



Koordinationsstelle zur Bekämpfung der Internetkriminalität
Service de coordination de la lutte contre la criminalité sur Internet
Servizio di coordinazione per la lotta contro la criminalità su Internet
Cybercrime Coordination Unit Switzerland

Servizio di coordinazione per la lotta contro la criminalità su Internet SCOCI

Rapporto annuale 2011

Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI)
Nussbaumstrasse 29
3003 Berna

www.scoci.ch
www.cybercrime.ch

Pubblicato il: 03.04.2012

Indice

1. L'ESSENZIALE IN BREVE	1
2. COMUNICAZIONI PERVENUTE	2
3. CONTENUTO DELLE COMUNICAZIONI	4
4. RICERCHE ATTIVE (MONITORING)	8
4.1 RICERCHE ATTIVE NELLE RETI PEER TO PEER.....	8
4.2 INCHIESTE MASCHERATE SVOLTE IN CHAT E RETI SOCIALI IN ASSENZA DI SOSPETTI.....	8
5. ALCUNI CASI	10
6. DESTINATARI DEI CASI E DELLE DENUNCE	12
7. RICONTRI DEI CANTONI	14
7.1 RICONTRI DELLE AUTORITÀ CANTONALI DI POLIZIA	15
7.2 RICONTRI DELLE AUTORITÀ GIUDIZIARIE CANTONALI.....	17
8. GRUPPI DI LAVORO	19
8.1 NAZIONALI	19
8.2 INTERNAZIONALI.....	19
9. PROGETTI	20
9.1. COLLABORAZIONE CON I PROVIDER SVIZZERI DI ACCESSO A INTERNET PER IL BLOCCO DI SITI PEDOPORNOGRAFICI	20
9.2 RACCOLTA NAZIONALE DI FILE E VALORI HASH (NDHS)	20
9.3 STRATEGIA NAZIONALE PER LA PROTEZIONE DELLA SVIZZERA DAI RISCHI INFORMATICI (PRECEDENTEMENTE DENOMINATA «STRATEGIA NAZIONALE PER LA CYBER DEFENCE») .	21
10. INTERVENTI POLITICI A LIVELLO FEDERALE	22
10.1 DURANTE L'ANNO IN ESAME SONO STATI PRESENTATI I SEGUENTI INTERVENTI PARLAMENTARI:	22
10.2 SVILUPPI GIURIDICI.....	23
11. PRESENZA NEI MASS MEDIA, ATTIVITÀ DIDATTICA E CONFERENZE	25
11.1 PRESENZA NEI MASS MEDIA	25
11.2 ATTIVITÀ DIDATTICA E CONFERENZE.....	25
12. COOPERAZIONE E CONTATTI	26
12.1 COLLABORAZIONE CON ALTRI SERVIZI DELLA CONFEDERAZIONE.....	26
12.2 RIUNIONI DI LAVORO E SCAMBI DI ESPERIENZE CON I CANTONI	26
12.3 COLLABORAZIONE CON ACTION INNOCENCE (AIG)	26
12.4 COLLABORAZIONE CON IL SETTORE PRIVATO (PARTENARIATO PUBBLICO-PRIVATO, PPP).....	27

12.5 VISITATORI ESTERNI	27
12.6 COLLABORAZIONE INTERNAZIONALE	27
13. GLOSSARIO	28
14. TENDENZE DEL 2011	29

1. L'essenziale in breve

- Nel 2011 sono pervenute a SCOCI 5330 comunicazioni trasmesse mediante l'apposito modulo online. Questa cifra corrisponde a un calo di quasi il 14 per cento rispetto all'anno precedente.
- Nonostante la flessione rispetto all'anno precedente, la categoria «pornografia illegale» (in particolare la pedopornografia) resta quella con il maggior numero di segnalazioni.
- Nell'anno in esame il monitoraggio delle reti peer to peer ha permesso a SCOCI di identificare 214 persone che hanno partecipato attivamente allo scambio di file con contenuti pedopornografici. Chi fa consumo di materiale pedopornografico sostiene la produzione di nuovo materiale visivo ed è quindi indirettamente coinvolto nell'abuso di minori.
- Si è registrato nuovamente un aumento delle segnalazioni nella categoria «criminalità economica».
- SCOCI ha compiuto notevoli progressi nello sviluppo della Raccolta nazionale di file e valori hash NDHS (Nationale Datei- und Hashwertsammlung). Nell'anno in esame i corpi di polizia cantonali sono stati istruiti con buoni risultati e SCOCI ha già ricevuto i primi archivi cantonali con immagini e filmati.
- Da maggio 2011 SCOCI fa parte del gruppo di progetto della Strategia nazionale per la Cyber Defence e rappresenterà gli interessi delle autorità cantonali e federali di perseguimento penale anche nel quadro dell'attuazione della strategia.
- La cooperazione internazionale nell'ambito della lotta contro la criminalità su Internet è stata considerevolmente ampliata in stretta collaborazione con Interpol ed Europol.

2. Comunicazioni pervenute

Nel 2011 sono pervenute a SCOCI 5330 comunicazioni trasmesse via Internet utilizzando l'apposito modulo. Si tratta di una diminuzione di quasi il 14 per cento rispetto all'anno precedente (6181 segnalazioni). Finora, ad eccezione dell'anno record 2007, la media annuale delle segnalazioni inviate via Internet mediante l'apposito modulo oscillava costantemente tra le 6000 e le 7500 comunicazioni. L'evoluzione del numero di segnalazioni pervenute non consente di trarre conclusioni in merito allo sviluppo effettivo della criminalità su Internet o ai contenuti illegali diffusi in rete. È tuttavia possibile rilevare le tendenze concernenti la disponibilità della popolazione a segnalare eventuali casi di cybercriminalità e al modo in cui la società percepisce la criminalità su Internet. I motivi per il calo delle segnalazioni trasmesse tramite il modulo online possono essere molteplici. Forse alcuni tipi di criminalità su Internet ormai sembrano talmente ordinari che la popolazione li considera banali e le vittime rinunciano a segnalarli a SCOCI. Rispetto agli anni precedenti nel 2011 è pertanto diminuita la quantità delle segnalazioni, ma quelle pervenute sono risultate più utili a causa della loro buona qualità. Il calo delle comunicazioni è presumibilmente dovuto al fatto che nell'anno in esame non vi sono stati casi che abbiano richiamato l'attenzione dei media e della popolazione.

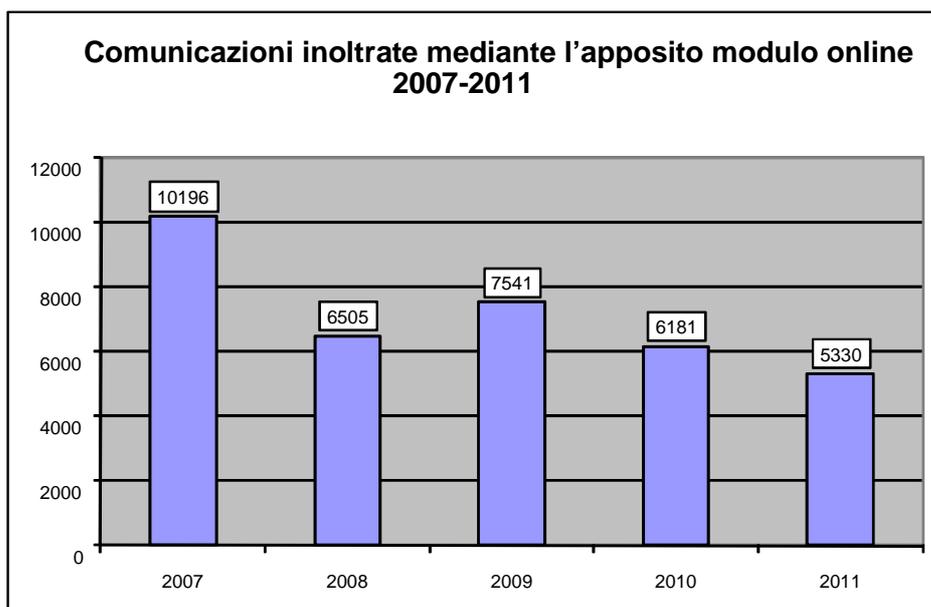


Grafico 1 : Comunicazioni pervenute tramite www.scoci.ch – dati annuali

Nell'anno in esame il numero di comunicazioni pervenute nei vari mesi è rimasto costante (cfr. grafico 2). Le oscillazioni sono spesso riconducibili a eventi concreti e circoscritti nel tempo. Questo avvalorata la teoria secondo cui la diminuzione delle segnalazioni registrata nel 2011 è dovuta in primo luogo alla mancanza di casi di ampia portata.

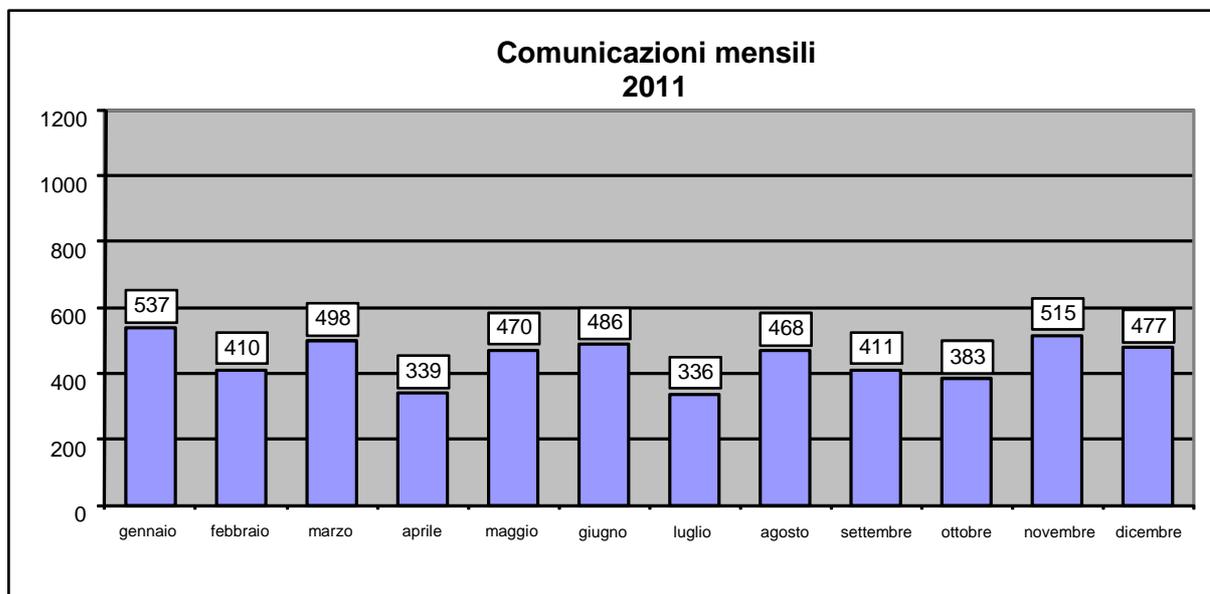


Grafico 2 : Comunicazioni pervenute tramite www.scoci.ch – dati mensili (totale: 5330 comunicazioni)

3. Contenuto delle comunicazioni

Se si analizzano le comunicazioni pervenute ripartendole in categorie, si constata, rispetto all'anno precedente, soprattutto un forte calo delle segnalazioni nel settore della «**pornografia dura**» (cfr. grafico 3). Questa categoria comprende le fattispecie di cui all'articolo 197 capoverso 3 del Codice penale (CP). Il 90 per cento delle segnalazioni concerne la fattispecie di pedopornografia. La diminuzione in questa categoria delle segnalazioni trasmesse a SCOCI mediante il modulo online è direttamente correlata al calo generale delle comunicazioni. Questo non significa tuttavia che tali contenuti e i reati pertinenti compiuti su Internet siano veramente diminuiti. Una simile ipotesi è infatti confutata sia dal lavoro quotidiano di SCOCI sia dallo scambio d'informazioni con i partner nazionali e internazionali. La flessione delle comunicazioni è in primo luogo riconducibile al fatto che i contenuti pedopornografici sono sempre meno accessibili al pubblico. I pedofili si servono consapevolmente di piattaforme protette o difficilmente accessibili quali forum, gruppi e reti sociali, che permettono loro di scambiare materiale pedopornografico in modo più discreto e anonimo. Nonostante il numero delle segnalazioni sia diminuito rispetto all'anno precedente, la categoria «pornografia dura» (in particolare la pedopornografia) resta tuttavia quella con il maggior numero di comunicazioni.

Nell'anno in esame le segnalazioni della categoria «**pornografia in generale**» sono leggermente aumentate rispetto all'anno precedente in cui erano invece diminuite. Le comunicazioni della categoria «**spam**» sono invece calate per il quarto anno consecutivo. Queste oscillazioni evidenziano che l'evoluzione del numero di comunicazioni inviate a SCOCI non rispecchia necessariamente il vero sviluppo della cybercriminalità. Benché da studi effettuati sull'evoluzione dello spamming, nel 2011 sia risultata una leggera decrescita del fenomeno a livello globale¹, nessuno studio è stato invece in grado di dimostrarne una riduzione pluriennale. È possibile che le vittime siano generalmente diventate più indifferenti nei confronti dello spamming e rinuncino pertanto a segnalarlo a SCOCI. I filtri di spam sono inoltre diventati sempre più affidabili cosicché i messaggi indesiderati sono spesso riconosciuti e filtrati ancor prima di essere percepiti dagli utenti.

Nella categoria «**criminalità economica**»² spicca in particolare l'aumento del 53 per cento delle comunicazioni nel settore delle **truffe**. Questo incremento conferma la tendenza riscontrata negli anni precedenti. Soprattutto le persone che acquistano prodotti (automobili, appartamenti, apparecchi elettrici ecc.) tramite programmi di condivisione online o siti di piccoli annunci finiscono nel mirino di truffatori, spesso di origini straniere. Sulle medesime pagine Internet vengono inoltre defraudati anche i venditori con false conferme di pagamento o rimborsi riscossi a posteriori. Continuano a fare vittime anche le cosiddette truffe dell'anticipo che, con il pagamento di una piccola tassa, promettono una grande vincita (p. es. nella lotteria). Oltre ai soldi anticipati, i truffatori sono sempre più interessati ai dati personali e ai documenti d'identità delle loro vittime (copia del passaporto o della carta d'identità). Oggigiorno,

¹ Cfr. p. es. i rapporti sulle minacce (Threats Reports) di McAfee

http://www.mcafee.com/apps/view-all/publications.aspx?pg=1&sz=10&tf=mcafee_labs.

² La categoria criminalità economica comprende i reati di truffa e quelli economici (soprattutto phishing e riciclaggio di denaro).

chiunque trasmette informazioni personali deve aspettarsi che i truffatori utilizzino la sua identità in modo abusivo per compiere altri reati.

Le segnalazioni concernenti **altri reati economici** (in particolare casi di phishing e di riciclaggio di denaro) sono aumentate di ben il 28 per cento. Nell'anno in esame la popolazione svizzera è stata ripetutamente colpita da tentativi di phishing. Gli artefici degli attacchi mirano principalmente a impossessarsi dei dati di accesso ai conti di e-banking e di programmi di condivisione online.

Il numero costantemente elevato di richieste d'informazione o di sostegno conferma che la popolazione e i fornitori di servizi Internet considerano SCOCI un centro di competenza in materia di criminalità su Internet.

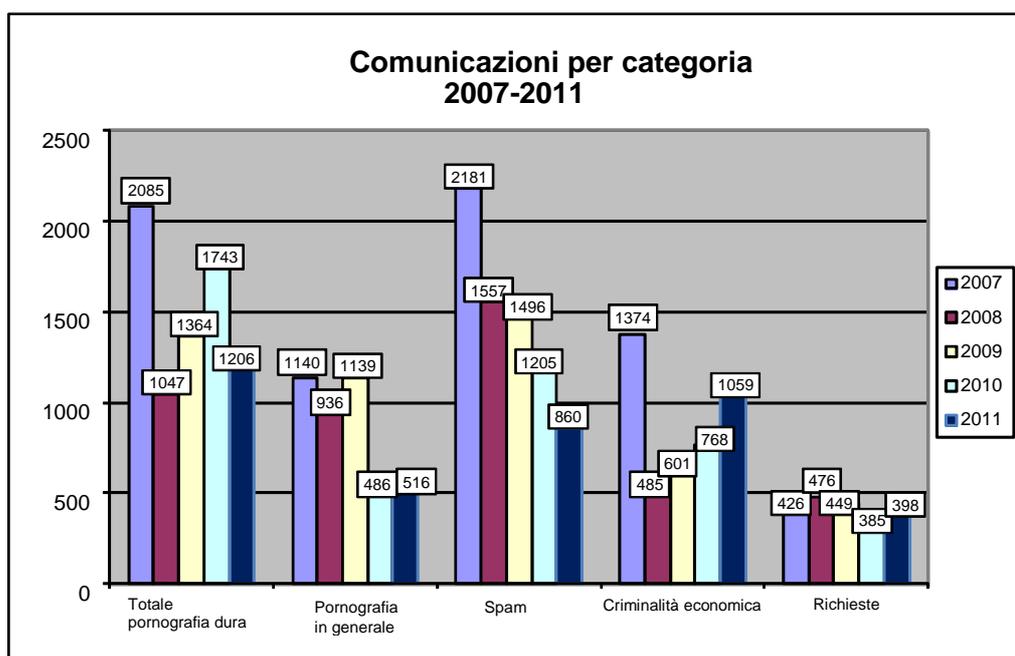


Grafico 3 : Sviluppo delle categorie di reato con il maggior numero di comunicazioni

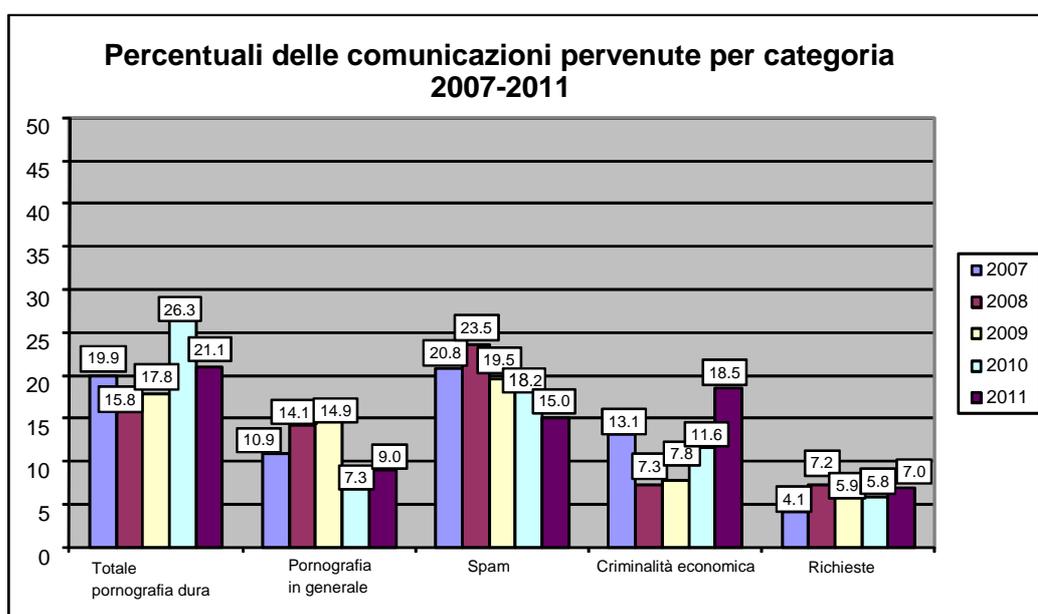


Grafico 4 : Paragone fra le percentuali di alcune categorie nell'arco degli ultimi cinque anni

Come ogni anno, anche nel 2011 sono state trasmesse tramite l'apposito modulo comunicazioni concernenti i reati più diversi. Il grafico 4 fornisce una panoramica sullo sviluppo delle categorie di reato più importanti degli ultimi cinque anni. Si è registrata una notevole crescita delle segnalazioni nelle categorie «**delitti contro l'onore**» (dal 0,7 % all'1,97 %) e «**minaccia e coazione**» (dal 0,42 % allo 0,67 %). Questi reati sono perlopiù commessi mediante reti sociali. Sono contenuti in tali categorie anche 30 casi di **ciberbullismo**³ (di cui almeno cinque concernono dei minori).

Nel settore della cibercriminalità sono aumentate le segnalazioni nelle categorie «**accesso indebito a sistemi di elaborazione dati**» (dal 0,44 % allo 0,84 %) e «**danneggiamento di dati**» (dal 0,57 % all'1,29 %). Sono stati segnalati a SCOCI anche diversi attacchi contro sistemi informatici di privati. In tale contesto si rimanda al punto 5 in cui sono descritti alcuni casi riscontrati nell'anno in esame, quale l'attacco di un malware che in Svizzera ha bloccato i computer di innumerevoli persone esortandole a pagare una tassa per sbloccare i PC colpiti. SCOCI segue da vicino l'evoluzione di questo fenomeno.

³ Si parla di ciberbullismo quando sono utilizzati moderni mezzi di comunicazione per pubblicare testi, immagini o filmati diffamatori con cui denigrare, offendere o molestare una determinata persona.

Percentuali delle comunicazioni suddivise per categoria 2011

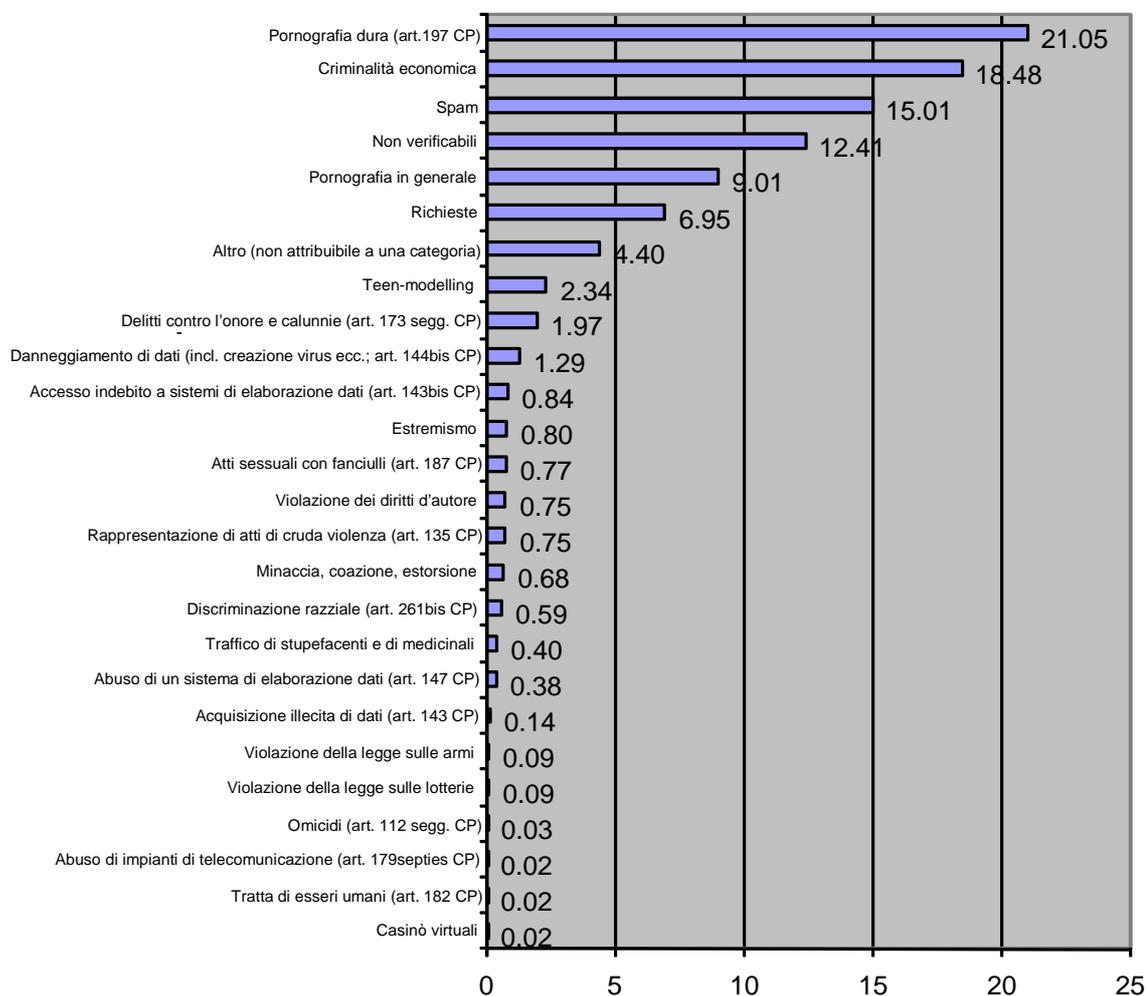


Grafico 5 : Comunicazioni del 2011 suddivise per categorie (in percentuale rispetto al totale delle segnalazioni)

4. Ricerche attive (monitoring)

Il lavoro di SCOCI non si limita soltanto alla ricezione e al trattamento di comunicazioni inoltrate dalla popolazione. SCOCI effettua ricerche in rete anche indipendentemente dalla presenza di indizi ed è quindi presente su Internet anche in settori meno accessibili, riuscendo così a produrre un effetto preventivo. Ogni anno il comitato direttivo di SCOCI fissa un nuovo settore su cui incentrare le ricerche attive. Come negli anni precedenti, anche nel 2011 tali ricerche erano focalizzate sulla lotta alla pedocriminalità su Internet. Il comitato direttivo aveva tuttavia dichiarato espressamente che SCOCI non deve escludere dalle ricerche i reati economici e la criminalità su Internet in senso stretto.

Il numero di casi prodotti dalle ricerche attive dello SCOCI nel 2011 (225) è simile a quello del 2010 e conferma la crescita iniziata nel 2009.

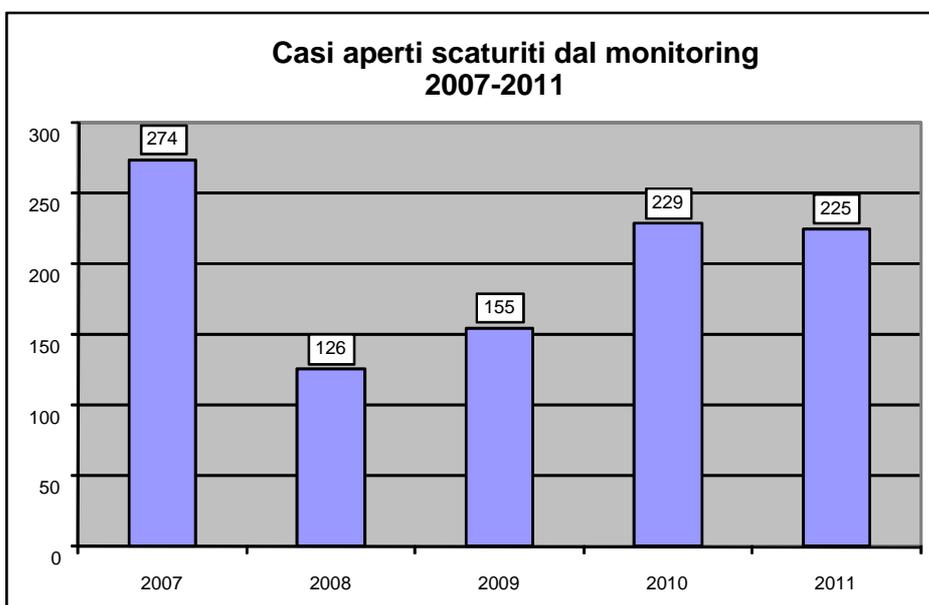


Grafico 6 : Casi scaturiti dalle ricerche attive

4.1 Ricerche attive nelle reti peer to peer

La maggior parte dei casi (214 su 225) è scaturita dal monitoraggio delle reti peer to peer, volto a individuare gli utenti di Internet che in Svizzera partecipano attivamente allo scambio di file con contenuti pedopornografici. Le reti peer to peer sono tuttora uno degli strumenti preferiti per scambiare dati su Internet in modo relativamente anonimo.

Nonostante SCOCI cerchi specificamente utenti domiciliati in Svizzera, nell'anno in esame sono stati riscontrati alcuni reati compiuti da due persone domiciliate all'estero. SCOCI ha trasmesso tali informazioni via Interpol ai Paesi competenti.

4.2 Inchieste mascherate svolte in chat e reti sociali in assenza di sospetti

Il 1° gennaio 2011 è entrato in vigore il nuovo Codice di diritto processuale penale svizzero (CPP) che ha sottratto alla Confederazione la competenza di eseguire in-

chieste mascherate in assenza di sospetti. La competenza in materia è stata assegnata esclusivamente ai Cantoni e deve pertanto essere disciplinata nelle singole leggi cantonali sulla polizia. Poiché entro il 1° gennaio 2011 soltanto pochi Cantoni avevano elaborato una relativa base giuridica, si temeva che potesse crearsi un vuoto giuridico.

Per evitare tale problema, l'Ufficio federale di polizia (fedpol) insieme al Cantone di Svitto ha elaborato un accordo stipulato il 23 dicembre 2010 con validità indeterminata. L'accordo sulla collaborazione in materia di indagini preliminari di polizia svolte su Internet al fine di combattere la pedocriminalità (monitoraggio di chat) concluso tra SCOCI, il Dipartimento di sicurezza del Cantone di Svitto e fedpol, disciplina le modalità secondo cui i collaboratori di SCOCI possono svolgere indagini preliminari mascherate per combattere la pedocriminalità in rete⁴. In virtù dell'accordo i collaboratori di SCOCI eseguono indagini preliminari mascherate esclusivamente su incarico e sotto il controllo della polizia cantonale di Svitto. In questo modo si garantisce che nel settore della pedocriminalità su Internet le ricerche attive potranno essere eseguite anche in futuro sotto forma d'inchieste mascherate di carattere preventivo. Con decisione del 14 gennaio 2011 il giudice cantonale dei provvedimenti coercitivi del Cantone di Svitto ha approvato la nomina di sei collaboratori di SCOCI ad agenti infiltrati che operano durante le indagini preliminari. Con decisione dell'11 gennaio 2012 lo stesso giudice ha prorogato tali nomine con effetto fino al 14 luglio 2012 e ha inoltre deciso la nomina di altri due collaboratori di SCOCI.

A seguito della decisione del giudice cantonale dei provvedimenti coercitivi, SCOCI ha attuato diversi lavori tecnici e operativi. L'istruzione necessaria in seno a SCOCI e la definizione dei processi con i Cantoni e fedpol hanno richiesto un certo tempo viste le poche risorse a disposizione.

Nel 2011 16 casi sono stati trattati conformemente all'ordinanza del Cantone di Svitto. Sono state adottate delle misure e la situazione è la seguente:

- sono state eseguite cinque perquisizioni domiciliari con interrogazione dell'indiziato di reato;
- è stato interrogato un indiziato di reato;
- quattro casi sono ancora in valutazione presso i pubblici ministeri competenti;
- in un caso il pubblico ministero ha deciso di non entrare nel merito;
- in quattro casi si è deciso di non procedere per mancata identificazione dell'autore o mancata concretizzazione di un sufficiente sospetto iniziale;
- un caso è ancora nelle mani di SCOCI ed è oggetto di ulteriori indagini.

Alla fine del 2011 non era ancora stato concluso l'esame del materiale sequestrato durante le perquisizioni domiciliari e non erano ancora pervenute nemmeno le valutazioni dei tribunali competenti.

⁴ Intervento ai sensi del § 9d dell'ordinanza del 22 marzo 2000 del Cantone di Svitto sulla polizia cantonale (PoIV – SRSZ 520.110).

5. Alcuni casi

Nell'anno in esame SCOCI ha trattato e coordinato tipologie di casi molto diverse. I seguenti esempi arricchiscono l'analisi dei dati puramente statistici e consentono di farsi un'idea delle attività di SCOCI.

Nel primo trimestre dell'anno in esame durante il monitoraggio di reti peer to peer sono state svolte indagini nei confronti di una persona che caricava in rete immagini e video pedopornografici mettendoli a disposizione di terzi. In occasione della successiva perquisizione domiciliare effettuata dalla polizia cantonale competente, oltre al reato nel settore della pedopornografia, il sospettato ha anche confessato di aver a più riprese abusato sessualmente di fanciulli. Il sospettato, fino ad allora sconosciuto alla polizia, era un puericultrice che lavorava in un asilo nido. La vittima più giovane dei suoi abusi aveva soltanto tre anni. Grazie al monitoraggio di reti peer to peer è stato quindi possibile smascherare un pedocriminale ed evitare che compiesse ulteriori reati sessuali a danni di fanciulli.

Nell'ambito delle sue inchieste mascherate, un'autorità estera di perseguimento penale aveva scoperto informazioni secondo cui un cittadino svizzero si sarebbe prossimamente imbarcato per la Gran Bretagna con lo scopo di commettere atti sessuali con un minore. L'autorità estera ha trasmesso le informazioni a SCOCI. Dagli accertamenti di SCOCI è emerso che il sospettato aveva precedenti per reati sessuali con minori e che era già stato condannato con sentenza passata in giudicato. La stretta cooperazione tra i due Paesi coinvolti ed i fornitori di servizio internet, grazie al quale è stato possibile identificare il sospettato, ha permesso di arrestare il cittadino svizzero all'entrata in Gran Bretagna. Il materiale trasportato nel bagaglio ha rafforzato il sospetto che l'uomo fosse seriamente intenzionato ad abusare sessualmente di un minore. Oltre a una prenotazione d'albergo, che risultava a nome del sospettato e di una persona minorenni, sono state sequestrate una videocamera e una quantità considerevole di nastri di registrazione. Questo caso dimostra che la cooperazione stretta e tempestiva tra Stati e fornitori di servizi Internet coinvolti, gestita tramite un centro nazionale di contatto, è decisiva per un'esecuzione efficace dell'azione penale. Senza le indagini mascherate dell'autorità estera di perseguimento penale non sarebbe mai stato possibile arrestare il sospettato prima della commissione del reato.

Un cittadino ha utilizzato il modulo per segnalare a SCOCI un forum, in cui un utente metteva a disposizione la propria figlia tredicenne per abusi sessuali. Tramite gli accertamenti di SCOCI è stata svelata l'identità del sospettato. Dal successivo interrogatorio effettuato dalla polizia cantonale competente è risultato che il sospettato non aveva nessuna figlia. Le sue osservazioni erano soltanto fantasie sessuali senza alcuna correlazione con la realtà. Le indagini allora si sono concentrate sulla moltitudine di persone che avevano scritto un'e-mail manifestando interesse per la ragazza minorenni. Per l'identificazione delle persone sospette il Cantone competente si è avvalso del sostegno di due agenti infiltrati di SCOCI che hanno fornito assistenza durante gli accertamenti effettuati in virtù del CPP. All'inizio del 2012 questa collaborazione è infine culminata nell'arresto di diverse persone domiciliate in Svizzera. Tutte le persone sono state fermate dalla polizia cantonale competente in occasione di un finto incontro con la presunta figlia tredicenne.

SCOCI si è occupato anche di diversi casi di cybercriminalità in senso stretto. Nell'autunno 2011 alcuni criminali hanno ad esempio infettato i computer di numerosi utenti svizzeri tramite siti di streaming. Gli autori si sono serviti di lacune nel software e nel sistema di sicurezza dei computer privati per perpetrare attacchi considerevolmente complessi e raffinati: mentre un malware bloccava il computer infetto, una finestra pop-up sollecitava gli utenti a pagare una tassa per sbloccare il PC. Il messaggio sembrava provenire dal Dipartimento federale di giustizia e polizia (DFGP) di cui i criminali avevano imitato il logo e il sito Internet. Reati analoghi vengono commessi di continuo, variano soltanto i siti imitati e il gruppo di utenti colpiti.

Tramite l'apposito modulo online a SCOCI è stato segnalato un uomo che si dichiarava sieropositivo e offriva in diversi forums la possibilità di trasmettere l'HIV. In questo caso è stato molto difficile accertare la competenza dal punto di vista tecnico. Grazie alle ricerche attive di SCOCI è infine stato possibile trovare sufficienti elementi per stabilire la competenza cantonale. La persona intenzionata a compiere il reato è stata in seguito denunciata al Cantone competente.

6. Destinatari dei casi e delle denunce

Nell'anno in esame SCOCI ha trasmesso alle autorità cantonali di perseguimento penale complessivamente 263 casi. Nonostante il leggero calo rispetto all'anno precedente (299), non si tratta comunque di un'inversione di tendenza.

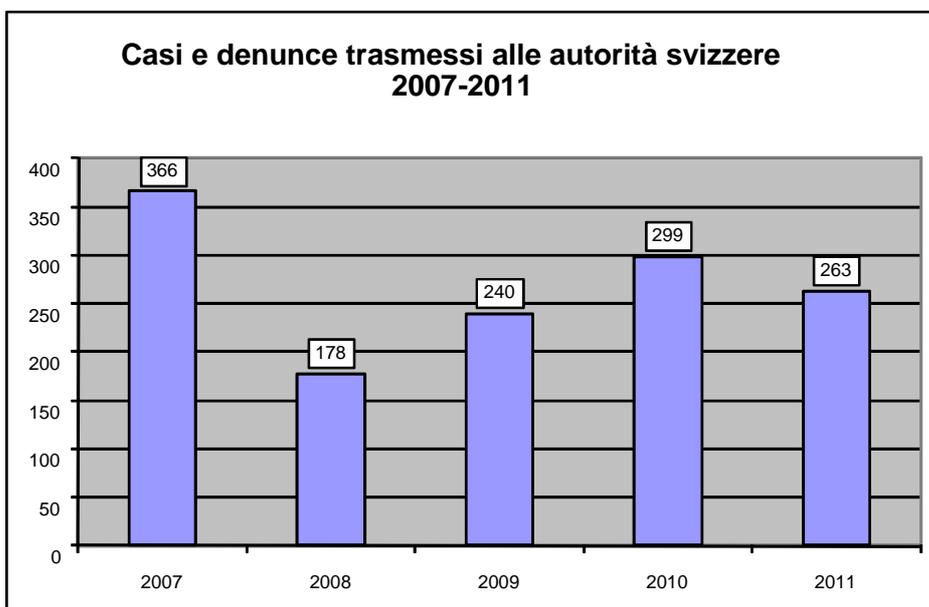


Grafico 7 : Numero di casi e denunce trasmessi

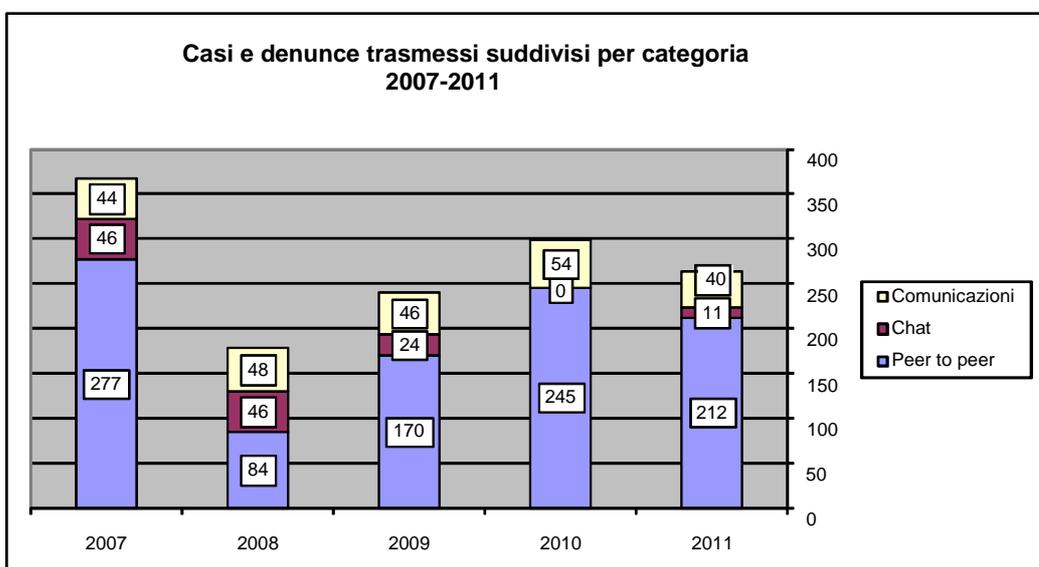


Grafico 8 : Casi e denunce trasmessi suddivisi per categoria

Il grafico 8 indica il motivo che ha indotto a trasmettere i casi e mostra che la flessione è in parte dovuta alla diminuzione dei casi della rubrica «comunicazioni». Quest'ultima comprende tutti i casi scaturiti da segnalazioni che i cittadini avevano inviato a SCOCI.

Anche il numero di casi riconducibili alle ricerche attive nelle reti peer to peer (212) è leggermente calato rispetto all'anno precedente (-14 %). Un'analisi più approfondita delle cifre ha rivelato che la flessione risale ai mesi di luglio, agosto e settembre,

quando i processi del progetto P2P-Scan sono stati perfezionati e potenziati al fine di incrementarne l'efficienza.

Undici casi adempivano la fattispecie di atti sessuali con fanciulli (art. 187 CP) e sono stati scoperti da SCOCI nell'ambito di inchieste mascherate nelle chat.

Come in passato, SCOCI ha trasmesso la maggior parte dei casi alle autorità dei Cantoni più popolosi, quali Zurigo, Berna e Vaud (cfr. grafico 9). Alcuni casi sono stati trasmessi all'interno di fedpol ai commissariati Criminalità generale, organizzata e finanziaria, Pedocriminalità e pornografia e Protezione dello Stato della PGF.

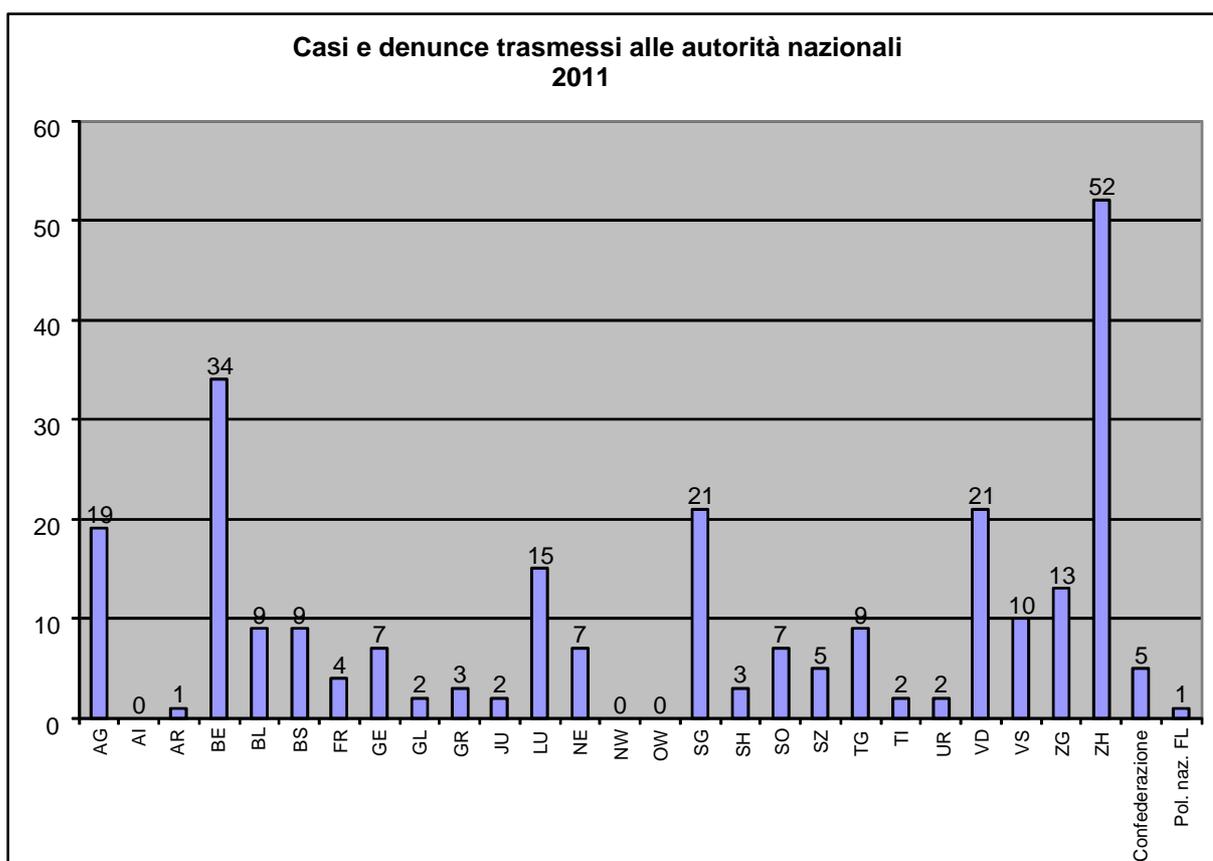


Grafico 9 : Numero di casi e denunce trasmessi alle autorità svizzere e del Principato del Liechtenstein (Pol. naz. FL)

In più di cinquanta casi SCOCI si è avvalso dei canali di Interpol ed Europol per trasmettere comunicazioni ad autorità estere di perseguimento penale. Si è trattato quasi esclusivamente di siti Internet con contenuti pedopornografici o di casi di criminalità su Internet in senso stretto che erano stati segnalati a SCOCI mediante l'apposito modulo. Oltre alle comunicazioni tramite Interpol o Europol, SCOCI ha spesso segnalato contenuti illeciti direttamente ai fornitori di servizi Internet e ai gestori di siti Internet per la cancellazione.

7. Riscontri dei Cantoni

SCOCI trasmette i casi in cui sussistono sospetti fondati di reato ai Cantoni per il trattamento (cfr. grafico 7). Per avere una panoramica generale delle attività intraprese dai Cantoni, SCOCI chiede loro informazioni sullo sviluppo dei casi segnalati, in particolare sulle misure adottate dalla polizia e sull'esito dei procedimenti giudiziari.

L'analisi di questi riscontri costituisce un mezzo importante per valutare l'efficacia dell'attività di SCOCI e la qualità dei casi e delle denunce inoltrati ai Cantoni. La maggior parte dei casi (74 %) scaturisce dalle ricerche attive nelle reti peer to peer. I casi riguardano pertanto persone che partecipano attivamente allo scambio di contenuti illeciti di carattere pedopornografico.

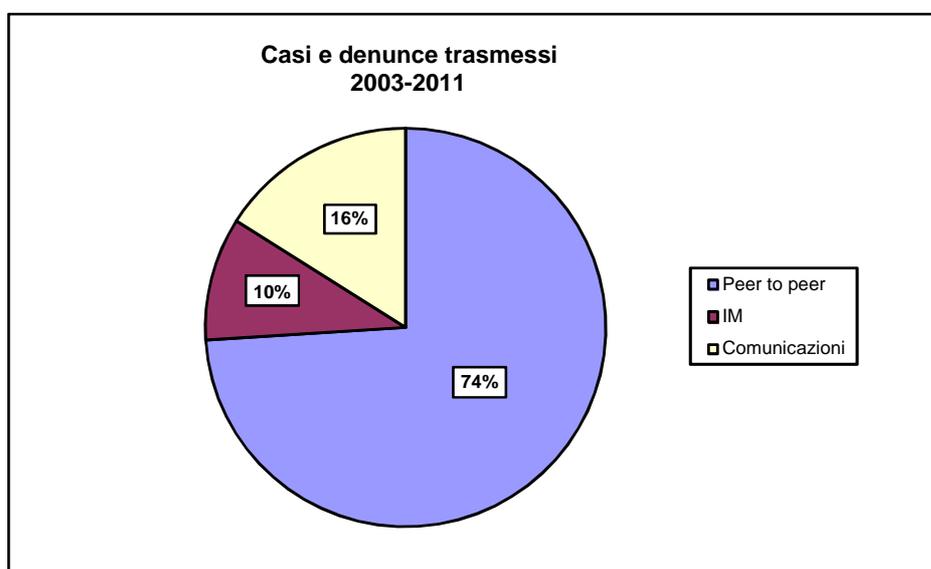


Grafico 10 : Dal 2003 sono stati trasmessi 2437 casi e denunce⁵.

⁵ IM = instant messaging o messaggistica istantanea è un sistema di comunicazione che consente a due o più utenti di comunicare (chattare) inviandosi dei testi in tempo reale.

7.1 Riscontri delle autorità cantonali di polizia

Come si evince dal grafico 11, nel 91 per cento di tutti i casi trasmessi da SCOCI le autorità cantonali di polizia sono state indotte a eseguire perquisizioni domiciliari. Oltre il 98 per cento delle comunicazioni della categoria «peer to peer» ha dato luogo a una perquisizione domiciliare, mentre le segnalazioni della categoria «comunicazioni» (cfr. grafico 10) di norma non giustificano una perquisizione domiciliare.

Il 95 per cento delle perquisizioni domiciliari sono state ordinate in seguito a un caso della categoria «peer to peer».

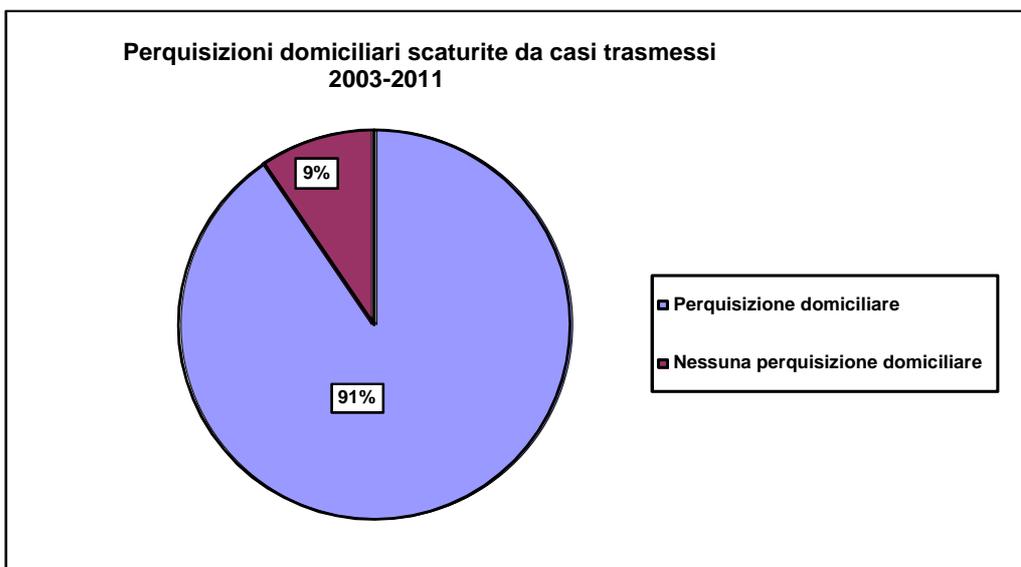


Grafico 11 : Perquisizioni domiciliari (791 riscontri)

Nell'84 per cento delle perquisizioni domiciliari effettuate sulla scorta delle segnalazioni di sospetto è stato sequestrato del materiale illegale. Solamente nel 16 per cento dei casi le perquisizioni non hanno consentito di confiscare materiale penalmente rilevante. Vi sono molteplici ragioni per le quali una perquisizione domiciliare non produce risultati e non sempre sono facili da individuare.

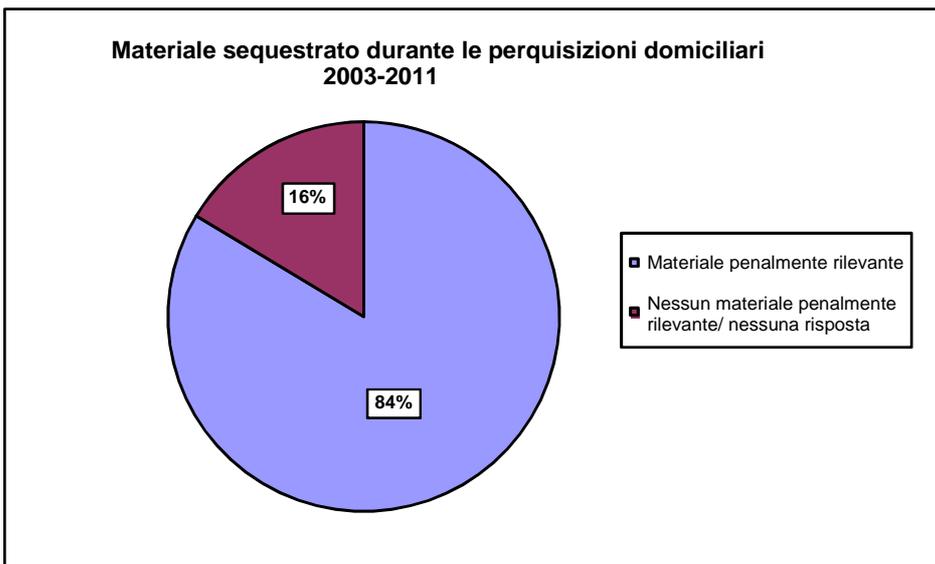


Grafico 12 : Sequestro di materiale illegale (716 perquisizioni domiciliari)

Nel 94 per cento dei casi il materiale penalmente rilevante sequestrato era di carattere pedopornografico. La percentuale elevata tuttavia non stupisce se si considera che le ricerche attive nelle reti peer to peer sono incentrate sui reati di questo genere e che la maggior parte dei casi scaturiscono da tali ricerche. È inoltre degno di nota che in più della metà dei casi sono stati riscontrati anche altri reati correlati alla pornografia vietata (art. 197 CP; cfr. grafico 13). Infatti, nella metà delle perquisizioni domiciliari sono stati inoltre sequestrati contenuti di pornografia con animali.

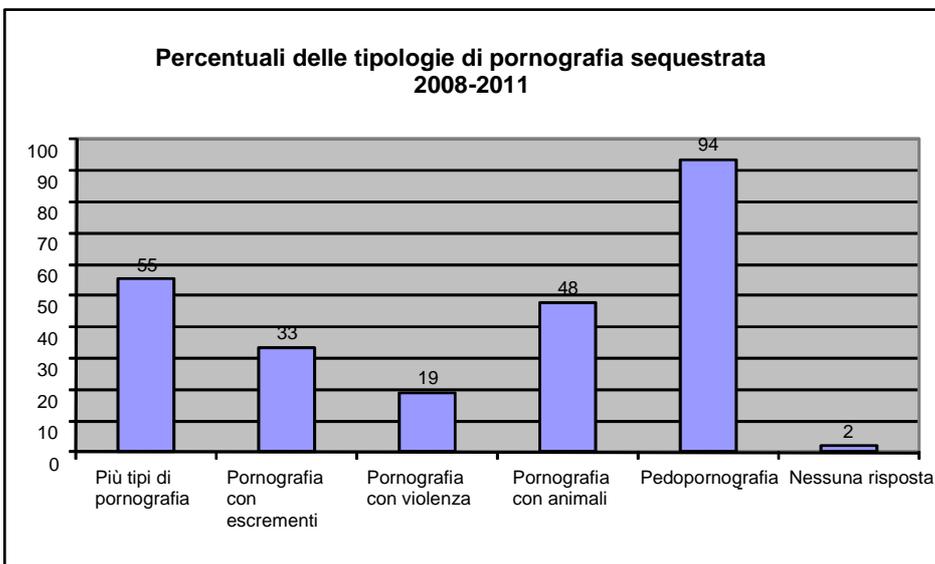


Grafico 13 : Tipologia di materiale sequestrato (251 riscontri)

Dai riscontri forniti dalle autorità cantonali di polizia emerge che nell'80 per cento delle perquisizioni domiciliari con esito positivo sono stati sequestrati filmati e nel 63 per cento immagini. In molti casi è stato trovato e confiscato materiale probatorio di entrambe le categorie. Le perquisizioni domiciliari complessivamente hanno consentito di sequestrare decine di migliaia di filmati e centinaia di migliaia di immagini.

7.2 Riscontri delle autorità giudiziarie cantonali

Nel 90 per cento dei casi in cui le autorità giudiziarie cantonali hanno fornito un riscontro a SCOCI, i procedimenti penali si sono conclusi con una condanna.

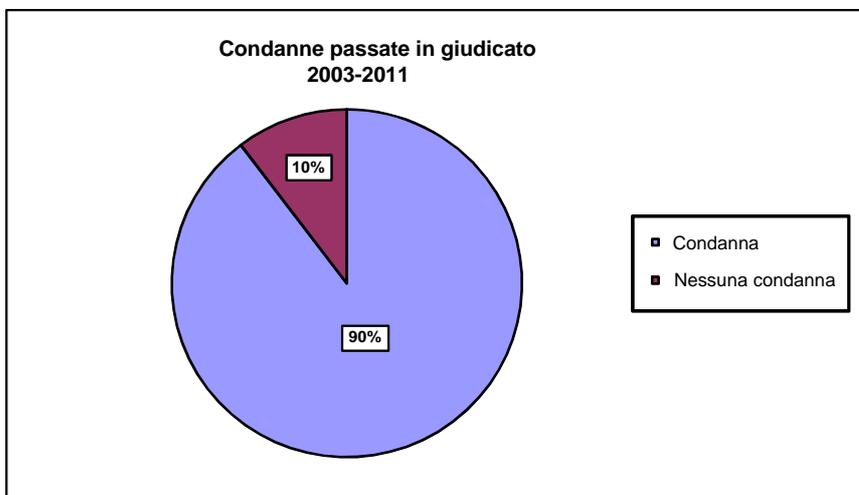


Grafico 14 : Condanne passate in giudicato (589 riscontri)

La maggioranza delle condanne è stata pronunciata per possesso di pornografia dura e quindi sulla base della fattispecie penale della pornografia (art. 197 CP) e in particolare delle fattispecie di cui ai numeri 3 e 3^{bis}⁶. In singoli casi vi sono state condanne per violazione dell'articolo 187 numero 1 CP (atti sessuali con fanciulli).

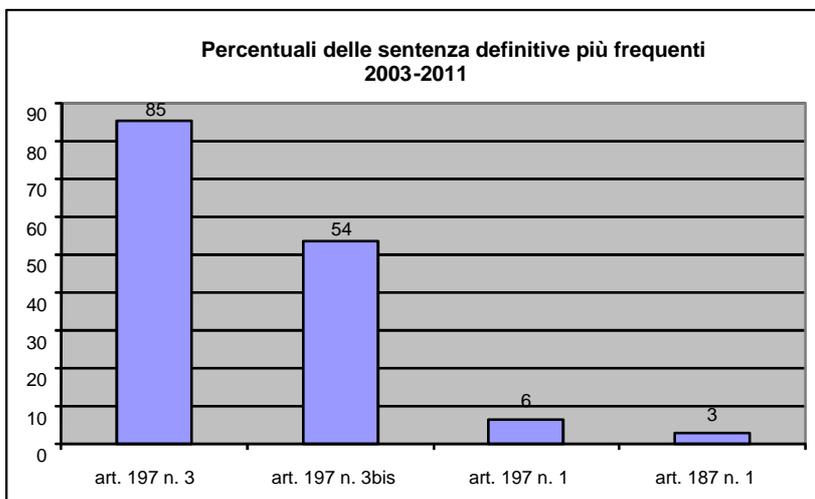


Grafico 15 : Condanne più frequenti (532 sentenze definitive)

⁶ n. 3. Chiunque fabbrica, importa, tiene in deposito, mette in circolazione, propaganda, espone, offre, mostra, lascia o rende accessibili oggetti o rappresentazioni a tenore del numero 1, vertenti su atti sessuali con fanciulli, animali, escrementi umani o atti violenti, è punito con una pena detentiva sino a tre anni o con una pena pecuniaria.

Gli oggetti sono confiscati.

n. 3^{bis}. Chiunque acquista, si procura per via elettronica o in altro modo o possiede oggetti o rappresentazioni a tenore del numero 1, vertenti su atti sessuali con fanciulli, animali o atti violenti, è punito con una pena detentiva sino ad un anno o con una pena pecuniaria.

Nella maggioranza dei casi, le condanne consistevano in una pena pecuniaria (in aliquote giornaliere), spesso accompagnata da una multa. Nel 91 per cento dei casi è stata pronunciata una pena pecuniaria con la condizionale. Il lavoro di pubblica utilità e le misure terapeutiche sono state ordinate soltanto in pochi casi. Le pene più severe, quali la privazione della libertà (carcere) e le pene pecuniarie senza condizionale, sono state inflitte quasi esclusivamente in caso di recidiva.

In due terzi dei casi l'importo delle multe era inferiore ai 1000 franchi. Nel 16 per cento dei casi la loro entità era compresa tra i 1000 e i 2000 franchi. Soltanto il 18 per cento delle multe ha superato i 2000 franchi. Il 48 per cento delle pene pecuniarie ammontava a meno di 51 aliquote giornaliere, mentre nel 35 per cento dei casi il loro numero era compreso tra 51 e 100. Soltanto nel 17 per cento dei casi sono state comminate più di 100 aliquote giornaliere. Per quanto concerne, infine, l'importo delle aliquote giornaliere, il 24 per cento oscilla tra 1 e 50 franchi, il 38 per cento tra i 51 e i 100 franchi e il restante 38 per cento supera i 100 franchi.

L'importo della maggior parte delle multe pronunciate era compreso tra i 500 e i 3000 franchi, mentre la multa più elevata era pari a 6000 franchi. I condannati di regola sono inoltre tenuti ad assumere le spese procedurali che spesso superano ampiamente la multa. La maggior parte delle pene pecuniarie inflitte erano comprese tra 20 e 200 aliquote giornaliere di cui l'importo di ciascuna oscillava tra i 20 e i 200 franchi.

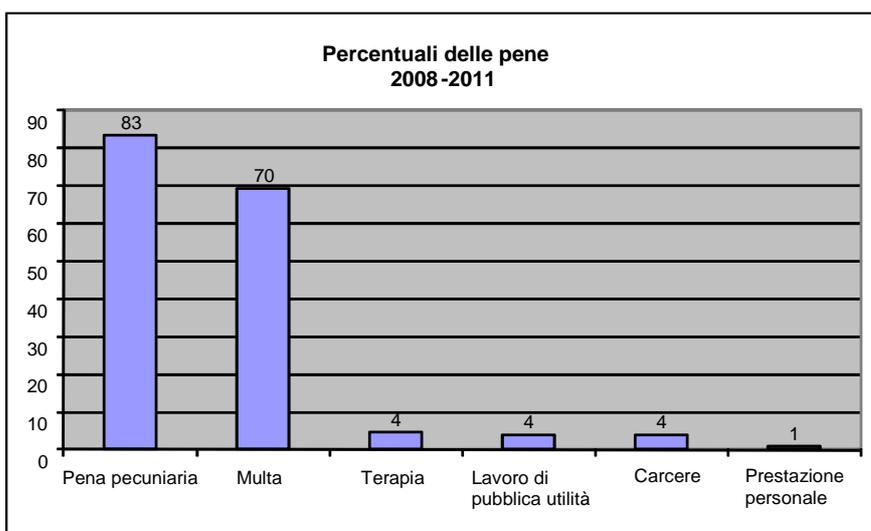


Grafico 16 : Tipi di condanne (242 riscontri)

8. Gruppi di lavoro

8.1 Nazionali

Nell'anno in esame, SCOCI ha partecipato a diversi gruppi di lavoro nazionali, in particolare nell'ambito della prevenzione della criminalità.

Anche nel 2011 ha collaborato, ad esempio, attivamente al gruppo di lavoro nazionale «Kindsmisbrauch» (abusi sui fanciulli), assieme al commissariato Pedocriminalità / pornografia di fedpol, a organizzazioni di utilità pubblica, ai Cantoni e alla Prevenzione svizzera della criminalità.

Nel 2011 SCOCI ha preso parte inoltre ai lavori del programma nazionale Protezione della gioventù dai rischi dei media e competenze mediatiche, sia in seno al comitato direttivo, incaricato dell'elaborazione del programma, sia nel gruppo esecutivo di accompagnamento. Il programma intende aiutare i bambini e i giovani a utilizzare i media moderni in modo sicuro, responsabile e adeguato alla loro età. L'evento saliente del programma è stata la giornata nazionale delle competenze medial, che è stata organizzata per la prima volta e che si è svolta a Friburgo il 27 ottobre 2011.

Dal 2011 SCOCI rappresenta fedpol anche in seno alla commissione speciale della Prevenzione svizzera della criminalità. La commissione sviluppa il materiale informativo e i progetti per la prevenzione della criminalità nei Cantoni, valutandone l'attuazione.

SCOCI ha contribuito altresì ad attuare il piano denominato «Sicurezza e fiducia», diretto dall'Ufficio federale delle comunicazioni (UFKOM). Il piano illustra le misure volte a promuovere la sicurezza e la fiducia della popolazione nei confronti delle moderne tecnologie dell'informazione e della comunicazione.

Infine, partecipando ai gruppi di lavoro IT Ermittler (Inquirenti IT) e Telekommunikationsüberwachung (Sorveglianza delle telecomunicazioni), SCOCI si è occupato, anche nel 2011, delle tematiche legate allo sviluppo tecnico e all'efficienza nel perseguimento penale.

8.2 Internazionali

Nel 2011 SCOCI è diventato membro dell'Analysis Work Files (AWF) Cyborg di Europol. Lo scopo dell'AWF Cyborg è contrastare la criminalità sovranazionale su Intranet, in particolare i fenomeni del phishing, delle reti bot e dell'hacking. SCOCI collabora inoltre al CIRCAMP, un progetto che si prefigge di combattere la diffusione di materiale pedopornografico su Intranet, con particolare riguardo per le piattaforme che diffondono tali contenuti. Inoltre, come negli anni precedenti, anche nel 2011 SCOCI ha preso parte a Bruxelles al gruppo di lavoro European Financial Coalition.

Nell'anno in esame, SCOCI ha altresì partecipato a Strasburgo al Comitato della Convenzione del Consiglio d'Europa sulla cybercriminalità (T-CY). In tale occasione, oltre a commemorare il decimo anniversario della Convenzione, è stata celebrata anche la sua entrata in vigore in Svizzera il 1° gennaio 2012.

9. Progetti

9.1. Collaborazione con i provider svizzeri di accesso a Internet per il blocco di siti pedopornografici

Dal 2007 SCOCI fornisce supporto ai principali provider svizzeri di accesso a Internet per il blocco di siti a carattere pedopornografico. Il blocco riguarda esclusivamente i siti esteri contenenti materiale pedopornografico che, malgrado le segnalazioni trasmesse all'autorità di perseguimento penale competente, non sono stati ancora rimossi. SCOCI mette a disposizione dei provider una lista costantemente aggiornata dei siti Internet in questione. I provider bloccano l'accesso alle pagine contenenti materiale penalmente rilevante in virtù della propria etica aziendale e delle condizioni generali di contratto e rinviano successivamente l'utente a una cosiddetta «stop page».

Nel quadro di tale progetto, SCOCI collabora strettamente con Interpol. Anche Interpol gestisce una lista delle pagine Internet contenenti immagini e filmati pedopornografici («worst of list»). Nel 2011, è stato possibile ampliare ulteriormente la collaborazione a tale progetto, cui prendono parte diversi Paesi. L'elenco allestito dalla Svizzera è costituito dalla lista di Interpol, completata dalle pagine Web con materiale pedopornografico individuate da SCOCI. SCOCI integra quotidianamente la «worst of list» di Interpol nel proprio elenco segnalando, a sua volta, a Interpol nuove pagine Web da inserire nella «worst of list».

9.2 Raccolta nazionale di file e valori hash (NDHS)

Le autorità cantonali competenti trasmettono a SCOCI i file (p. es. immagini, video ecc.) sequestrati nell'ambito di indagini sulla pedopornografia. SCOCI attribuisce a ogni file un valore hash⁷ e lo registra nella Raccolta nazionale di file e valori hash. Tale lista può essere consultata dai Cantoni tramite la community JANUS⁸. Le autorità cantonali competenti attribuiscono anch'esse a ogni file appena sequestrato un valore di hash. I valori di hash così attribuiti possono essere in seguito confrontati con quelli attribuiti da SCOCI. Il confronto permette d'individuare corrispondenze tra file di grandi dimensioni e, dunque, di accertare agevolmente se un file è già stato catalogato. Grazie a tale prassi, gli inquirenti non sono quindi più tenuti a effettuare un'analisi visiva del materiale penalmente rilevante (dati grezzi), con conseguenti notevoli vantaggi in termini di tempo e di stress.

Nell'anno in esame è stato dato un impulso decisivo al progetto. fedpol ha concluso i lavori di pianificazione insieme ai Cantoni e ha creato l'infrastruttura necessaria. In occasione di riunioni informative, i rappresentanti di tutti i Cantoni sono stati istruiti sull'uso dell'NDHS. I Cantoni hanno inoltre trasmesso con successo a SCOCI le prime serie di dati contenenti immagini e filmati.

⁷ Valore attribuibile in modo univoco a un'immagine (impronta digitale).

⁸ Rete Intranet in cui sono pubblicate informazioni utili per le autorità di polizia svizzere.

Infine, grazie ad un software di riconoscimento delle immagini, sviluppato dall'azienda svizzera ATG insieme a SCOCI, si suppone che sarà possibile ridurre considerevolmente il tempo impiegato per la catalogazione e la verifica dei file trasmessi a SCOCI. In futuro, si prevede di utilizzare questo software anche per offrire supporto agli interventi operativi.

9.3 Strategia nazionale per la protezione della Svizzera dai rischi informatici (precedentemente denominata «Strategia nazionale per la Cyber Defence»)

Il 10 dicembre 2010 il Consiglio federale ha incaricato il DDPS di sviluppare una strategia nazionale per la Cyber Defence e ha designato il divisionario Kurt Nydegger come capo progetto. La strategia mira in particolare a proteggere le infrastrutture critiche da attacchi informatici. In tale contesto, occorre fornire informazioni precise sui lavori di attuazione previsti nonché sulle conseguenze in termini di tempo, costi, competenze e risorse nonché sotto il profilo legale. La strategia, unitamente alle diverse misure di attuazione proposte, sarà sottoposta all'attenzione del Consiglio federale nel primo trimestre del 2012. A partire dal maggio del 2011, SCOCI partecipa al gruppo di progetto e sarà inoltre chiamato a rappresentare gli interessi delle autorità cantonali e federali di perseguimento penale anche nel quadro dell'attuazione della strategia.

10. Interventi politici a livello federale

10.1 Durante l'anno in esame sono stati presentati i seguenti interventi parlamentari:

Protezione di bambini e adolescenti / pedocriminalità

Interpellanza Pasquier: Proteggere i minori dallo sfruttamento e dagli abusi sessuali
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20113141

Mozione Savary: Pornografia su Internet. Agire a monte.
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20113314

Domanda Bruderer-Wyss: Repressione degli atti sessuali con minori di età compresa tra i 16 e i 18 anni (Bestrafung sexueller Kontakte mit 16- bis 18-Jährigen)
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20115351

Domanda: Registro nazionale dei pedofili (Pädophilenregister)
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20115008

Mozione Schmid-Federer: Punire il grooming
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20114002

Oggetto del Consiglio federale CP, CPM e DPMIn. Imprescrittibilità dei reati sessuali o di pornografia commessi su fanciulli impuberi
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20110039

Altri

Interpellanza Amherd: Potenziare la sorveglianza di Internet
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20113862

Postulato Eichenberger-Walther: Per una rete nazionale di centri di competenza di polizia
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20113642

Domanda Leutenegger-Oberholzer: Uso di trojan da parte della Confederazione (Einsatz von Bundes-Trojanern)
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20115541

Domanda Reimann: Pratiche dubbie di PayPal in Svizzera (Fragwürdige Praktiken von PayPal in der Schweiz)
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20115438

Domanda Schmid-Federer: Punto della situazione a distanza di un anno sulla campagna di prevenzione dell'UFAS (Stand der Präventionskampagnen des BSV nach einem Jahr)
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20115198

Postulato Amherd: Diamo un quadro legale ai social media
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20113912

Postulato Schmid-Federer: Legge quadro sulle TIC
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20113906

Petizione: Divieto per i videogiochi violenti (Verbot von Killerspielen)
http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20112005

10.2 Sviluppi giuridici

La lotta contro la cybercriminalità pone anche la giurisprudenza e la legislazione di-
nanzi a nuove sfide. La presente sezione si sofferma sui particolari sviluppi giuridici a
livello nazionale e internazionale.

Decisione del Tribunale federale 6B_744/2010

Nel 2011 il Tribunale federale ha affrontato la questione della punibilità di persone
che detengono materiale pedopornografico nella cache del proprio computer. Con
decisione del 12 maggio 2011, il Tribunale federale ha stabilito che tutti i dati elettro-
nici nonché tutte le modalità di salvataggio di tali dati rientrano nel campo
d'applicazione dell'articolo 197 numero 3^{bis} CP. Le pagine Web visitate vengono au-
tomaticamente salvate sul disco rigido, precisamente nella cartella dei file tempora-
nei di Internet. Ciò consente in caso di nuovo accesso al sito di caricare più veloce-
mente la pagina già visitata. Grazie ai comuni software disponibili gratuitamente (Ca-
cheViewer o Cache Reader) è possibile inoltre accedere, anche in assenza di con-
nessione (p. es. in modalità offline), alle pagine Internet memorizzate. Il Tribunale
federale precisa che il possesso di pornografia dura, punito dall'articolo 197 numero
3^{bis} CP, comprende sia la possibilità sia la volontà di esercitare il proprio potere sulla
cosa. A tale proposito, va ricordato che un normale utente d'Internet non ha un ruolo
attivo nella memorizzazione di un file temporaneo nella memoria cache e che
l'eventuale presenza in cache di tali dati non è quindi sufficiente a comprovare
l'esistenza di un potere di fatto sulla cosa, qualificabile come possesso. Chi invece
consulta più volte e intenzionalmente nell'arco un lungo periodo delle pagine Web
contenenti materiale di pornografia dura, non si limita semplicemente a visionarne i
contenuti. L'accesso ripetuto a questo tipo di siti dimostra infatti la volontà dell'utente
di esercitare il proprio potere sulla cosa. Nonostante il salvataggio temporaneo av-
venga in modo automatico, l'utente ha sempre la possibilità di disattivare tale funzio-
ne o di svuotare la memoria cache. Secondo il Tribunale federale, inoltre, oggi do-
vrebbe essere noto a ogni utente che le pagine Internet consultate vengono salvate
temporaneamente nella memoria cache.

Il divieto sancito dall'articolo 197 numero 3^{bis} CP di procurarsi materiale di pornogra-
fia dura si applica già nel caso in cui un utente ottenga, tramite una password, un
accesso costante e illimitato a una pagina Web con questo tipo di contenuti, dispo-
nendo quindi liberamente dei dati. Lo stesso principio deve valere anche per il pos-
sesso di questo tipo di dati, ovvero qualora un utente possa accedere in qualsiasi
momento ai file illegali archiviati, ad esempio attraverso la cartella dei file temporanei
di Internet. Tale decisione permette di colmare, come auspicato, ogni lacuna in mate-
ria di punibilità della pornografia dura.

Il Consiglio federale non modifica la legge sul diritto d'autore

Nel novembre 2011, il Consiglio federale ha risposto con un rapporto al postulato
depositato nel marzo del 2010 dalla consigliera agli Stati Géraldine Savary (PS/VD).

Il Consiglio degli Stati aveva approvato il postulato, chiedendo al Consiglio federale di esaminare la possibilità di adottare misure contro le violazioni del diritto d'autore. Dal rapporto del Consiglio federale emerge che in Svizzera un terzo delle persone sopra i 15 anni scarica gratuitamente da Internet musica, film e giochi. Il rapporto afferma inoltre che sebbene Internet abbia radicalmente cambiato il modo di consumare musica, film e giochi, ciò non influisce negativamente sull'attività culturale. Per tale ragione, il Consiglio federale non ritiene necessario modificare la legislazione sui diritti di autore. Pertanto, visto che la Svizzera non punisce il download per scopi privati di musica e film protetti dal diritto d'autore, gli utenti svizzeri di Internet potranno continuare a scaricare film e canzoni per uso personale, senza il rischio d'incorrere in sanzioni penali.

Cybercrime Convention

Con la ratifica della Convenzione del Consiglio d'Europa sulla cibercriminalità, la Svizzera partecipa all'intensificazione della lotta contro la criminalità informatica e in Internet. La Convenzione entra in vigore in Svizzera il 1° gennaio 2012. Per la stessa data il Consiglio federale ha fissato l'entrata in vigore delle pertinenti modifiche di legge.

La Convenzione del Consiglio d'Europa sulla cibercriminalità è il primo trattato internazionale per la lotta contro la criminalità informatica e in Internet. Essa obbliga gli Stati contraenti a punire in particolare la frode informatica, il furto di dati, la falsificazione di documenti mediante computer, l'accesso a sistemi informatici protetti come pure la pedopornografia e la violazione di diritti d'autore in Internet.

La Convenzione disciplina inoltre le modalità di raccolta e conservazione, nelle inchieste penali, delle prove costituite da dati elettronici. Intende in particolare garantire che le autorità inquirenti possano accedere rapidamente ai dati trattati elettronicamente, affinché questi ultimi non possano essere falsificati o eliminati nel corso della procedura. Infine, la Convenzione si propone di garantire una cooperazione ampia, rapida ed efficace tra gli Stati contraenti.

Per attuare la Convenzione è stato necessario adeguare il Codice penale e la legge sull'assistenza in maniera penale. Per quanto concerne la fattispecie penale dell'accesso illegale a un sistema per l'elaborazione di dati («hacking»), la punibilità è stata anticipata: in futuro sarà perseguibile anche chi rende accessibili o diffonde password, programmi e altri dati, sapendo o presumendo che essi saranno usati per accedere illegalmente a un sistema informatico protetto.

La legge sull'assistenza in materia penale conferirà in futuro alla competente autorità svizzera la facoltà di trasmettere, in determinati casi e a fini investigativi, i dati relativi al traffico informatico all'autorità richiedente prima della conclusione della procedura di assistenza giudiziaria. Tuttavia, tali dati, che forniscono informazioni sul mittente, il destinatario, l'orario, la durata, la dimensione e il percorso di un messaggio, possono essere utilizzati come mezzi di prova soltanto dopo che la decisione finale sulla concessione e sulla portata dell'assistenza giudiziaria è cresciuta in giudicato.

È stato deciso di affidare alla Centrale operativa fedpol (SPOC, CO fedpol), la funzione di punto di contatto 24/7 prevista dall'articolo 35 della Convenzione. SCOCI offre supporto allo SPOC nell'ambito del trattamento delle richieste ai sensi della Convenzione.

11. Presenza nei mass media, attività didattica e conferenze

11.1 Presenza nei mass media

Nel 2011, i media hanno dato ampia risonanza a SCOCI e alle sue attività. Particolare importanza è stata data alle indagini preliminari mascherate di carattere preventivo condotte da SCOCI nonché a singoli attacchi spettacolari ai danni di sistemi informativi (attacchi DDoS⁹). Il giudizio complessivo dei media è stato per l'anno in esame positivo.

11.2 Attività didattica e conferenze

Nell'anno in esame, i collaboratori di SCOCI hanno partecipato a numerose conferenze, convegni internazionali e corsi. Occasioni queste, che rappresentano anche dei momenti ideali per lo scambio d'idee con partners ed esperti, o per allacciare nuovi contatti.

In Svizzera :

- Giornata svizzera degli inquirenti IT, Berna
- giornata delle competenze medialti (nel quadro del programma nazionale «Giovani e media»), Friburgo
- World Summit Information Society (WSIS), Ginevra

All'estero :

- «RIPE NCC Meeting», Londra
- Conferenza «Octopus Interface», Strasburgo
- «E-crime Congress», Londra
- Riunione di esperti dell'ONU, Vienna
- Conferenza OSCE «Cybersecurity and Cybercrime», Vienna
- Simposio «Neue Technologien», BKA, Wiesbaden
- «Fighting Cybercrime : cooperation between law enforcement agencies and the internet industry», Accademia di Diritto Europeo, Treviri
- «Child Sexual Exploitation Experts Conference», Europol, L'Aia

⁹ Distributed Denial of Service

12. Cooperazione e contatti

12.1 Collaborazione con altri servizi della Confederazione

Nel 2011 SCOCI ha lavorato a stretto contatto con altri servizi della Confederazione nel settore della lotta alla criminalità su Internet. In seno a fedpol, SCOCI collabora intensamente con i commissariati Pedocriminalità/pornografia, Indagini Tecnologie dell'informazione, Protezione dello Stato e Inchieste mascherate della Polizia giudiziaria federale nonché con la divisione principale CIP. In virtù della convergenza nelle tematiche trattate e dei sei posti approvati nel 2011 dal Consiglio federale per la lotta alla pedocriminalità, si è sviluppata una collaborazione particolarmente intensa con il commissariato Pedocriminalità/pornografia.

Nell'anno in esame, SCOCI ha sviluppato e intensificato vari contatti, come pure la collaborazione con diversi servizi di altri Dipartimenti della Confederazione, tra cui la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), l'ambito direzionale Assistenza giudiziaria internazionale dell'Ufficio federale di giustizia (UFG), l'Ufficio federale della comunicazione (UFCOM), Swissmedic e la Commissione delle lotterie (Comlot).

Nell'anno in esame, la collaborazione con la Prevenzione svizzera della criminalità (PSC) è stata ulteriormente rafforzata in seguito alla decisione di accogliere SCOCI, come rappresentante di fedpol, in seno alla commissione speciale della PSC.

12.2 Riunioni di lavoro e scambi di esperienze con i Cantoni

Nel 2011 SCOCI ha avuto diversi contatti con vari corpi di polizia e ministeri pubblici cantonali. Oltre al normale scambio di esperienze, sono state organizzate, nel quadro di inchieste mascherate e del progetto NDHS, diverse riunioni di lavoro.

Nell'ambito della Strategia nazionale per la Cyber Defence e in seguito a diverse richieste del mondo politico in materia di cibercriminalità, SCOCI ha potuto stabilire un buon rapporto di collaborazione ed un regolare scambio d'informazioni con il Congresso delle forze di polizia svizzere sull'informatica (Schweizerische Polizei Informatik Kongress, SPIK).

12.3 Collaborazione con Action Innocence (AIG)

Da diversi anni SCOCI collabora strettamente con l'organizzazione non governativa Action Innocence (AIG). Grazie al sostegno attivo e al supporto finanziario offerto dall'AIG, negli ultimi anni è stato possibile portare avanti e sviluppare ulteriormente il progetto per il monitoraggio delle reti di peer to peer. La collaborazione con l'AIG assume un'importanza ancora maggiore, se si considera che la maggioranza delle ricerche attive condotte da SCOCI sono rese possibili dal software per il monitoraggio delle reti P2P, messo a disposizione dall'ONG. L'AIG sostiene inoltre SCOCI, sviluppando ulteriori progetti nell'ambito della lotta alla pedocriminalità.

12.4 Collaborazione con il settore privato (partenariato pubblico-privato, PPP)

La collaborazione di SCOCI con il settore privato sta assumendo un ruolo sempre più determinante nella lotta alla criminalità in rete. Nell'anno in esame si sono tenuti diversi incontri con i rappresentanti del settore che opera con Internet e le nuove tecnologie. Particolarmente positivi si sono rivelati i contatti allacciati con diversi fornitori di servizi Internet. Tale collaborazione è decisiva per effettuare accertamenti su persone sospette e su connessioni (indirizzi IP) nel quadro di indagini preliminari o di polizia. Per combattere la cybercriminalità tutti gli attori coinvolti devono agire rapidamente e in modo interattivo.

12.5 Visitatori esterni

Durante l'anno in esame, vari visitatori esterni si sono interessati all'attività di SCOCI. Queste visite consentono ai collaboratori di SCOCI di presentare il proprio lavoro e di attirare l'attenzione dei visitatori sulle relative tematiche e problematiche. Diversi giornalisti hanno inoltre visitato SCOCI nel 2011 in vista della redazione di un articolo. In occasione di tali visite, i giornalisti hanno avuto la possibilità di conoscere da vicino le attività svolte dagli specialisti di SCOCI.

12.6 Collaborazione internazionale

Oltre alle conferenze internazionali e ai gruppi di lavoro menzionati nel capitolo 8.2, SCOCI ha mantenuto contatti con diversi partner esteri. Tali scambi servono in primo luogo a sviluppare procedure congiunte volte a migliorare la collaborazione tra le parti. Da tempo la cooperazione internazionale non si concentra più soltanto sulla lotta alla pedocriminalità, ma verte sempre più anche su temi quali la lotta alla criminalità su Intranet in senso stretto e alla criminalità economica. Lo scambio diretto con le autorità estere di perseguimento penale si rivela proficuo soprattutto nell'ambito degli interventi operativi (p. es. inchieste mascherate, cfr. cap. 9.2).

13. Glossario

Adult check	Sistema per limitare l'accesso a un sito web esclusivamente agli utenti maggiorenni.
Chat	Comunicazione elettronica in tempo reale, solitamente via Internet.
Cloud Computing	Utilizzo della memoria, delle capacità di calcolo dei computer e di server sparsi in tutto il mondo, connessi tra loro attraverso una rete (Internet). Le applicazioni e i dati non si trovano più sul computer locale, ma in una cosiddetta nuvola (cloud) composta da un numero determinato di server distanti fra loro e interconnessi grazie a dei collegamenti a banda larga di eccellente qualità, indispensabile per la fluidità del sistema.
Ciberbullismo	Si parla di ciberbullismo quando sono utilizzati moderni mezzi di comunicazione come cellulari, chat, reti sociali informatiche quali Netlog o Facebook, portali video, forum o blog per pubblicare testi, immagini o filmati diffamatori con cui denigrare, offendere o molestare una determinata persona. Le aggressioni in genere si ripetono nel tempo o persistono durante un periodo prolungato e le vittime sono particolarmente indifese.
One-Click-hosting	Servizi web che offrono agli utenti spazio per salvare i propri file (soprattutto video o audio). Inoltre, viene fornito un URL semplice che permette d'accedere ai file per poterli scaricare.
Peer to peer	Modello di rete informatica per lo scambio di file tra utenti e con terze persone (peer).
Phishing	Metodo utilizzato per ottenere in modo fraudolento i dati personali dell'utente (password, nome utente ecc.), soprattutto imitando nella grafica e nel contenuto siti Internet autentici.
Pornografia dura	Rappresentazione di atti sessuali con fanciulli (pedofilia, pedopornografia), animali, escrementi umani o atti violenti. (art. 197 numero 3 CP).
Proxy	Un proxy è un server che funge da tramite tra un client (l'utente) e un server (il sito web che s'intende consultare).
Redirect Service	Un redirect service permette di beneficiare di un URL semplificato per accedere a un contenuto (URL più semplice da ricordare o comunque più breve rispetto a quello del contenuto verso cui si viene deviati).
Spam	Invio di enormi quantità di e-mail indesiderate per fini pubblicitari, e talvolta anche per installare malware sul computer dell'ignaro destinatario.
Streaming	Modalità di trasmissione di dati audio e video che vengono trasmessi di continuo, senza bisogno di scaricare per intero i contenuti (permettendo dunque la lettura del contenuto in diretta).
URL	(Uniform Resource Locator) sequenza di caratteri utilizzata per indirizzare gli utenti verso le risorse del web (indirizzo web).
Valore di hash	Valore attribuibile in modo univoco a un'immagine (impronta digitale).

14. Tendenze del 2011

L'evoluzione del numero di segnalazioni pervenute a SCOCI permette solo in minima parte di trarre conclusioni in merito allo sviluppo effettivo della criminalità su Internet o ai contenuti illegali diffusi in rete. Tutt'al più consente di rilevare tendenze relative alla disponibilità della popolazione a segnalare eventuali casi di cybercriminalità e al modo in cui la società percepisce la criminalità su Internet. I motivi per il calo delle segnalazioni trasmesse tramite il modulo online possono essere molteplici. È ipotizzabile che alcuni tipi di criminalità su Internet siano diventati talmente ordinari che la popolazione li considera banali e le vittime rinunciano a segnalarli a SCOCI. Tuttavia, le segnalazioni dei cittadini sono essenziali per poter valutare la portata del fenomeno e affrontarlo mediante l'intervento delle autorità di perseguimento penale o l'adozione di altre misure.

La flessione delle comunicazioni è inoltre riconducibile al fatto che i contenuti pornografici sono sempre meno accessibili al pubblico. I pedofili si servono consapevolmente di piattaforme protette o difficilmente accessibili quali forum, gruppi e reti sociali, che permettono loro di scambiare materiale pedopornografico in modo più discreto e anonimo. Considerando il rapido sviluppo tecnologico di Internet, è possibile ipotizzare che tale tendenza andrà sempre più accentuandosi.

Per tale ragione, le indagini condotte su Internet dalla polizia, e in particolare le inchieste mascherate, stanno assumendo un'importanza sempre maggiore per individuare e accertare i reati compiuti online.

Si prevede anche un aumento costante dei casi di truffa commessi da persone operanti dall'estero. Questa tendenza, riscontrata già negli ultimi anni, è stata osservata anche nell'anno in esame. Alla luce di tali considerazioni, è opportuno condurre un'attività di prevenzione e sensibilizzare la popolazione all'uso corretto di Internet.

Per contrastare con efficacia tale fenomeno, come pure tutte le forme di cybercriminalità, è indispensabile la collaborazione di tutte le parti coinvolte (governi, autorità di perseguimento penale, provider e autorità regolatrici). SCOCI partecipa già a diversi gruppi di lavoro nazionali e internazionali incentrati sulla lotta a reati specifici. Si presume infine che la collaborazione tra le istituzioni pubbliche e private (partenariato pubblico-privato) finalizzata a contrastare la criminalità su Internet assumerà un ruolo sempre più decisivo.