online phenomena. Figure 4 shows the results of an analysis of 2010 incidents according to the adopted content classification. For yet another

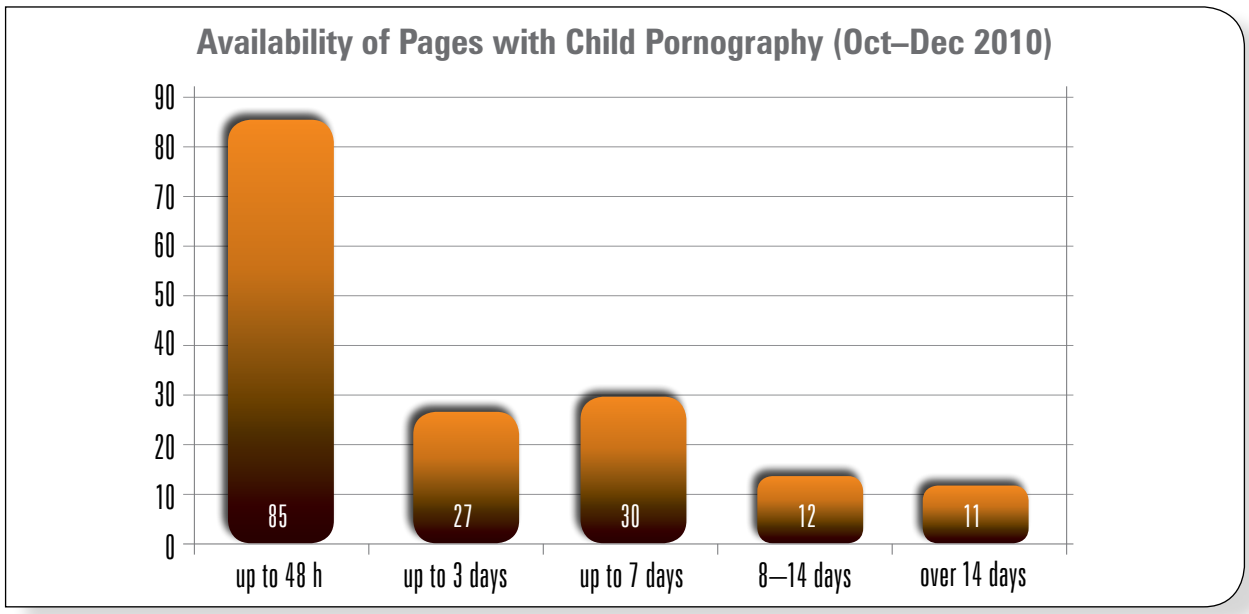


Fig. 3. The availability of a web page with child pornography after reporting it to Dyżurnet.pl

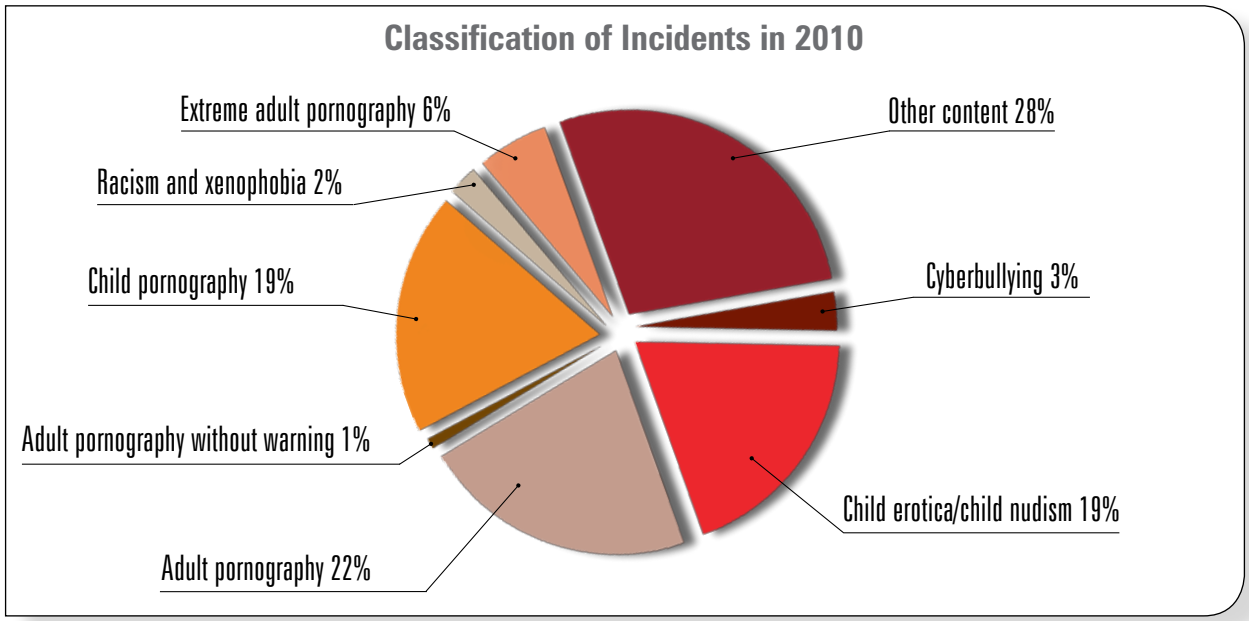


Fig. 4. The breakdown of analysed incidents

year running, Dyżurnet.pl has been observing a large group of reports about "other content", i.e. content that is not necessarily illegal, but certainly harmful to young Internet users, e.g. animal abuse, profanity or encouraging the misuse of pharmaceuticals.

Most reports classified as "other content" are web pages linking to other pages that present the sexual abuse of children, but do not contain illegal images, videos or other content themselves. In 2010, they made up 64% of the "other content" reports. This category also covers forums with links used to exchange information about content posted on the Internet, including passwords. Such forums serve as bulletin boards for people who seek such information.

Reports about pornographic content that involves minors are the main group. Analyses conducted by the team show that most of them do not qualify as child pornography but rather adult pornography (models often impersonate minors), child erotica or nudism. Some of the reported content is no longer available during the analysis, is password-protected or requires downloading to the hard drive, which is not allowed by the hotline's procedure. Figure 5 shows a comparison of the qualification of reports about child pornography by the submitters and later by the Dyżurnet.pl team.

The Dyżurnet.pl team runs a basic technical analysis to establish the location of the server hosting illegal content, because this determines further actions.

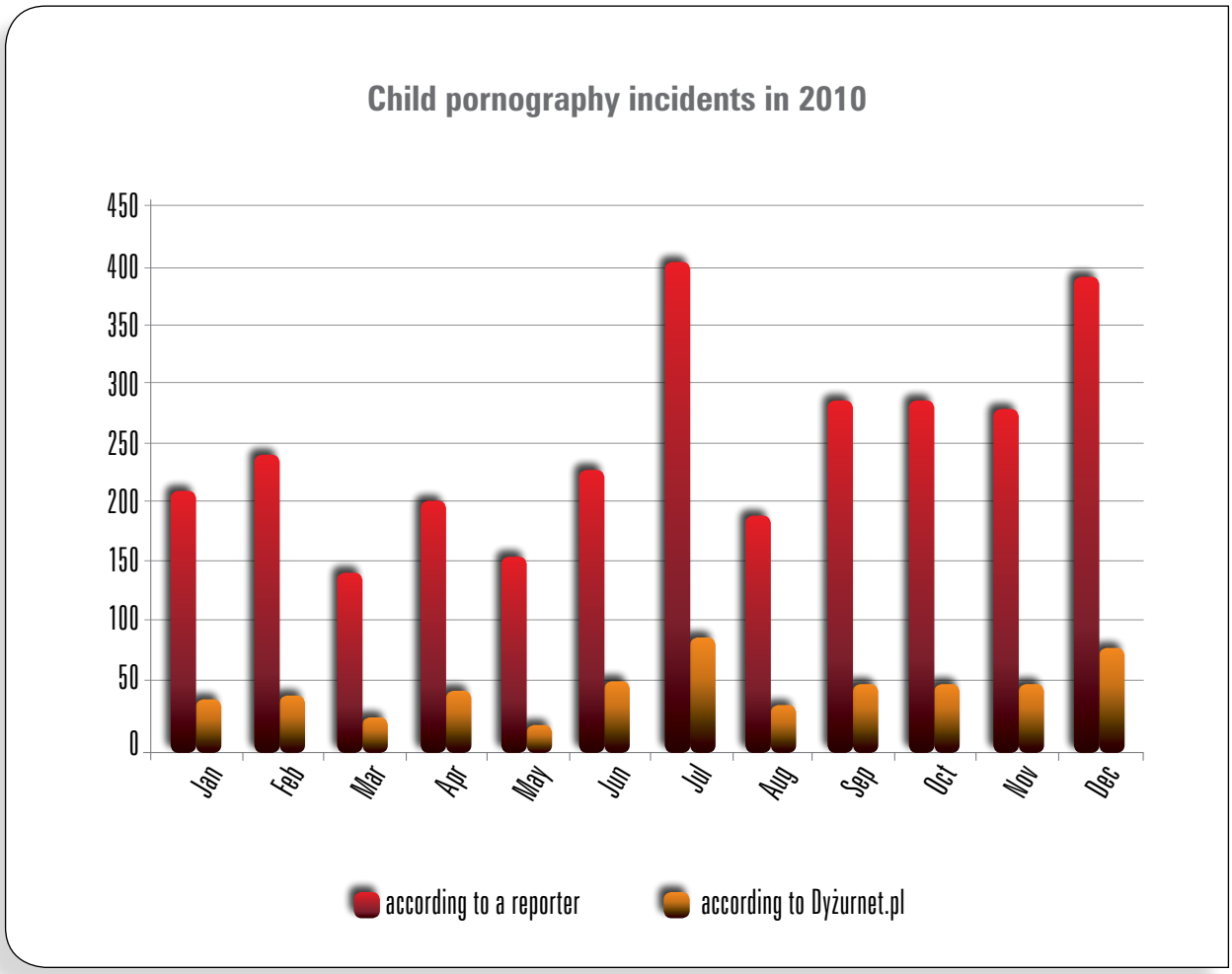


Fig. 5. The breakdown of reports concerning child pornography in 2010

Figure 6 shows the location of servers. They are usually located in the US, Russia and Holland. All those countries are INHOPE members; consequently, cooperation in removing illegal content is efficient as long as the reported content violates the local law.

Action against illegal and harmful content is taken according to adopted procedures. The most frequently taken course of action is contacting other INHOPE response teams (1078 cases) as well as website or server administrators (257 and 167 cases, respectively). A significantly lower number of cases are forwarded to other organisations like CERT Polska or Helpline.org.pl (82 cases). Information about potentially illegal content posted on servers located in Poland or a country

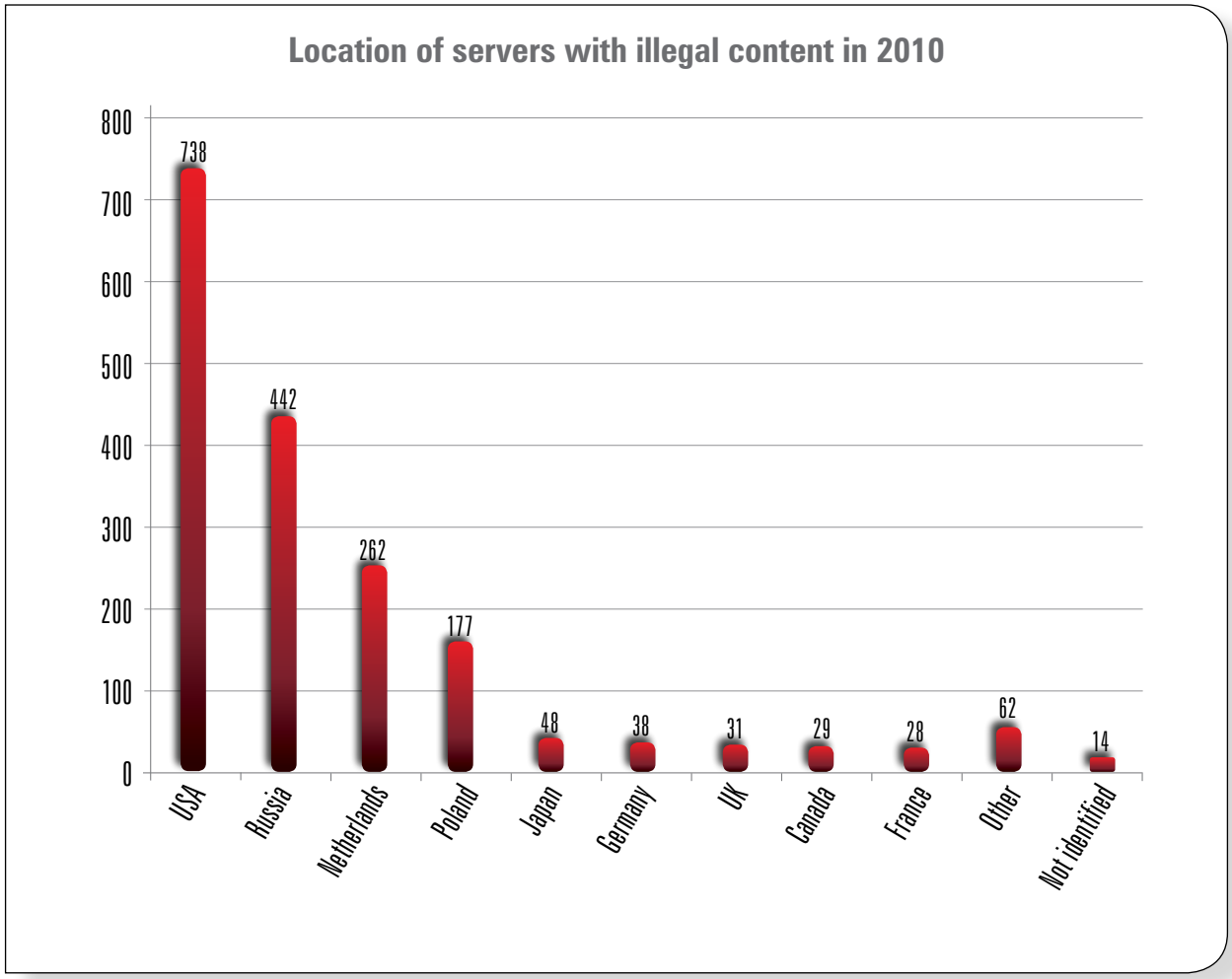


Fig. 6. Server locations

not represented in INHOPE is immediately forwarded to the Police (39 cases). The role of website administrators in user safety is increasing. Forms and buttons that allow the quick submission of abuse reports, and especially teams with extended working hours (the support team of nk.pl works 24/7, for example) help to respond to harmful or illegal content quickly.

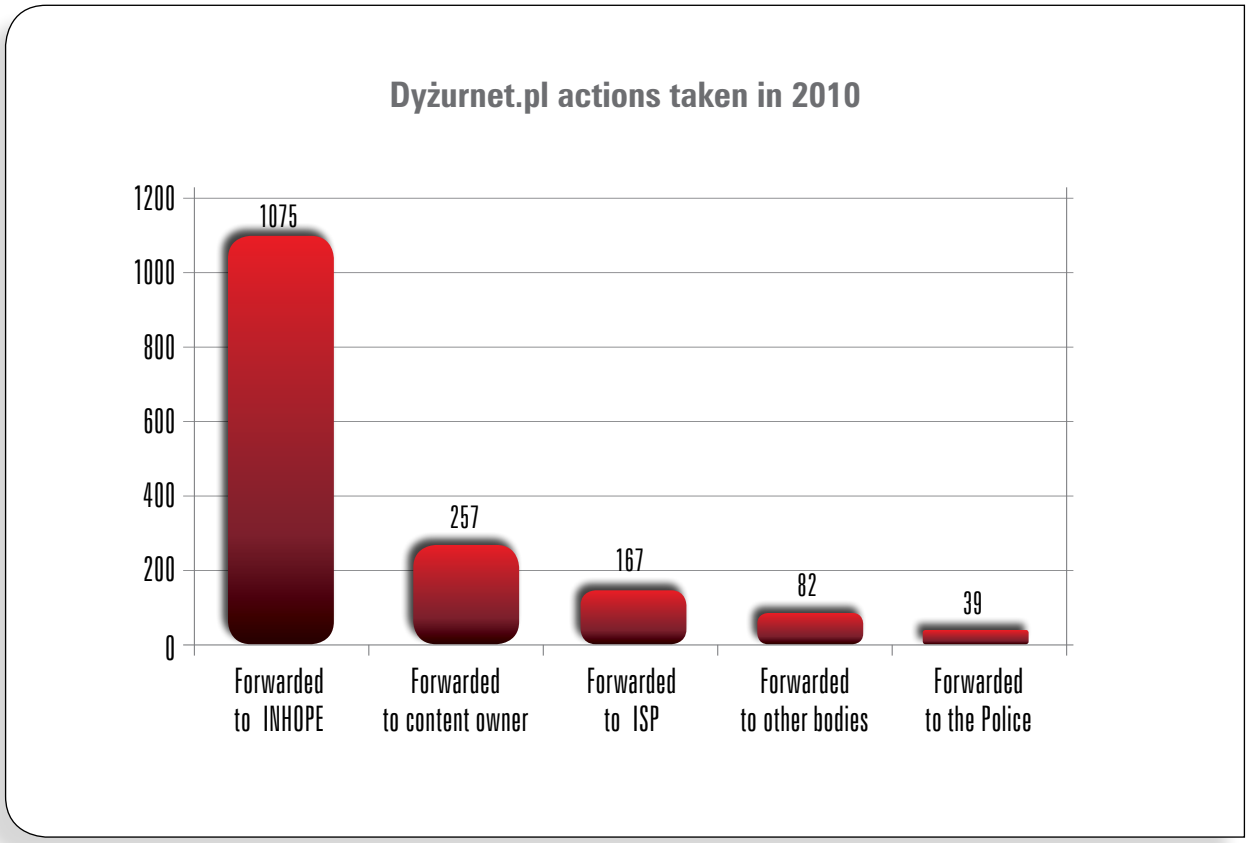


Fig. 7. Actions taken against illegal and harmful content

Every year, Dyżurnet.pl takes part in many events that raise public awareness of children's and young people's safety on the Internet. In 2010, the team participated in the following initiatives:

Safer Internet Day

Observed on the initiative of the European Commission since 2004 (since 2005 in Poland), it aims to promote efforts for safe access to Internet resources by children and young people. The organiser in Poland is the Polish Safer Internet Centre. In 2010, Safer Internet Day was observed on 9 February under the motto **„Think before you post"**. During a conference accompanying the national events, a team member showed a presentation of the Dyżurnet.pl activity, talked about its achievements in combating illegal content on the Internet and presented statistics on the reports.

The 4th International Conference "Keeping Children and Young People Safe Online"

The conference organisers were the Polish Safer Internet Centre and Klicksafe, which manages a German project to improve online safety for children and young people. A part of the European Commission's "Safer Internet" programme, the conference was held on 28–29 September, and the main topic was the safety of social network users and online privacy protection. A Dyżurnet.pl representative showed current report statistics and discussed new trends in online threats observed by the team.

The "To Be Safe Online" Seminar

The organisers of the event were NASK and the Police Academy in Szczytno. The meeting consisted of three blocks which drew 900 participants in total. The first block was dedicated to 7–9 year old children, the second one—to upper secondary school students, and the third one was addressed to adults involved in education on the proper use of the Internet. The Dyżurnet.pl team actively participated in the organisation of the event and provided expert support in the preparation of the block for the youngest participants - the **"File's and Folder's Adventures on the Net"** show. A Dyżurnet.pl member showed the adult audience the possible ways to respond to illegal content on the Internet as well as the significant role of the team in the process.

Workshops for Primary School Students

Sharing knowledge and experience with children and young people, i.e. those exposed the most to potential Internet threats, is an important responsibility of Dyżurnet.pl. One way of doing that is by preparing training sessions. In 2010, Dyżurnet.pl employees together with representatives of the Social Initiative Association "The Responsible" (Stowarzyszenie Inicjatyw Społecznych „Odpowiedzialni") prepared classes in safety on the Internet for primary school students. Workshops for 7–9 year olds focused on general issues related to the Internet, using its potential, and developing specific responses to unexpected situations (informing an adult). Taking into account participants' developmental changes and interests, workshops for 10–13 year olds promoted safe behaviours when using social media (privacy protection) and introduced the topic of cyberbullying.

Study Visits

As part of its international cooperation, in 2010 Dyżurnet.pl played host to representatives of response teams and organisations forming new hotlines from various European countries. Such visits enable the exchange of experience in applying procedures, sharing best practices, and discussing trends in threats in specific countries. Dyżurnet.pl was visited by employee of an Internet Watch Foundation (IWF) – the UK hotline, as well as representatives from Bosnia and Herzegovina, Ukraine, Moldova and Hungary. Such visits are very important with regard to good cooperation among teams, which is necessary to respond effectively to reports about potentially illegal content.

Speaking at Events for Professionals

Dyżurnet.pl representatives speak at many Polish and international conferences every year. Presenting the work of Dyżurnet.pl is a very important element in raising awareness of ways to combat illegal content on the Internet. It helps us to reach the widest possible audience from various circles, e.g. IT specialists, educators or law enforcement representatives. Pres-

ence at international conferences is vital, as it enables the exchange of experience in ensuring safety on the Internet for children and young people. In 2010, team representatives spoke at the following events:

- Workshops for prosecutors as part of the TRES programme for protecting women's and children's rights in Ukraine, **"Protecting children online - Internet Hotlines"**, Kiev, 18–19 March 2010
- The international conference on **"The Effects of the Internet on Children and Youngsters"**, Budapest, 21–22 September 2010. Presentation: "Combating Illegal and Harmful Content on the Internet in Poland"
- The 14th **SECURE** Conference, Warsaw, 26–27 October 2010, organised for ICT security professionals. Presentation: "Initiatives for the Removal of Illegal Content from the Internet"
- The **"Modern Technologies in Education— Opportunities and Threats"** conference, Kraków, 24 November 2010, organised by the Chief Education Officer of the Małopolska Region for teachers and headmasters. Presentation: "About Harmful Content on the Internet"

The year 2010 saw a continuation of a training cycle for prosecutors, judges and police officers conducted as part of the "Safer Internet" project under the motto: **"Combating Internet-Related Crime - Cyberbullying among Children and Young People, Child Pornography"**. The goal was to present the activities of the Helpline.org.pl and Dyżurnet.pl teams, discuss new legal regulations on child pornography and paedophilia, the current situation, and the actions undertaken by regional representatives participating in the seminar. In 2010, the training sessions took place in Lublin and Olsztyn.

A Vicious Circle of Aggression

On 28 December 2010, the Dyżurnet.pl team received a report on a movie where a 2–3 year old child brutally abuses a cat. The case was publicised by the media and sparked a wide debate over animal abuse, uploading such content, and anonymity on the Internet. Even though the media did not publish the direct link, Internet users managed to find the movie themselves.

Posted on a popular website, the movie had almost a hundred thousand views and was reposted on many other sites with calls for help in detaining the offender. Soon before the movie was deleted from the original site, it had been commented on over 9 thousand times. Most users abusively and crudely threatened the author of the movie, the child and its parents. Commenters tried to track the author by searching for a similar nickname on other social sites. It didn't take long before the personal data of several people (including their phone numbers and home addresses) and links to profiles on other sites appeared, as nobody was certain who the actual uploader was. Their linked profiles were soon filled with comments and unlawful menace.

The commenters reported the actions they had taken—calling the Police, news media, hotlines and animal welfare foundations. All that was done to track the person responsible for the cat abuse as soon as possible.

On the one hand, we can see the good intentions of helpful users, but on the other hand, publishing more and more calls for help breeds more hatred and publicises the offending content. Disclosing personal data and threats to Internet users who happened to have similar nicknames didn't help the cause, either.

Eventually, the author of the film was detained following a police investigation. According to press reports, it was a 15-year-old boy who filmed his brother. The extent to which the Police used the findings of Internet users is unknown.

Aggression on the Web

A large portion of information submitted to Dyżurnet.pl are reports about aggressive behaviour and content that promotes aggression. It doesn't only present trolling and profanity on web forums, but also squabbles between people who are using a public forum instead of private messages. Another phenomenon is impersonating popular users and insulting other people in chat rooms. There are also reports about posts on forums, under articles, galleries or other editorial content with comments intended against the author (often pointing out stylistic or topic-related mistakes) or against people and facts that are the subject of the article. The largest number of such comments appeared on the Web after the presidential plane crash and during the presidential campaign.

Trolling is various kinds of hostile behaviour towards other Internet users, aiming at disrupting a discussion. The phenomenon can be observed on sites dedicated to the exchange of opinions, i.e. on discussion groups, forums, chat rooms etc. It could manifest itself as open contempt for other users, pointing out spelling mistakes in an obsessive way, or spiteful off-topic remarks. The perpetrators are called trolls and the phenomenon itself is very unwelcome and often countered by moderators and website administrators.

Flaming is the purposeful exacerbation of the exchange of views among users of various discussion sites which leads to a "war" with no holds barred. A flame often results in escalated aggression, abandoning the original topic, biting remarks, insults and even threats.

Another type of abuse is movies showing homeless or intoxicated people. Such content is preying on the ignorance or helplessness of the portrayed people. It is accompanied by scornful and insulting comments. Aggression is also associated with racist songs or websites dedicated to sports fans - topics that can be actively searched for by young people.

Minors' Profiles on Dating Websites

Profiles on dating sites often contain only photos that serve as the main basis for online relations (or an element that helps to continue a real life relationship in the virtual world). Such profiles hardly ever contain additional user information and fields like "Interests", "I like", "I dislike", "I dream about" are often filled with preset answers. The dialogue and interaction among users is based on photos and comments posted below. It is alarming that minors post photos with erotic poses. Comments posted by other users are very literal and crude. This could lead to inappropriate acquaintances or abuse in the form of copying and reposting photos on other websites where they can be commented on in an insulting way, ridiculed and used in cyberbullying.

It is important to note that setting up profiles on social websites (including dating sites) is often forbidden by the terms and conditions for people under 18 (sometimes 15) years of age.

Children's Privacy and Parents

One of the reports received by the team exemplified alarming disrespect for a child's privacy. The case was sensitive and difficult, because the page in question was published by the father in order to regain the right to contact his daughter following a divorce. Trying to use the potential of the Internet in good faith, the father unknowingly put her in danger.

The daughter's photos are accompanied with a dramatic description of the family situation and court rulings. There is information about the child's illness, a detailed map of her whereabouts, and details about the form and school she goes to. The details expose the child, who in the current family situation must feel lost and abandoned and can't protect her privacy. In such circumstances she may be looking for friendship and support from other adults.

The child may even be unaware that her image and personal data have been made public. She might object to that. The Internet is an open medium, accessible to countless users, who may include the child's schoolmates, teachers or even a future employer. Those are issues that parents should pay attention to when publishing any information or images of their children.

Social website administrators often reserve the right to use content posted on user profiles. It means that even if we mark an image or a movie as visible only to us or our friends, we could see it later in an ad or marketing gadget for the website. Parents care about their children's future by sending them to language courses or sports classes, and yet they fail to understand that posted images could pose problems in the future. Users need to be always reminded that **content uploaded to the Internet is in no way protected against copying and reposting against the original authors' intentions**. That is why an important aspect of children's privacy are photos which have no erotic or sexual overtones on the sites where they were originally posted by parents, but commenters draw viewers' attention to the sexual context. Open to vivid and broad interpretation are holiday photos and images from the beach, bathtime photos, pictures of gymnasts, child beauty or dance contest participants.

Cyberbullying

Cyberbullying is bullying with the use of modern technologies—mobile phones or the Internet. It can manifest itself in harassing, ridiculing or even intimidating people on social sites, discussion forums or Internet pages. The victims are very often children and young people, who perceive it as a very difficult, unsolvable problem. The wide range of cyberbullying types mainly stems from the unique nature of the Internet, its apparent anonymity, fragmentation and easy multiplication

Stalking is another form of cyberbullying is stalking using new technologies. In a case analysed by Dyżurnet.pl, a fake profile used only to humiliate the victim was set up and deleted dozens of times before the team was contacted. In 2011, new legal regulations will come into force that will penalise such behaviours.

of the content. A perpetrator who types insulting comments on a forum or blog hiding behind an Internet nickname is anonymous only to an extent. His or her anonymity is illusory, because tracking such a user poses no problem to specialists. A perpetrator often behaves impulsively and incautiously, because it is so easy to publish insulting comments or manipulated images. However, once a file has been published, it reaches a countless group of viewers, which makes the victim believe that "everyone knows", "everyone has seen" an embarrassing photo, and "everyone" laughs at insults. It is important to remember that a victim is convinced that there is no shelter from cyberbullying. Unfortunately, although Dyżurnet.pl and Helpline.org.pl teams help children and young people by responding to cyberbullying on the Internet, all files or comments cannot always be removed. They may be stored on foreign websites and contacting their administrators is difficult.

The Dyżurnet.pl team has been receiving a growing number of reports about cyberbullying among adults. Unfortunately, in such cases the team cannot intervene on behalf of the user—victims should take action themselves with the assistance of the Police or a lawyer. All evidence, e.g. printouts, email or SMS messages, should be preserved, because it will be necessary for further proceedings. Without court proceedings, a perpetrator can sometimes feel uncontrollable, which will provoke him or her to further actions. Cyberbullying may meet the criteria of various offences; therefore, it requires decisive response. If, for any reason, the victim cannot use the help of law enforcement agencies, he or she should try reporting abuse to the website administrators. It is always a good idea to read the terms and conditions as well as policies regarding reporting abuse towards also other users. Larger and responsible websites can be expected to offer such a possibility.

There are popular sites where users post pictures they find funny and add comments that can be crude. The team has made attempts to remove such photos. Unfortunately, this is difficult, because administrators are reluctant to recognise that the victim is right, do not respond to contact attempts, or require evidence, like ID documents or photos that confirm the person reporting abuse is depicted in the content.

Hate Speech and Hostile Language

Hate speech is a recently publicised phenomenon associated with the Internet.

It consists in using discriminatory, aggressive or even hateful expressions to create a negative atmosphere around specific people or social groups which could be subject to prejudice due to their race, ethnic origin, nationality, gender, psychosexual orientation or religion.

People who use hate speech are falsely convinced that they are anonymous and one of many Internet users, and consequently not accountable for their words and expressed views. Hate speech spreads on many web communities, forums, among people commenting on current events. It can be observed wherever there is any verbal interaction among users. Sometimes it is a unilateral form of communication directed against an author or web page owner.

The phenomenon is very dangerous, because it promotes intolerant attitudes based on stereotypes and closed to other nationalities, cultures or lifestyles. Sometimes it even calls for applying aversion expressed online in the real world, i.e. for direct violence against the victims of discrimination. Hate speech is dangerous to all Internet users and easy to come across; consequently, it is easy to become insensitive to it because of its ubiquity. This is especially harmful with regard to young people who grow up among intolerance and can develop such an attitude as adults. Hate speech can meet the definitions of various crimes and offences specified in the Criminal Code. The law forbids threats, inciting to hatred, and the public insulting of people due to their nationality, ethnicity, race or religion (including the lack of one). The Polish Constitution forbids any forms of discrimination, but specialists who deal with various forms of discrimination point out that the protection of people discriminated against because of their sexual orientation is inadequate. It should be noted that the Dyżurnet.pl team takes appropriate steps against reported hate speech but is sometimes limited by the location of the server. This is the case of racist pages on servers in the United States. Legal freedom of speech guarantees in the U.S. make it difficult for victims from other countries to exercise their rights.

If the Dyżurnet.pl team is unable to intervene, the case can be submitted to the Police or prosecutor's office as well as various associations and foundations that combat discrimination.

Privacy on Social Sites. Like?

The social site Facebook is gaining popularity in Poland. Users who are already familiar with social networks like nk.pl or grono.net are willing to use the American counterpart.

Social sites were designed to facilitate communication between friends or members of various communities. They provide a forum for the exchange of views and information, and build relations based on friendship, interests or knowledge. They enable users to pursue various activities, show their unique interests, skills, and also everyday lives. That is where problems often begin—careless users exchange all details about their lives, post many private photos, voice different opinions about their employers, schools or current events, often remaining unaware how many people can access that information.

Recruiters in companies admit that screening candidates' online lives is a part of the hiring process. People who don't mince their words commenting on their current employers or post inappropriate photos should not expect an invitation to a job interview. Every day there are media reports about people getting fired or divorced because of reckless Facebook posts.

Dyżurnet.pl recommends checking privacy settings on social sites. Facebook and other such sites offer many options. Some of them include hiding our profile from search engines. Most information or images should be reserved for friends only. When the entire profile is accessible to all, we can face unwanted consequences and lose control over posted content, which can be copied, for example. Pictures from a wild party or intimate photos are not always suitable for public access. Be careful when adding new "friends"—don't accept invitations from people you don't know and don't send invitations to strangers just to make your collection of friends bigger. Those are just a few pieces of advice on how to try and protect privacy on the web. It is important to realise the possible consequences of excessive exposure on the Internet and make informed decisions. Before uploading any content—an image, a movie or even a comment—consider how many people will see it, and how it can be used against your intention or even yourself. And by the way, do all your friends really need to know that you have a fancy for something sweet? Like?

Amended Criminal Code

Over the last few years, the Dyżurnet.pl team has urged that national legal regulations should be adjusted for the dynamic development of the Web environment. In June 2010, an amendment to the Criminal Code came into force which penalises issues that had remained beyond the reach of the judiciary. The amendment covers such harmful and dangerous Internet phenomena as child grooming and propagating paedophiliac behaviours.
Regulations in force since 8 June 2010:

Article 200 a.
§ 1. Whoever, in order to commit the crime specified in Art. 197 § 3 (2) (paedophiliac rape) or Art. 200 (sexual abuse of a minor) or to produce or record pornographic content, contacts a minor of less than 15 years of age using an Information and Communications Technology system, aiming to meet the minor by misleadingly exploiting an error or inability to comprehend the situation adequately or with unlawful menace, shall be subject to imprisonment for a period of up to 3 years.
§ 2. Whoever, using an Information and Communications Technology system or a telecommunications network, makes an offer of sexual intercourse, subjection to or performance of another sexual act or participation in the production or recording of pornographic content to a minor of less than 15 years of age and aims to actualise the offer shall be subject to a fine, restriction of liberty orders, or imprisonment for a term up to 2 years.

Article 200 b.
Whoever publicly propagates or approves of behaviours of a paedophiliac nature shall be subject to a fine, restriction of liberty orders, or imprisonment for a term up to 2 years.
Today, encouraging a child on the Internet to meet in real life in order to exploit the child sexually or produce

pornographic content with the child is already a crime. It is also a crime to make sexual offers to a child on the Internet and to aim to actualise such offers

Article 200b criminalises the propagation or public approval of paedophiliac behaviours. Consequently, not only web pages that explicitly present child pornography but also pages that approve of and propagate paedophiliac behaviours are now illegal.

Both types of crime are prosecuted ex officio.

The Amendment of July 2010 has also introduced a provision that enables combating a type of cyberbullying where intimate images are distributed without the consent of the people depicted. In such cases the prosecution occurs upon a private charge:

Article 191a.
§ 1. Whoever records an image of a naked person or a person engaged in a sexual act, using violence, unlawful menace or deceit, or distributes an image of a naked person or a person engaged in a sexual act without that person's consent, is subject to imprisonment for a term of 3 months to 5 years.
§ 2. The prosecution shall occur on a motion of the aggrieved person.

The Dyżurnet.pl team still points out problems that could result from the lack of a precise definition of "pornographic content", which is important especially when analysing often appalling content that borders on pornography and child erotica. This coincides with the general shift in European discourse from the term "child pornography" towards "child sexual abuse materials", which also includes the abovementioned erotic content.

When discussing the legal context of analyses of content reported to Dyżurnet.pl, it is important to note that most content is stored on foreign servers where other regulations are in force.

Dyżurnet.pl Plans for 2011

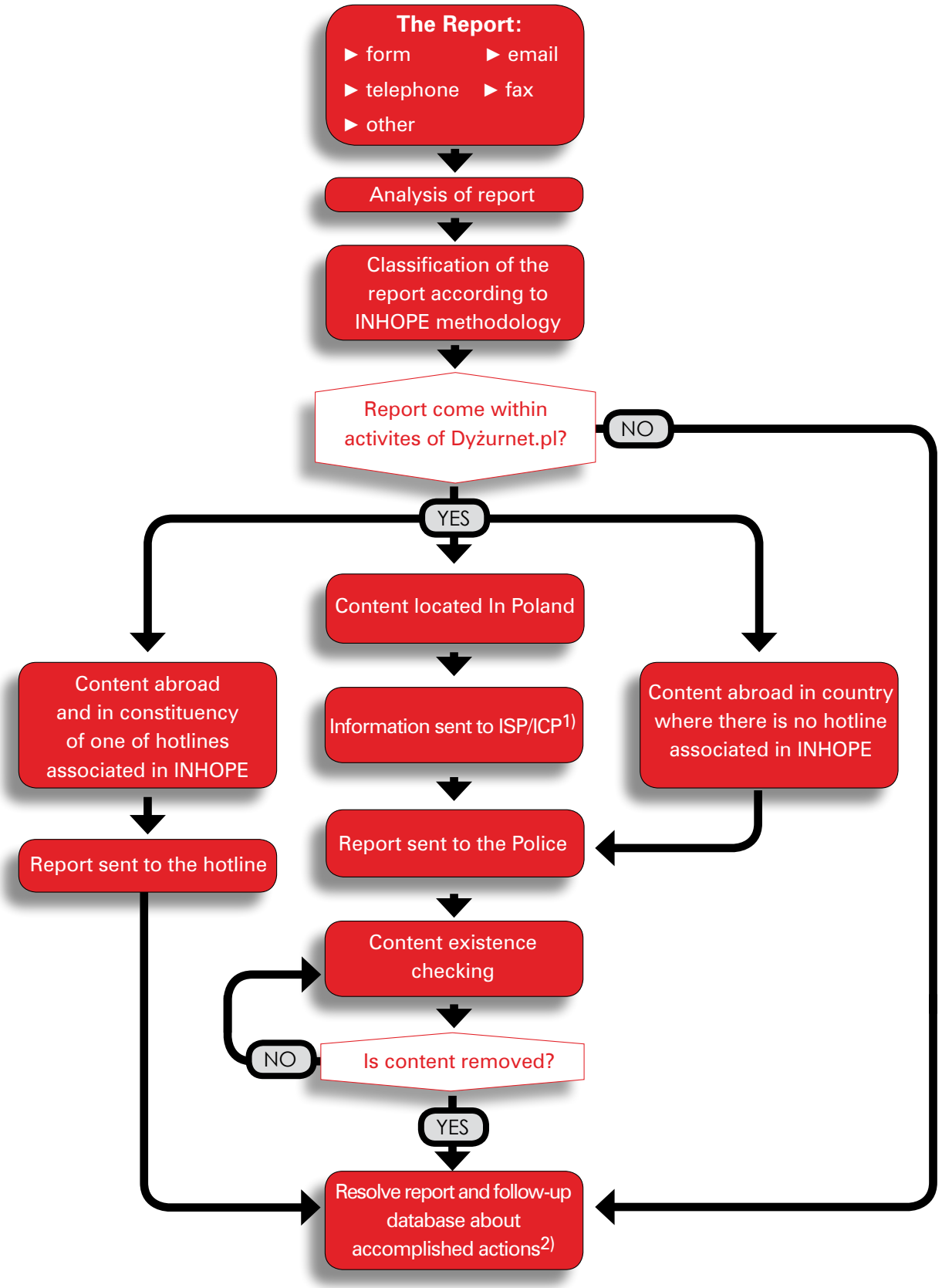
In the immediate future, Dyżurnet.pl will be working to raise Internet users' awareness of network threats and ways to respond to harmful, dangerous or illegal content. In mid-2011, a media campaign is planned to increase the recognisability of the Dyżurnet.pl team.

In order to boost the efficiency of the team's work, close cooperation is necessary with administrators of websites and portals where most content is generated by users. The team's experience shows that administrators' knowledge of their rights and duties as well as ways to report crime to law enforcement agencies is insufficient. Therefore, guidelines should be prepared for administrators with advice how to deal with abuse or violations of law.

Cooperation with universities is also needed to teach future specialists about issues related to safety on the Web.

Another initiative will be establishing the Congress of Young Internet Users and preparing teaching aids in cooperation with student governments. They can be used in preparing information about using the Internet and ways to respond to threats.

Promoting children's and young people's safety on the Internet is another important task of the team. Its immediate plans include the preparation of teaching aids for 7–9 year old primary school students.



1) Request for content removing and data preservation for law enforcement.
2) Additionally, if the reporter leaves any contact or personal information then Dyżurnet.pl gives an information on report resolving or reason of refusing.

Report illegal content:

- via e-mail at: **dyzurnet@dyzurnet.pl**
- via online form at: **www.dyzurnet.pl**
- via phone: **0-801-615-005** (local rate)