GLACY
Global Action on Cybercrime
Action globale sur la cybercriminalité

Version 9 September 2014

Good practice study

Cybercrime reporting mechanisms

Prepared under the GLACY project

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Table of content

Note:

This document has been prepared under the GLACY project on Global Action on Cybercrime by Jean-Christophe Le Toquin, SOCOGI, France.

Result 6 of GLACY refers to "Information sharing: Increased public/private and interagency information sharing in line with data protection standards" with the implementation of the following indicators:

"Objectively verifiable indicators of achievement for objectives & results / means for activities:

– Online reporting mechanism on information sharing policies of private sector entities and data protection requirements available
– Law enforcement/ISP cooperation agreements adopted in up to 10 countries
– Up to 10 countries have the necessary information to set up public reporting mechanisms"

The assumption under this activity is that private and public sector authorities are prepared to cooperate under the framework to be established. The commitment to this effect is to be sought in the course of project activities.

The study supports in particular activity 6.4: "Provide advice in the creation of public reporting mechanisms and criminal justice statistics on cybercrime".

It is also of support to two separate but related activities:

– 6.1: Creation of an online resource (platform) on private/public information sharing and related data protection requirements (planned for June to December 2014)
– 6.2: Support the creation of the legal basis for interagency (including law enforcement/CSIRT) and private/public information sharing in line with data protection standards (planned throughout the project until May 2016).

The selection of the reporting systems surveyed in this study was made based on their reputation of effectiveness, combined with their responsiveness in participating in this study. The authors would like to express their gratitude to all experts who devoted their time to share information in confidence.

1 Background and objectives of the study

1.1 About GLACY

The GLACY project (Global Action on Cybercrime) is a 36-month project running from November 2013 to October 2016. It has a global scope and is conceived as a resource to support, in a pragmatic manner, States that are prepared to implement the Budapest Convention on Cybercrime. It is funded as an action aimed at fighting organised crime under the long-term component of the European Union's Instrument for Stability. It is co-funded by the Council of Europe.

The GLACY project aims at enabling criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime. More generally it aims at developing harmonisation of legislation, training and cooperation at national and international level against cybercrime.

It is expected that by the end of the GLACY project:

- up to 70 States participate in international efforts on cybercrime using the Budapest Convention as their common framework,
- legislation and criminal justice capacities will have been enhanced to enable increased investigation, prosecutions and adjudication of cases involving cybercrime and electronic evidence,
- international police and judicial cooperation on cybercrime and electronic evidence will have increased,
- private and public sector organisations will be able to share information in line with data protection requirements,
- progress made will have been assessed and results will feed into future policies and strategies.

1.2 Objectives of the study

In line with the objectives of the GLACY project, this good-practice study focuses on cybercrime reporting mechanisms. Building on the experience of several existing reporting mechanisms around the world, it aims at providing advice to countries which consider or are in the process of setting up their own cybercrime reporting mechanisms.

While GLACY is a project funded and designed to support a limited number of countries in the Africa and Pacific region, this study has been intended to be of value to any country which looks at building capacity against cybercrime.

1.3 Scope

While fighting cybercrime is of primary responsibility of criminal justice authorities, the role of the private sector should not be underestimated given the highly technical nature of this phenomenon and the necessity to develop a fast and effective response.

Cybercriminals are substantially motivated by profit, and in particular financial profit. As for any legitimate business, they conduct cost/benefit analyses. As a result, their activities ignore legal boundaries between criminal law and civil law, and therefore fall under the remit of law enforcement agencies as well as other public authorities, mainly those in charge of protecting consumers and personal data.

It is therefore not surprising that the scope of this study does not focus solely on initiatives established and run by law enforcement agencies, but covers also other public authorities and the private sector.

The study does not pretend to provide an exhaustive view on existing reporting mechanisms, which are up and running in 2014. It has selected a series of initiatives which represent the different operating models currently in place.

Two elements of any reporting mechanism are of particular importance:

1. The initiative: whether it is initiated by the public sector (typically law enforcement or public authorities) or by the private sector (industry association or NGO).

2. Funding: whether funding comes from the public sector or from voluntary contributions of companies.

The combination of these two elements results in four types of reporting mechanisms:

1. *Public*: established, run and funded by public sector, with some level of cooperation with the private sector
2. *Public/private*: established by the private sector, not sustainable without funding from the public sector,
3. *Private/public*: established by the private sector, sustainable without funding from the public sector, but requires input from the public sector
4. *Private*: established by the private sector with some level of cooperation with the public sector.

The reporting mechanisms surveyed in this study can be categorised as follows:

Initiative	**Reporting mechanisms**
Public	Action Fraud, UK Consumer Sentinel Network (CSN), USA e-cops, Belgium Internet Signalement, France Cyber Security Mauritius
Public/private	National Cybersecurity Center (NCSC), the Netherlands Internet Crime Complaint Centre (IC3), USA INHOPE, European Union
Private/public	Signal Spam, France
Private	Anti-Phishing Working Group, USA

1.4 Overview of the study

When considering the setup of a cybercrime reporting mechanism, the first consideration concerns the types of threat to be covered. Typically, a law enforcement agency or a public authority, which considers expanding its operations from the offline world to the online environment, may see a cybercrime reporting mechanism as a new way to receive reports in an electronic format. It will then seek additional funding to set up its online reporting mechanism. This organic approach has the benefit of being straightforward, and does not require prioritisation among different threats at the country level. But the creation of a new reporting mechanism is not necessarily the decision of a single agency, and can be the result of a decision taken at a higher level, in a ministry or even at government level. For a country which does not yet have any reporting mechanism and have limited public funding, this organic approach may not be the most appropriate: at a country level, public funding may be allocated to combating threats which are considered of strategic priority nationwide. Therefore, it may be useful for a country willing to set up an online reporting mechanism to consider which type of threats should be addressed in priority. This is the purpose of Section 2.

Once the list of threats to be addressed by the cybercrime reporting centre has been defined, the next question concerns the benefits expected from the reporting mechanism: what is the rationale behind it, how should it be established and what impact it may accomplish. This is discussed in Section 3.

Section 4 of the study provides a more specific description of each reporting mechanism surveyed with a focus on their benefits and also how they contribute to information sharing locally and internationally.

The last part, Section 5, summarises the lessons learned and outlines a series of recommendations for countries intending to set up cybercrime reporting mechanisms.

2 Types of threats to be addressed by a cybercrime reporting mechanism

2.1 Definition

Cybercrime, for the purpose of this study, is understood in a broad sense and covers any unlawful activity which is investigated or regulated under administrative, civil and criminal law, and committed against or through computer system or a computer technology.

2.2 Threats and impacts

2.2.1 Threats

Cybercrime is a versatile concept, as any type of unlawful activity can involve some electronic element in its preparation or its execution.

It is well known that cybercriminals ignore borders and actually take advantage of territoriality of legislation to make their activities harder to investigate and prosecute. If the international dimension of cybercrime is, for sure, a serious challenge for governments, another difficulty within each country lies in the fact that unlawful activities ignore also the distinction between law enforcement agencies, public authorities, and national security. For instance, a spam (unsolicited email) can be a phishing attack (designed to steal data and money) sent through a compromised computer by a botnet, with this computer being also used to conduct denial of service attacks against a national critical infrastructure.

This means that while organisations, regulators, agencies are extremely careful to stay in line with their own mandate, cybercrime is constantly blurring the lines and requires cooperation and exchange of expertise and information between organisations, regulators and agencies.

In addition, the constant innovation in technology fosters mobility: employees bring their own device at work on which they store professional data and companies outsource the management of their IT and move their data to servers in the cloud hosted overseas. Internet everywhere, social media and mobile applications gradually remove the traditional distinction between the professional, the public and the private sphere. Fraudsters and cybercriminals use all these new opportunities to their profit.

Threats typically include attacks against:

- Individuals through identity theft, personal data theft, e-reputation, sexual abuse online, incitement to racial hatred
- Infrastructure through botnets and malware
- Assets through theft of money or data (confidential data or copyrighted content)
- National security through espionage or terrorism.

When a country considers establishing its first online reporting mechanism against cybercrime, it may consider giving the mandate to an existing agency or authority and let it decide how best to expand its activities to the online environment.

Another approach can be more strategic and consider the impact cybercrime has on the country, and more specifically on its people, its industry and its national security.

2.2.2 Impact on individuals

Individuals are targeted in most cases in relation to their personal data and money. Malware, spam, phishing or social engineering can be used, amongst other ways, to steal information to perform frauds, abuse people's identity or blackmail them (e.g. "sextorsion").

Therefore the impact of cybercrime ranges from the breach of privacy to physical integrity and life threat (in case of crime scenes of sexual abuse being commercialised online).

The financial impact of these threats is difficult to measure. However setting up a reporting mechanism is likely to generate impact as a large number of reports can be expected.

2.2.3 Impact on industry

Industry is targeted in relation to the valuable assets it controls (confidential and protected data, money). Botnets, malware, hacking, social engineering or intelligence gathering are used to access protected information or disrupt its activities.

The impact of cybercrime ranges from reputational damages, intellectual property infringements, direct or indirect financial losses to denial of service, disruption of the service and the production.

The financial impact on these threats is theoretically easier to measure as the authorities deal with a much smaller number of victims, which are equipped with staff able to assess the loss they suffer and engage in a dialog with the authorities.

Setting up a reporting mechanism to protect industry may therefore produce more tangible results in measuring impact of cybercrime, but it requires also a deeper understanding as well as trust between the authorities and the companies in a position to report. Reaching a sufficient level of trust requires patience and a genuine willingness on both public and private sides. As such, trust may take an unpredictable time to materialise and the cybercrime reporting mechanism may consider collecting intelligence on the threats (compromised computers, vulnerable systems, phishing attacks…) as a way to engage in a dialog with the industry.

2.2.4 Impact on national infrastructure

Last but not least, the national infrastructure (i.e. the government, law enforcement agencies, public authorities, critical infrastructure) is also a target of politically motivated offenders seeking to cause disruption.

In this case, setting up a reporting mechanism does not seem an adequate response, as the victims will only report to their hierarchy and through pre-defined channels. This being said, gathering intelligence on online threats should be considered, especially as infrastructure like botnets are versatile and used against individuals, companies and national infrastructure.

Cybercriminals act on a global scale. Therefore, any action to address cybercrime should be considered as one element of a bigger picture. A better collaboration between public and private sectors and a closer involvement of individuals will lead to a better understanding of cybercrime mechanisms and scenarios, and provide key information to adapt strategies to fight against cybercrime.

3 Benefits expected from cybercrime reporting mechanisms

Based on the interviews and information collected through this study, this section outlines the rationale behind the setup of reporting mechanisms and the benefits they bring.

As it is outlined in the following sections, the initiative for launching reporting mechanisms originates either from the public sector, the private sector, or the two combined. As a result, the funding of these mechanisms differs from one initiative to another. This funding plays a critical role on the activity of these reporting mechanisms, mainly on how it uses the data it collects and the intelligence it creates.

As funding is a critical element in the decision of setting a new reporting mechanism, the study analyses the different initiatives according to their funding model, i.e. public, public-private, private-public and private.

3.1 Objectives of reporting mechanisms

Reporting mechanisms surveyed in the course of this study generally indicate that they have been created to contribute to a safe, open and stable information society, and to address what was perceived as a continuously increase in cybercrime.

The objectives of reporting mechanisms are both strategic and operational.

Strategic objectives:

- get a centralised reporting tool, and coordinate actions across law enforcement agencies or public authorities in a given country,
- demonstrate that regulation which applies offline also applies online,
- raise awareness towards consumer and businesses and provide educational tools,
- coordinate actions between the public and the private sectors.

Operational objectives:

- identify cybercrimes at country level and develop enforcement capacity,
- produce statistics on trends and threats,
- develop intelligence from these statistics and better target law enforcement actions,

– share information with other or international law enforcement authorities through publications, reports, symposiums…

Establishing a reporting mechanism as part of an overall strategy in the fight against cybercrime is a common purpose. Some reporting mechanisms deal with a large series of crimes (e.g. Action Fraud in the UK, Internet Signalement in France, IC3 in the USA), while some others are dedicated to specific threats, as this is the case in the USA with APWG (phishing) and in France with Signal Spam (primarily spam but also phishing and botnets).

In most cases, reporting mechanisms are available to citizens and victims of cybercrime so they can easily report their damage to relevant authorities. The collected data are hence centralised by the reporting mechanism before being processed by law enforcement agencies and authorities for them to track trends and take appropriate actions.

3.1.1 Reporting mechanisms managed by the public sector

Public reporting mechanisms surveyed in this section have been initiated by the public sector, with a various degree of support from the private sector.

3.1.1.1 Initiated by law enforcement

In Belgium, **e-Cops**[1] was initially set up to fight against child pornography on the Internet following a serious paedophile case in 1996. Created as a Central Judicial Reporting, e-Cops also collects input from Child Focus, a non-profit foundation for missing and sexually exploited children. Overtime its scope was extended. Nowadays, e-Cops provides a single point of contact for internet-related criminal activities including child pornography, internet fraud, cybercrime or racism with the objective to shut down criminal infrastructure (websites).

In France, **Internet Signalement**[2] was initiated in 2009 by the government to provide internet users with a reporting mechanism to report violent content. In addition, the government wanted to reassure citizens that internet was not an unregulated area. Funded by the Ministry of Interior, it acts as a single point of contacts for all cybercrime reports and partners with many actors from the private sectors, including webhosting companies, networking platforms and associations. Reports are handled by law enforcement officers, as this is considered as providing a better and faster law enforcement response, especially in most serious cases.

In Europe, building on growing number of national reporting mechanisms, the European Commission launched a **European Cybercrime Centre (EC3)**[3] at Europol in 2013 to support European Member States and the Union’s institutions in building faster operational and analytical capacity for investigations and cooperation with international partners. EC3 aims to become the focal point in the EU’s fight against cybercrime, contributing to faster reactions in the event of online crimes.

3.1.1.2 Initiated by public authorities

In the United States, the Federal Trade Commission (FTC US) started in 1997 its reporting mechanism after determining that consumer complaint collection would be helpful for law enforcement. The Federal Trade Commission (FTC US) is an independent agency of the

[1] https://www.ecops.be/

[2] https://www.internet-signalement.gouv.fr/

3 https://www.europol.europa.eu/ec3

United States government. It provides an investigative cyber tool and complaint database to law enforcement with access to identity theft, internet, telemarketing (including do-not-call), and other consumer related complaints. Consumer complaint information received by the FTC, including spam, is made available to thousands of civil and criminal law enforcement personnel in the United States and abroad through a secure Internet website called the **Consumer Sentinel Network (CSN)[4]**. By collecting, maintaining, and analysing data, the FTC is better able to target law enforcement action, provide consumer and business education to protect the public, and identify trends in consumer fraud and law violations.

In the United Kingdom, **Action Fraud UK[5]** was set up in 2010 to capture all fraud and internet crime intelligence in one place. Action Fraud is funded by through a grant provided by Central Government (Cabinet Office, Home Office) and the City of London. It provides a centralised reporting function for crime and information with respect to fraud and financially motivated internet crime.

The data collected by Action Fraud are analysed by the National Fraud Intelligence Bureau, which has a national view and can spot connections between seemingly unrelated crimes from around the country, hence providing victims with a greater level of protection against organised criminal groups.

The **Mauritian National Computer Security Incident Response Team (CERT-MU)[6]** was launched in 2008 as the main national body for coordination of information security incidents at national level. It is a division of the National Computer Board. The mission of CERT-MU is to provide information and assistance to its constituents in implementing proactive measures to reduce the risks of information security incidents as well as responding to such incidents as and when they occur. CERT-MU's main objectives are to handle security incidents and monitor security problems occurring within public and private sectors; provide guidance to providers of critical information infrastructure to adopt best practices in information security; and warn and educate systems administrators and users about latest information security threats and suggest countermeasures by means of information dissemination.

3.1.2 Reporting mechanisms managed by public–private cooperation

The reporting mechanisms listed below are public or private entities, but they have in common that they would not have been set up without the leadership and funding from the public sector.

In the Netherlands, the **National Cybersecurity Center (NCSC)[7]** is an extension of the Dutch CERT's mission. The NCSC considers the importance of exchanging information and collaborating nationally and internationally in order to improve digital resilience in the country, in the aftermath of the DigiNotar incident[8]. The NCSC monitors cybercriminals' activities and coordinate actions of law enforcement agencies. Collaboration with private sector is therefore understood as helping in achieving a more effective response to security incidents. While strictly a public entity, NCSC has made cooperation with the private sector a core component of its activity.

As a result, the CSIRT (Computer Security Incident Response Team) for government organisations and critical infrastructure has been established within the NCSC. It responds to

[4] http://www.ftc.gov/enforcement/consumer-sentinel-network

[5] http://www.actionfraud.police.uk/

[6] http://cert-mu.gov.mu/English/Pages/default.aspx

[7] https://www.ncsc.nl/

[8] DigiNotar incident : a serious security breach into DigiNotar, a Dutch certificate authority, which resulted in the fraudulent issuing of certificates

IT-related incidents and offer products (e.g. tools) and services (e.g. alerts and advices) that contribute to the prevention, detection, reduction and solution of cyber-incidents. Furthermore, it raises awareness.

The NCSC indicated that there were currently over 250 CIRTs in more than 70 countries and that every year, more CIRTs were being established. The cooperation between CIRTs is worldwide, informal and based on trust. However, the Dutch NCSC, where the CSIRT is embedded, is different from other response teams as it is a public-private partnership that focuses on national security. It has therefore an operational coordinating role in large incidents or crises that might harm national security, including cybercrimes with a national impact. The NCSC works closely with law enforcement authorities, judicial authorities, other CSIRTs, public bodies and private organisations on both national and international levels.

The NCSC is of the opinion that cooperation in fighting cybercrime is key. CSIRTs and law enforcement authorities both have their own roles and powers, but they share the goal of making the digital domain a safer place. By joining forces they can both contribute to that safety more effectively and more efficiently than they could ever have done when acting alone.

In the United States, the **Internet Crime Complaint Centre (IC3 US)**[9] was established in 2000 as a partnership between the Federal Bureau of Investigation (FBI) and a non-profit corporation, the National White Collar Crime Centre (NW3C). Initially built as a call center, the IC3 dropped the call-in function in 2003, accepting only online complaints from that time on.

The IC3 establishes a mechanism for victims of Internet crime to report their victimisation to law enforcement of relevant jurisdiction. Criminal complaints are then transferred to federal, state, local, or international law enforcement and/or regulatory agencies for any appropriate investigation.

Reports to IC3 are therefore used for a double purpose: to strengthen enforcement capacity by providing actual complaints, and to develop trends and statistics on Internet crime.

INHOPE[10] is an International Association of Internet Hotlines with 49 hotlines from 43 countries worldwide. By sharing knowledge, information and best practice, INHOPE and its members are working to tackle the global problem of illegal content online. Member hotlines include different types of organisations (NGOs, Governments, Private sector), that cooperate with Law Enforcement to essentially fight against child sexual abuse online. It was established in 1999 under the initiative of the European Union, which provided the public funding necessary to this project.

INHOPE hotlines provide reporting mechanism tools to public to report illegal content online. The hotlines then access the reports according to their national legislation, trace the apparent location of the content and, in case it is hosted in their own country, the hotlines pass the report on to either their national law enforcement agency for further investigation or Internet service providers for take-down or another INHOPE hotline.

[9] http://www.ic3.gov/

[10] http://inhope.org/

3.1.3 Reporting mechanism managed by private-public cooperation

In France, **Signal Spam**[11] has been launched in 2007 as a non-profit organisation which aims at combating spam by enabling internet users to report emails they consider as unsolicited or abusive. Public authorities (data protection, law enforcement agencies…) and the various stakeholders in the email ecosystem (senders of email marketing, providers of mail boxes as well as security vendors) are part of Signal Spam. Initially, it was specifically designed to help the French data protection authority to build its capacity in regulating and protecting consumers from SPAM.

The reports are collected and redistributed to Signal Spam's members which are best positioned to take the required action: it can be the data protection authority, law enforcement agencies, or the senders in case of legitimate email marketing. All complaints are kept as evidence for further investigations by authorities.

Signal Spam also provides educational tools and share useful data with relevant Internet players in the e-marketing business. It also contributes to empowering best practices through a mandatory Code of Ethics for its members.

Signal Spam started as a public-private initiative, under the leadership and funding from the public sector, and evolved in 2010 to a private-public model. It operates today with funding from the private sector only, but its management is shared equally by experts from public and private sector.

3.1.4 Reporting mechanisms managed by the private sector

The **Anti-Phishing Working Group (APWG)**[12] was established in the United States in 2003 as a clearinghouse for victimized institutions subject to phishing attacks. The phishing websites are reported to browser developers and antivirus companies to ensure these websites are blocked at the level of their browser or security product. Reports to APWG help understand trends and create statistics, but also enable first instance notifications: APWG's notifications help to clean corrupted nodes and to act for rapid suspension of criminally established domain names.

The APWG is a worldwide coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors. APWG's membership of more than 2.000 institutions worldwide is global and advises national governments, global governance bodies like ICANN, hemispheric and global trade groups, and multilateral treaty organisations such as the European Commission, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organisation for Security and Cooperation in Europe and the Organisation of American States.

3.2 Impact of reporting mechanisms on regulation and business practices

When asked if they have an impact on the regulatory framework in their own country, surveyed reporting mechanisms have the perception that they do have a direct impact on both business practices and the work of law enforcement agencies, more than on the regulation itself.

[11] https://www.signal-spam.fr/

[12] http://www.apwg.org/

With regard to law enforcement agencies, the general perception is that they help improving processes for a more efficient coordination between agencies. When actions used to be conducted several times in different agencies for the same offense, a global coordination enabled by the reporting mechanism led to a faster and better response to cybercrime.

Regarding business practices, several countries noticed an increase in collaboration between law enforcement agencies, public authorities, industry associations and businesses. This is the case for Signal Spam (France) that created an ecosystem between email providers, regulators, email marketers and email senders. In addition, its code of ethics defines rules which have resulted in exclusion of the infringing companies.

Different reporting mechanisms can co-exist at country level. Their missions' statements can be different with regard to the type of offense (e.g.: child sexual abuse, bullying, spam, phishing and scamming, etc.). However, these reporting mechanisms all aim at improving cooperation between law enforcement, public authorities and the private sector. They collect complaints from consumers or businesses and refer them to either the competent authority or the competent reporting mechanism. IC3 in the United States, for instance, referred in 2010 121,710 complaints to law enforcement and 2,597 child pornography complaints to the National Center for Missing and Exploited Children.

Some reporting mechanisms contribute to a centralised database. This is the case in the United States, where the Consumer Sentinel Network acts as a centralised tool that is made available to all registered law enforcement authorities. Data are gathered from consumers and other external contributors, including other reporting mechanisms.

3.3 Impact of reports on criminal cases

Organisations that run a reporting mechanism collect numerous notifications of crimes and frauds. These data often constitute an important source to understand the trends of cybercrimes and trace criminals. Many reporting mechanisms work in close cooperation with judicial and law enforcement authorities. The objective of these mechanisms usually lies mainly in the need for a centralised point of contact as a tool for law enforcement and judicial authorities. According to their scope, platforms transfer the information they received to the identified competent authorities, when applicable. As such, a first analysis of the reports received at the reporting mechanism is required to understand the scope and the relevance of the information received before it can be transmitted to the competent services.

In the United States, data received by reporting mechanism feed into a database centralised by the FTC's **Consumer Sentinel Network** and available to all police forces of the country.

In the Netherlands, **the NCSC** stressed that CSIRTs does, however, not have any investigative powers such as law enforcement authorities. They cannot take any coercive measures such as ordering organisations to produce or freeze data, or to take down a website. In some countries, the law prevents them even from sharing certain information with law enforcement authorities. Nevertheless, the NCSC believes that CSIRTs can be of great value in fighting cybercrime by taking action where law enforcement authorities encounter difficulties. Indeed, CSIRTs excel in trust-based informal cooperation. In addition, CSIRTs can contribute to creating a mutual understanding of the use of techniques and tools that are used by criminals, by defining the mean threats of cybercriminal and by raising awareness together.

In France, **Internet Signalement** analyses the information they receive through a first investigation before it is effectively transmitted to police forces or judicial instances (governmental decrees identifies the different authorities according to the type of content).

e-Cops was initially created as a central judicial reporting platform for Belgium, handling notifications related to child sexual abuse material and economic crimes. However, its team doesn't have the central research rights (with the exception of phishing websites hosted in Belgium and swindling cases where money is transferred to Belgium) and redirects valid notifications, after localisation, to either the Human Trafficking Department of the police for all child sexual abuse matters or to local police partners. Economic crimes are referred to Federal Public Service Economy who benefits from research rights and therefore can handle these reports as complaints.

Action Fraud UK provides a central point of contact about fraud and financially motivated internet crime. The service is run by the City of London Police working alongside the National Fraud Intelligence Bureau (NFIB) who is responsible for assessment of the reports and to ensure that fraud reports reach the right place. Like in France and in Belgium, the NFIB does not investigate crimes, but does make sufficient enquiries to determine which agency should have primacy for the matter. Generally this will involve allocation of crimes to a territorial police service; this is primarily on the basis of the offender's location. Where the circumstances merit, reports of crime are also passed to national bodies such as the Serious Fraud Office, National Lead Force for Economic Crime (City of London Police), National Crime Agency which incorporates the National Cyber Crime Unit and foreign jurisdictions via Interpol. The service acts in compliance with the Data Protection Act and in accordance with the purpose of the police service. As such, information is shared with a wide variety of public and private bodies on the basis that it is for the prevention of crime and disorder and that it can be demonstrated that there is a policing purpose. In addition, Action Fraud contributes to national crime statistics by providing details of crime recorded to the Home Office.

If these reporting platforms work closely with law enforcement and judicial authorities, they generally do not have any thorough investigative power. Their investigative work is hence limited to the determination of the validity, the scope and the localisation of the notifications before they transmit them further to the relevant local authorities. These authorities then assess what follow-up it should give. In France, **Internet Signalement** is considered as an important stakeholder in the French Internet sector with a real-time overview of the last internet and cybercrime trends. **Internet Signalement** is often consulted within legislative working groups (including governmental working groups). Nonetheless, they do not take part in discussions regarding penal actions and indicated they were generally not kept informed about the actions undertaken by police forces following information they transmitted.

3.4 Awareness

Surveyed reporting mechanisms insisted on the importance of creating awareness among citizens and businesses about their existence and their purpose. Raising awareness and educating people about the reporting mechanism is key to ensure the success of the organisation. In addition, it shows that the public sector is acting, be it alone or in cooperation with the private sector, to counter cybercrime and provide support to consumers and businesses.

Communication and awareness actions should preferably be carried out during the introduction phase of the reporting mechanism and should continue moving forward afterwards.

During the launch phase, communication can be done through an awareness campaign involving local media (press articles, TV spots, posters…) in particular. Other interesting tools that were used by some countries include:

- SMS campaigning
- Leaflets attached to phone bills
- Social media campaigning.

Afterwards, awareness raising activities should continue to ensure the efficiency of the reporting mechanism in the long run. Existing mechanisms are using different means to promote their services:

- Regular publications of regular reports
- Communication through social media
- Partnership with internet services providers (website referencing)
- Regular reports to the press
- Publication of periodic public service announcements
- Attendance of national and international conferences and meetings on cybercrime.

In the United Kingdom, individuals who call territorial policing services are directed to **Action Fraud** when appropriate. The reporting mechanism is present on the web and communicates with the population through social media.

According to **Internet Signalement** in France, raising awareness about the reporting mechanism contributes to its success. An official communication campaign was performed in 2009. Internet Signalement has since been publishing regular press releases. In addition, it develops partnership with many internet players (private companies and associations) which ensure a better referencing of the website.

The Belgium reporting mechanism **e-Cops** is promoted with a link on the homepage of the different Belgian Internet Service Providers, but also the on different e-commerce websites, as well as other sites.

3.5 Establishment and operational costs

As one may expect, establishment and operating costs vary widely among reporting mechanisms, depending on:

- the scope of the reporting mechanism (specialised on specific threats as opposed to reporting mechanisms which accept all cybercrime reports)
- the method to collect the reports (manual processing as opposed to automated processes)
- the size of the population of the country.

Taking into account that the surveyed reporting mechanisms are different in sizes, scopes and missions, this report can only outline some trends and estimations. The calculation of cost covers hardware for the website, the implementation and maintenance of a database but also how technically law enforcement agencies are connected to the reporting tool to retrieve and process information.

Most reporting mechanisms operate solely or primarily with public funding. However, **Signal Spam** in France and **APWG** in the United States are private initiatives that are entirely funded by the industry. Running as not-for-profit entities, they justify the contributions and membership fees through the valuable information they collect and share with the paying participants and with the broader community.

3.5.1 Overview of complaints handled by reporting mechanisms according to scope and population size

Surveyed reporting mechanisms vary greatly among them in terms of size and volume of reports processed, as shown in the following chart:

Territory	Population size	Scope of the mechanism	Public funding	Public-Private mechanisms	Private mechanisms
U.K.	Ca. 63 millions	All fraud	Action Fraud: 229,018 frauds handled by police and Action Fraud altogether from March 2012 to March 2013		
Belgium	Ca. 11 millions	Cybercrime only	e-Cops : 24,220 complaints received in 2011		
France	Ca. 66 millions	Internet Signalement: cybercrime Signal Spam: spams, phishing	Internet Signalement : 123,987 complaints received in 2013		Signal Spam: 2,454,369 complaints received in 2012
U.S.	Ca. 314 millions	FTC: all fraud IC3 US: cybercrime	FTC with the Consumer Sentinel: 2,101,780 complaints received in 2013	IC3: 303,809 complaints received in 2010	

3.5.2 Cost

Set up costs and operational costs are complex to calculate and often confidential. However, an approximate range can be provided, starting from EUR 200,000 based upon information received from surveyed reporting mechanisms.

- Establishment and maintenance of the reporting mechanism: starting from EUR 200,000
  - Reporting mechanisms with a limited scope: Signal Spam in France estimated their annual costs at around EUR 200,000 and APWG in the United States at more than EUR 400,000.
  - Reporting mechanism with a larger scope covering all frauds: for the U.S. Federal Trade Commission’s Consumer Sentinel, it was necessary to secure an entire building and purchase all the IT equipment amounting several millions Euros.

- Dedicated staff: from 2 to more than 30 persons
  - A few staff members can be sufficient for specialised initiatives which receive reports through automated systems (e.g.Signal Spam in France that deals with spam and phishing). Larger initiatives (FTC, IC3 US, Action Fraud UK, Internet Signalement France) require an initial staff of minimum 10 members.

- Specialised staff may be required
  - In cases where complaints are analysed by general Police staff (not only specialised in cybercrime), basis knowledge of internet and computer science is required. However, police forces should be trained to differentiate the type of content and transfer the reports to the relevant competent authorities for further investigation.
  - In cases where complaints are analysed by specialized units, staff of Internet and cybercrime specialists is a requirement.

- ICT infrastructure
  - Costs for ICT infrastructure include: website development and maintenance, phones and phone lines, internet connectivity, computers, printers, photocopiers, fax, Report Management System, security (firewalls, anti-virus systems, encrypted connections to remain anonymous when viewing suspect websites).
  - Some of the costs or infrastructure equipment may be supported or provided by local industry partners (internet industry players or private donors). It is therefore important to approach them right from the start. In addition, in many countries, it is possible to apply for government funding

3.5.3 Common requirements

Based on the contributions provided by the surveyed reporting mechanisms, a list of common requirements can be summarised as follows:

- Political/top management support: support from government or from top management is a primary requirement for any reporting mechanism, both to ensure the initiative is perceived as relevant at all levels, and to secure the budget and the staff required for its launch and its operation.

- Experienced staff:
  - ICT project manager to set up the ICT environment
  - police manager that liaise with senior management in order to solve any occurring problems during the establishment and the operational phase of the reporting mechanisms
  - digital investigators to help define the working structure of the reporting mechanism
  - digital investigators to handle complaints assisted by administrative employees that can do a first selection of the complaints.

- Support of the judiciary, as police cannot always decide which cases should be prosecuted.

3.5.4 Other criteria to be considered

- Participation of internet users to help define what individuals should expect from the reporting mechanism, and why they should report.

- Capacity to measure return on investment: privately funded initiatives have a greater flexibility in terms of developing their pricing strategy and develop their capacity, but they have to be able to articulate what is the return on investment for the paying members.

3.6 Seeking assistance and promoting best practices

The surveyed reporting mechanisms have not set up programs to support the development of similar initiatives in other countries, with the notable exception of INHOPE.

In 2010, INHOPE established the INHOPE Foundation to support start up activities of new hotlines outside of the European Union, mainly in countries where Child Sexual Abuse Material is being facilitated, produced or distributed. The foundation focuses its efforts in countries around the world where there is an identified need but limited funding, awareness or support for an online reporting mechanism to help identify, report, remove and/or investigate child sexual abuse material found on the Internet (2014-2015: focusing on the development of partnerships in Latin America, South East Asia and Africa).

The INHOPE Foundation identifies and enters into partnerships with national organisations (mainly NGOs, private companies) in priority countries that already operate a start-up hotline or would like to establish a national hotline. Foundation 'participants' are organisations meeting the Foundation's criteria for development support. The Foundation can provide initial 'start-up' support and training on best practices to the staff of qualified organisations within specifically targeted countries to develop a hotline that addresses the issue of child sexual victimisation via the internet. The Foundation also provides guided oversight during the initial start-up phase, including instruction on best practices for staffing requirements, equipment needs, location security, data safeguarding, and internal and external policy development. With regard to funding, however, INHOPE can only provide a limited financial support and does therefore not respond to requests for funding.

In 2013, INHOPE published, together with the GSMA's Mobile Alliance Against Child Sexual Abuse Content, a Guide To Establishing And Managing A Hotline Organisation[13]. As outlined in the document, "the key starting point [...] to found a hotline will be to get to grips with the particulars of their national context – developing a thorough understanding of the local legislation, the cultural expectations, the likely scale of the problem, and so on." The guide defines a series of question that can be asked before starting. These questions are focused on activities dealing with child sexual abuse material but could also be applied to any other type of illegal activity a hotline could cover:

- How clearly are the legal parameters of child sexual abuse images defined? – Is the existing legislation adequate?
- What are the legal implications of looking at an image of online child sexual abuse content?
- Is a cached image, automatically created when the image is viewed, an offence (i.e. does that constitute 'creating' an image)?
- What exemptions would a hotline / hotline employee need to be able to view potentially illegal content to do their job?
- Are there issues around data storage (e.g. relating to the URLs, files, reporters ID / IP address)?
- Are there issues around maintaining reporter anonymity?
- What are the hotline's legal liabilities? What might happen if the hotline got sued?
- Does the hotline need to be a registered entity / charity or equivalent? What legal requirements are there in terms of ownership, governance, transparency and accountability? – Is there a requirement for a hotline to be managed under the auspices of a national authority (e.g. film classification board, a media and communications authority etc)?

[13] Hotlines: Responding to reports of illegal content online, October 2013, http://inhope.org/tns/news-and-events/news/13-10-14/Partnership_in_action_new_INHOPE_GSMA_resource_guide_the_ABC_on_how_to_set_up_and_manage_a_hotline_released.aspx

In addition, INHOPE and GSMA recommend getting the support and engagement of external stakeholders, including:

- The government: government will provide credibility, may lead to government funding, enable law enforcement to give the required levels of assistance and can re-define legislations if necessary.
- Law enforcement authorities: a strong working relationship with law enforcement will simplify and strengthen the processes relating to the foundation and running of the hotline.
- The internet industry: getting national internet industry players understand and share the hotline’s objectives will facilitate the removal of illegal content or the blocking of URLs.
- Child welfare agencies (in the case of CSAM): they will be able to help the hotline gain traction with key stakeholders, from government to the general public, as well as give valuable insights into the status of child sexual abuse content initiatives during the hotline development process.
- Other hotlines or INHOPE.

4 Overview of reporting mechanisms surveyed

This chapter section an overview on the reporting mechanisms which have been surveyed:

- Belgium: eCops
- EU: European Cybercrime Centre (EC3), INHOPE
- France: Internet Signalement, Signal Spam
- The Netherlands: Nationaal Cyber Security Centrum (NCSC)
- UK: Action Fraud
- US: Anti-Phishing Working Group (APWG), Internet Crime Complaint Center (IC3), Federal Trade Commission (FTC)
- Mauritius: CERT-MU

4.1 Belgium: e-Cops

<table>
<tr><th colspan="2">Website</th></tr>
<tr><td colspan="2">https://www.ecops.be</td></tr>
<tr><th colspan="2">Scope</th></tr>
<tr><td colspan="2">• Report Internet fraud and cybercrime (although the contact points was not really meant for complaints at first)
• Close child pornography websites (focus on those in Belgium)
• inform other countries of "illegal websites" on their territories
• awareness raising towards internet users about the dangers on the internet and possible reactions (informative documents on different topics)</td></tr>
<tr><th colspan="2">Reporting mode</th></tr>
<tr><td colspan="2">Online form at www.ecops.be</td></tr>
<tr><th colspan="2">Information sharing</th></tr>
<tr><td>Domestic level</td><td>Some basic statistics are shared with Child focus (Foundation for Missing and Sexually Exploited Children in Belgium)</td></tr>
<tr><td>International level</td><td>When child pornography websites are found in the jurisdiction of another country, the handling police agents send a police information report about the police findings (especially the URL, domain name, type of illegal material) to the Interpol NCB of the concerned country.
No information shared with similar entities in other countries</td></tr>
<tr><td>Information value
Statistical
Operational
Strategic</td><td>• Analysing trends and new phenomena
• Closing fraud websites (different websites – especially these in Belgium were closed thanks to reports to eCops.</td></tr>
<tr><td>Publicly available statistics</td><td>Annual reports of the economic and financial crime directorate since the creation of e-cops.
2007 (p. 100); 2008 (p. 94); 2009 (p. 95); 2010 (p.26), 2011 (p.32)</td></tr>
</table>

4.2 EU: European Cybercrime Center (EC3)

Website	
https://www.europol.europa.eu/ec3	
Scope	
• Online fraud • Child sexual abuse • Other forms of cybercrime	
Reporting mode	
No direct reporting. Links to national reporting mechanisms (as to warrantee a follow-up by national police).	
Information sharing	
Domestic level	EC3 is not a reporting mechanism. It is a reporting platform for Europol members to exchange best practices and coordinate actions.
International level	With Europol members for coordinated actions
Information value *Statistical* *Operational* *Strategic*	Data analyses to understand how cybercriminals, child sexual offenders and fraudsters think and operate. What they learn not only helps law enforcement target its operations more effectively: it also informs changes in policy and legislation and, most important of all, is the basis for our advice to citizens and businesses on how to protect themselves from online threats.
Publicly available statistics	No

4.3 EU: INHOPE

Website	
www.inhope.org	
Scope	
Criminally illegal content and activity with a focus on Child Sexual Abuse Material. INHOPE members may additionally deal with other types of content according to their national legislations.	
Reporting mode	
Internet Link to national hotlines	
Information sharing	
Domestic level	Exchange of information between INHOPE members and with national law enforcement authorities
International level	Exchange reports between hotlines internationally
Information value *Statistical* *Operational* *Strategic*	• Data analysis for statistics: Trend Analysis Update and statistics at INHOPE'S and members' level • Member hotlines share information with relevant law enforcement authorities in their countries for further actions
Publicly available statistics	Basic statistics are published on INHOPE'S website. Details statistics per country are to be found on member hotlines' websites.

4.4 France: Internet Signalement

Website	
www.internet-signalement.gouv.fr	
Scope	
All types of offense if perpetrated on the Internet	
Reporting mode	
• Website complaint forms • Dedicated protected access on the website for professionals	
Information sharing	
Domestic level	Data is shared with local law enforcement agencies
International level	• Some data related to minors is shared with EUROPOL • The INTERPOL network is used to notify illegal data hosting in other countries • Special relationship has been established with French speaking countries (Canada, Switzerland, Belgium)
Information value *Statistical* *Operational* *Strategic*	Data analysis helps to : • Identify and analyse new criminal trends • Provide efficient public and professional awareness and alerting • Establish the typology of illegal content on the internet • Perform preventive measures with several partners
Publicly available statistics	Trends are published without specific information

4.5 France: Signal Spam

Website	
https://www.signal-spam.fr	
Scope	
• Spam • Spambot • Phishing • Scam • Abusive e-mail marketing • Grey e-mail marketing	
Reporting mode	
• Internet-based complaint forms • Email client plugins	
Information sharing	
Domestic level	A lot of data is shared with local companies and entities
International level	Signal Spam shares feed with similar entities or lawfully acknowledged agencies in other countries.
Information value *Statistical* *Operational* *Strategic*	Signal Spam collects full spam reports from end users, aggregated statistics from ISP and provide strategic data to public agencies.
Publicly available statistics	Quarterly reports: Octobre-Novembre 2013 Annual report: 2012
Statistics available on request	Signal Spam can provide statistics and detailed information at a country level, upon request.

4.6 The Netherlands: Nationaal Cyber Security Centrum (NCSC)

Website	
https://www.ncsc.nl	
Scope	
Receive, review, and respond to network security incidents (such as software vulnerabilities, virus outbreaks and specific attacks.	
Reporting mode	
The NCSC has a 24/7 watch team that scans the internet for digital threats and vulnerabilities in software and operating systems.	
Information sharing	
Domestic level	TARANIS system: advisory reports, End-of-Week e-mails, mails to an internal mailing list, alert e-mails and SMS messages to inform the Dutch general public. BEITA system: honeypots with a network of sensors installed at government organisations, offers an insight into threats and the status of the network traffic to government bodies.
International level	Cooperation within the CSIRT-community worldwide
Information value *Statistical* *Operational* *Strategic*	• The NCSC advises the national crisis structure • The NCSC works closely with LEAs, judicial authorities, other CSIRTs, public bodies and private organisations on both a national and international level
Publicly available statistics	Fact-sheets and whitepapers publicly available on NCSC’s website

4.7 UK: Action Fraud

Website
http://www.actionfraud.police.uk
Scope
• Financial fraud and online fraud • Theft of a vehicle • Suspicious online behaviour with or towards a child • Online hate or bullying crime, material or messages • Counterfeit medicine or medical devices available to purchase online • Business or personal tax fraud or a related HMRC (Her Majesty's Revenue and Customs) matter • Benefit fraud • Immigration fraud
Reporting mode

The two primary reporting channels are:

- Telephone
- Website

Within the web channel:

- a general tool is provided for members of the public and small medium enterprises (SME's)
- an abridged tool (the Business Reporting Tool) that assumes a greater level of knowledge about fraud/cyber dependent crime is also provided to public (government) and private organisations
- where the crime involves an offender present or it is inferred that they are local to the victim there is an option for the victim to contact their local police, this is known as a 'call for service'

Information sharing	
Domestic level	• Statistics and detailed information are shared with Police and anti-fraud agencies within the country • Information is shared with a wide variety of public and private bodies on the basis that it is for the prevention of crime (under the Data Protection Act) • Where there is a regular need to share information and/or collaborate with an organisation, the service will seek to establish an Information Sharing Agreement
International level	• The service actively shares intelligence with foreign jurisdictions via the recognised pathways (National Crime Agency to Interpol) • The service participates in various cross border initiatives such as the International Mass Marketing Fraud Working Group
Information value *Statistical* *Operational* *Strategic*	• The NFIB leverages data collected via Action Fraud to provide a variety of analytical intelligence products that provide strategic and tactical direction • The NFIB also learns from criminals through the use of prison debriefs and formats that learning into documents that it shares with industry, in order to reduce risk and eliminate systemic weaknesses within systems • The NFIB also triages reports of crime made via Action Fraud with a view to passing them to an investigative agency. Where the circumstances merit, reports of crime are also passed to national bodies such as the Serious Fraud Office, National Lead Force for Economic Crime (City of London Police), National Crime Agency which incorporates the National Cyber Crime Unit and foreign jurisdictions via Interpol
Publicly available statistics	The service provides details of crimes recorded to the Home Office, these are subject to the scrutiny of the Office of National Statistics

4.8 USA: Anti Phishing Working Group (APWG)

<table>
<tr><th colspan="2">Website</th></tr>
<tr><td colspan="2">www.apwg.org</td></tr>
<tr><th colspan="2">Scope</th></tr>
<tr><td colspan="2">• Phishing
• All forms from BOTNET node infection to crimeware dropping to phishing
• Botnet reporting only – though with deep characterization of mode of corruption detected

Consists in 3 main systems :
• APWG URL Block List (UBL)
• Bot-Infected Systems Alerting and Notification System (BISANS)
• APWG Malicious Domain Suspension (AMDoS)</td></tr>
<tr><th colspan="2">Reporting mode</th></tr>
<tr><td colspan="2">• Forward the phishing email to reportphishing@apwg.org
• Web forms to fill in for the general public
• Business operations personnel bulk upload to the UBL database using HTTPS services</td></tr>
<tr><th colspan="2">Information sharing</th></tr>
<tr><td>Domestic level</td><td>• UBL : All data is shared automatically and routinely on a 24/7 basis with member companies, NGOs, national CERTs and TLD Registries
• BISANS : All data is shared automatically and routinely on a 24/7 basis with member companies, NGOs, national CERTs and ISPs and other Internet infrastructure providers
• AMDoS : Data between Accredited Intervener (who submits the request) is shared with the Registry</td></tr>
<tr><td>International level</td><td>-</td></tr>
<tr><td>Information value
<i>Statistical</i>
<i>Operational</i>
<i>Strategic</i></td><td>They all produces information valuable for statistical, operational and strategic purposes</td></tr>
<tr><td>Publicly available statistics</td><td>Public statistical reports Q3 2013</td></tr>
</table>

4.9 USA: Consumer Sentinel Network

Website	
http://www.ftc.gov/enforcement/consumer-sentinel-network	
Scope	
• Consumer complaints about cybercrime • Fraudulent, deceptive, and unfair practices in the marketplace: including identity theft, telemarketing fraud, Internet fraud, and consumer credit issues.	
Reporting mode	
Call centre services and Internet-based complaint forms	
Information sharing	
Domestic level	Registered law enforcement personnel can access the data base
International level	No
Information value *Statistical* *Operational* *Strategic*	Consumer complaint information received by the FTC, including spam, is made available to thousands of civil and criminal law enforcement personnel in the United States and abroad.
Publicly available statistics	Statistics and annual reports

4.10 USA : Internet Crime Complaint Center (IC3)

Website	
www.ic3.gov	
Scope	
Internet fraud in general, including: • Intellectual Property Rights matters • Computer intrusions (hacking) • Economic espionage (theft of trade secrets) • Online extortion • International money laundering • Identity theft	
Reporting mode	
Online reporting via IC3.gov	
Information sharing	
Domestic level	IC3 builds referrals based on their data and send the referrals to appropriate law enforcement agencies at the local, state, national and national levels
International level	IC3 sends the referrals they build from their complaint data to law enforcement agencies of participating nations (only to law enforcement agencies)
Information value *Statistical* *Operational* *Strategic*	• IC3 US provides statistical reports to the FBI chain of command • IC3's groups victim complaints into cases that meet jurisdictional thresholds and forwards those cases to relevant law enforcement agencies. • Data helps the FBI anticipate needs and plan for future cyber challenges.
Publicly available statistics	Internet Crime Schemes Prevention Tips Annual report 2010

4.11 Mauritius: Mauritian National Computer Security Incident Response Team

Website	
http://cert-mu.gov.mu/English/Pages/default.aspx	
Scope	
• Information security: security incidents and vulnerability occurring within public and private sectors (e.g. DOS attacks against the Governmental portal and ISPs, phishing attacks against financial organisations) • Privacy breaches • Online harassment • Awareness raising and education programme	
Reporting mode	
Internet-based form, email, hotline, post	
Information sharing	
Domestic level	CERT-MU provides incident handling to the constituency members, which includes ISPs, academia, ICT vendors, Media, Law enforcement agencies, home users, government sector and private sectors
International level	CERT-MU is affiliated with the following international organizations: • CERT-CC • IMPACT • FIRST • APWG
Information value *Statistical* *Operational* *Strategic*	• Alerting Mauritian Internet Users in the event of a security breach • Coordination of expert advice while providing remedial assistance
Publicly available statistics	http://cert-mu.gov.mu/English/Pages/default.aspx

5 Conclusions/recommendations

The present study is to facilitate the setting up of cybercrime reporting mechanisms and further support by the GLACY project in this respect.

Cybercrime is a versatile concept, as any type of unlawful activity can involve some electronic element in its preparation or its execution. It is therefore no surprise that the same versatility can be found among cybercrime reporting mechanisms, with a variety of scopes, roles, public and/or private initiatives and funding models.

Beyond their diversity, cybercrime reporting mechanisms have in common that they contribute to measures against cybercrime by:

- Providing actionable information/complaints which can be the basis for investigations and prosecutions

- Identification of cybercrime threats on citizens and organisations, understanding and measuring trends

- Establishing a channel of communication between citizens (victims/witnesses of cybercrime) and the authorities/initiatives in charge

- Coordination between law enforcement and public authorities

- Fostering a culture of public/private cooperation and information sharing.

The GLACY project is available to provide further further advice in the creation of public reporting mechanisms and the collection of criminal justice statistics on cybercrime. At this point, the following five key recommendations should be highlighted:

1. Define the main objectives of a reporting mechanism

The five benefits listed above should serve as useful guidelines to define the objectives of a cybercrime reporting mechanism.

A critical aspect is the way reports will be managed by different agencies in order to take action against offenders. More specifically, two points should be kept in mind:

- *Will the reports be the basis for an investigation and a prosecution?* Receiving reports only to understand trends is important but not sufficient to fully justify the setup of a reporting cybercrime mechanism. Empowering enforcement action should be an integral part of a reporting mechanism.

- *Will the reports be the basis for a continuous improvement of the criminal justice?* A significant difference of approach is found between judicial authorities and initiatives of the private sector. While private initiatives are keen to measure the impact of their activities, learn from them and improve their processes, law enforcement agencies tend to adopt a more linear approach whereby reports are received and processed efficiently and diligently. A cybercrime reporting mechanism is also a tool to measure and improve the efficiency of criminal justice. An interesting long-term benefit of cybercrime reporting mechanisms is to improve the legal framework in order to help government agencies to give better responses to cybercrime.

2. Focus on major threats

As described in chapter 2, countries can be affected by different threats, with various levels of impact. Therefore, setting up a cybercrime reporting centre requires a focus on the main threats that matter most, as it is hardly possible to deal with all kind of threats, especially in an early phase of a reporting mechanism.

A focus on major threats will also add credibility to a cybercrime reporting mechanism.

3. Be open for insights

When a law enforcement agency sets up a reporting mechanism to enable reports online, this agency may have a mandate for specific threats, and it will only accept reports on offenses it is responsible for.

On the other hand, if a government is willing to set up an open reporting mechanism for all types of online threats, it may obtain interesting insights into what are the concerns of individuals and businesses, and build a better and more targeted response to threats.

4. Opt for the most suitable user interface to collect reports

Websites and call centres are the two most popular interfaces for cybercrime reporting mechanisms to collect and process reports. Obtaining reports through add-ons on a browser or from mobile applications are available but not commonly found at the moment.

Choosing the interface will depend on parameters such as local organisation, budget or availability of skills. The experience of most platforms surveyed shows that they often begin with a small staff and budget and later on expand their capacity, especially through cooperation between private and public sectors.

5. Streamline operations and share results

As shown by the survey, cybercrime reporting mechanisms contribute significantly to improving cooperation between law enforcement agencies and to streamlining operations. So, when setting up a reporting mechanism, it is critical to define how the information collected will be distributed among agencies and authorities, and will contribute to avoid duplication of efforts and make the overall organisation of law enforcement more effective.