KOBIK SCOCI CYCO

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 2013

10 ANNI DI ATTIVITÀ

Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI)
Nussbaumstrasse 29
3003 Berna
www.scoci.ch
www.cybercrime.ch

Pubblicazione: TRADUZIONE DELLA VERSIONE DEFINITIVA del 26.02.2014
(pubblicazione prevista il 27 marzo 2014)

Fonti delle illustrazioni: Thinkstock, SCOCI

PREFAZIONE

del consigliere di Stato Christoph Neuhaus,
presidente del comitato direttivo dello SCOCI

Ogni cosa è in continuo mutamento, tranne il principio stesso del mutamento. Lo sosteneva già Eraclito ai tempi degli antichi greci. Chi la dura la vince – e chi non avanza indietreggia. Chi di noi non conosce queste sagge parole, parole che nel caso del Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI) suonano ancora più vere. Primo perché, come sostiene uno studio condotto da ibusiness.de, un anno Internet equivale a quattro anni di vita, e secondo perché lo SCOCI può ormai volgere lo sguardo a dieci anni di esperienza. Visionario e un passo davanti a tutti sin dall'inizio, lo SCOCI continuerà quindi a guardare avanti e ad agire di anticipo.

Oggi come oggi, più di otto cittadini svizzeri su dieci hanno l'abitudine di navigare più volte alla settimana nel World Wide Web. Per le autorità di polizia e giudiziarie si sono così dischiusi nuovi settori di attività e campi di intervento. Quest'ultime sono già chiamate a garantire offline, con le risorse a loro disposizione, la sicurezza di circa otto milioni di persone. Quali sono le conseguenze per queste autorità se altri 2,7 miliardi di persone sparse nel mondo possono accedere ugualmente ai sistemi svizzeri con un semplice clic? E quali sarebbero le conseguenze se, come previsto da Europol, entro il 2017 queste persone diventassero addirittura 3,5 miliardi e se una parte, pur minima, di esse fosse mossa da cattive intenzioni?

Nell'anno in rassegna è stato scoperto il primo *botnet* costituito per il 25 per cento da «oggetti», per l'esattezza frigoriferi e altri elettrodomestici. Che cosa succederà se nel 2020 circa 200 miliardi di questi «oggetti» saranno collegati a Internet? Che cosa comporterà tutto ciò per ciascuno di noi, per la piazza economica svizzera e per le autorità di perseguimento penale? Con il passaggio dal Servizio di analisi e prevenzione alla Polizia giudiziaria federale, lo SCOCI è assurto al ruolo di polizia giudiziaria con competenze in ambito di criminalità informatica ed è divenuto un partner riconosciuto di autorità inquirenti internazionali quali l'European Cybercrime Center di Europol (EC3) e l'Interpol Global Complex for Innovation (IGCI) con sede a Singapore. Sono state così poste le basi per una cooperazione internazionale efficace in materia di lotta a questa nuova forma di criminalità. La Svizzera dispone in tale ambito delle conoscenze, delle risorse e di premesse di per sé ideali.

A livello federale, lo SCOCI dovrà sottoporre al Consiglio federale entro la fine del 2016 un documento programmatico, elaborato sulla base della misura 6 della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi, per la gestione di una panoramica svizzera dei casi e il coordinamento di affari di portata intercantonale. Si tratta di una sfida su due fronti: da un lato, occorrerà trovare una soluzione atta a contrastare efficacemente la cibercriminalità organizzata e internazionale che risulti accettabile per tutti e sia al contempo interessante sotto il profilo finanziario, soprattutto in un periodo in cui i tagli al bilancio sono all'ordine del giorno; dall'altro, sarà necessario adottare un approccio fondato sulla ripartizione del lavoro per evitare che eventuali questioni di competenza tra le autorità di perseguimento penale cantonali e federali rischino di mettere in discussione lo stesso progetto. Le opportunità offerte dalla misura 6 della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi non vanno sacrificate nel nome della salvaguardia del federalismo; tale misura non comporta infatti alcun rischio per il nostro federalismo, ma solo benefici.

Domande su domande, ardue sfide, molto lavoro – lo SCOCI affronta il prossimo decennio con il consueto vigore e la necessaria immaginazione, e sempre con lo sguardo puntato al futuro (digitale)!

Indice

1. L’essenziale in breve

- Nel 2013 sono pervenute allo SCOCI complessivamente 9208 segnalazioni tramite l’apposito modulo online, ovvero l’11,7 per cento in più rispetto all’anno precedente.

- Il 61 per cento delle segnalazioni pervenute riguardava reati contro il patrimonio. Anche nel 2013 questa categoria di reati registra un ulteriore incremento rispetto ai reati contro l’integrità sessuale, confermando una tendenza già delineatasi negli anni precedenti.

- In totale, 356 segnalazioni sono sfociate direttamente, in virtù della loro rilevanza penale, in una denuncia ad autorità e organizzazioni nazionali o estere.

- Nell’anno in rassegna, le ricerche attive condotte nelle reti *peer to peer* (P2P) hanno permesso allo SCOCI di identificare 238 persone coinvolte nello scambio attivo di materiale pedopornografico.

- Le indagini preliminari sotto copertura e le indagini secondo il Codice di procedura penale (CPP) condotte dallo SCOCI nel 2013 sono sfociate in 17 casi nella trasmissione di una denuncia al Cantone competente e in altri 176 casi nella trasmissione di una denuncia ad autorità di perseguimento penale estere.

- Lo SCOCI ha avviato con successo i lavori di attuazione della misura 6 della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC). Nell’anno in rassegna si è già potuto procedere a un’analisi di progetto dettagliata e alla definizione dell’organizzazione di progetto.

- Nel contesto del suo decimo anniversario di attività, il 22 dicembre 2013 lo SCOCI ha inaugurato due nuovi canali di comunicazione, uno su Facebook (http://www.facebook.com/1406807632890549) e uno su Twitter (@KOBIK_Schweiz).

2. Retrospettiva sui 10 anni di attività dello SCOCI

2000–2002: nascita dell'idea

Nel giugno 2000 la Conferenza dei Comandanti delle Polizie Cantonali dell Svizzera (CCPCS) istituisce il Gruppo di lavoro intercantonale per la lotta contro gli abusi nel settore delle tecniche d'informazione e di comunicazione (Gruppo di lavoro BEMIK[1]) con l'incarichi di studiare in modo approfondito i presupposti e le condizioni quadro per la creazione di un servizio nazionale di monitoraggio e di presentare proposte concrete a tal fine. Di fronte all'urgente bisogno di coordinamento in materia di polizia, il Gruppo di lavoro BEMIK, presieduto da Adrian Lobsiger, attuale direttore supplente di fedpol, propone una serie di misure concrete e raccomanda all'unanimità di costituire un servizio nazionale incaricato di coordinare gli sforzi nella lotta contro la criminalità su Internet.

Alla luce dei risultati presentati dal Gruppo di lavoro BEMIK, nella primavera del 2001 il Dipartimento federale di giustizia e polizia (DFGP) e la Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP) decidono di procedere fianco a fianco nella lotta contro la criminalità su Internet. In un accordo amministrativo vengono così definiti mandato, struttura organizzativa e finanziamento di un servizio nazionale di coordinazione.

Il comitato direttivo e l'assemblea plenaria della CDDGP si esprimono unanimemente a favore dell'attuazione dell'accordo. Con lettera del 4 febbraio 2002, il presidente della CDDGP invita i Cantoni a stanziare le risorse finanziarie necessarie all'attuazione di tale progetto. Tutti i Cantoni, salvo Zurigo, dichiarano la loro adesione al progetto. Il 20 febbraio 2002 il Consiglio federale ribadisce a sua volta la propria intenzione di introdurre insieme ai Cantoni, a partire dal 1° gennaio 2003, un servizio nazionale di coordinazione per contrastare con maggiore efficacia la criminalità su Internet.

1° gennaio 2003: debutto

Il 1° gennaio 2003 lo SCOCI apre i battenti e pubblica su Internet la prima versione del modulo di comunicazione in quattro lingue (immagine a destra). Oltre al modulo, il sito www.cybercrime.ch contiene oggi anche informazioni di contorno riguardanti lo SCOCI e la criminalità su Internet in generale. L'esordio dello SCOCI è oggetto di ampia risonanza sui media e desta un vivo interesse in particolare da parte dei media elettronici e della stampa specializzata. In un primo bilancio, allestito al termine dei primi sei mesi di attività, lo SCOCI annuncia il suo esordio positivo con un comunicato stampa.

[1] AG BEMIK : Arbeitsgruppe zur Bekämpfung des Missbrauchs von Informations- und Kommunikationstechnologien, ossia Gruppo di lavoro per la lotta contro gli abusi in materia di tecnologie dell'informazione e della comunicazione.

Maggio 2003: introduzione delle ricerche attive

A inizio maggio il Servizio di coordinazione incomincia il monitoraggio attivo di Internet incentrato sulle reti *peer to peer*. La prima fase del monitoraggio consiste nel ricercare file illegali condivisi da utenti con indirizzo IP svizzero. Una volta terminate queste attività preliminari, i casi sospetti vengono denunciati al Cantone competente.

9 gennaio 2004: pubblicazione del primo rapporto annuale

Il primo rendiconto consta di una breve retrospettiva sulla genesi dello SCOCI, sul reclutamento del suo team, sulla costituzione del comitato direttivo e di un capitolo che riporta i primi dati statistici e commentati in merito alle segnalazioni e alle attività di monitoraggio. Da questo primo rapporto si evince che nel primo anno di attività la popolazione ha inviato allo SCOCI 6457 segnalazioni e che il monitoraggio attivo ha consentito di trasmettere oltre 100 denunce ai Cantoni.

2004: prima fase di riorganizzazione

Per rafforzare e centralizzare la conduzione del team SCOCI, si decide di integrare nel Servizio di analisi e prevenzione (SAP) anche il settore Clearing SCOCI, che finora era accorpato alla Polizia giudiziaria federale.

2005: integrazione nella sezione MELANI/Criminalità informatica

La riorganizzazione strutturale del settore Clearing SCOCI si conclude con il raggruppamento dei settori Analisi e Clearing dello SCOCI e della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) nella nuova sezione MELANI/Criminalità informatica. In seguito all'adesione del Cantone di Zurigo, il team incaricato del monitoraggio viene potenziato con l'assunzione di un ulteriore collaboratore, portando così a nove il numero dei suoi componenti.

2005–2006: sviluppo delle attività di prevenzione

Nel contesto della campagna nazionale «Stop alla pornografia infantile» avviata nel 2005, lo SCOCI collabora strettamente con il servizio intercantonale «Prevenzione Svizzera della Criminalità» (PSC) e partecipa a una serie di giornate di formazione e convegni. Dallo stesso contesto nasce anche il progetto «DNS-Blacklist», promosso nel 2007, che prevede il blocco di determinati siti web a carattere pedopornografico. Lo SCOCI diventa inoltre partner di Microsoft Svizzera per il programma di prevenzione «Security for Kids».

2006: accordo di cooperazione con la Polizia nazionale del Principato del Liechtenstein

In virtù di un accordo concluso con la Polizia nazionale del Principato del Liechtenstein, dal 2006 lo SCOCI fornisce servizi anche al Principato.

2007: realizzazione del progetto DNS-Blacklist

Nel 2007 viene introdotto in Svizzera il software di filtraggio Child Sexual Abuse Anti-Distribution, che consente di bloccare i siti Internet pedopornografici. Si tratta di un progetto basato su una cooperazione volontaria tra lo SCOCI e i principali provider di servizi Internet della Svizzera. Lo SCOCI si impegna a mettere a disposizione dei provider una lista costantemente aggiornata dei siti Internet con contenuti pedopornografici. Tale lista è allestita grazie alle segnalazioni provenienti dalla popolazione. Dal canto loro, i provider provvedono a bloccare i siti iscritti nella lista fondandosi sulle condizioni generali dei loro contratti.

2007: nuovo record di segnalazioni

Per lo SCOCI, il quinto anno di attività è caratterizzato da un netto aumento delle segnalazioni provenienti dalla popolazione. Il Servizio effettua un importante lavoro di selezione sulle oltre 10000 segnalazioni ricevute, consolidando il proprio ruolo di referente nazionale in materia di criminalità su Internet. L'aumento delle segnalazioni è ascrivibile all'incremento di casi di criminalità economica e all'assiduo impegno di singoli cittadini, alcuni dei quali inviano addirittura decine di segnalazioni al mese. Guardando ai primi cinque anni di attività, la direzione dello SCOCI stila un bilancio positivo: il Servizio nazionale per la lotta contro la criminalità su Internet è pronto ad affrontare le sfide future nel ruolo di centro di competenza nazionale.

2008: anno di metamorfosi

In vista dell'imminente integrazione nella Polizia giudiziaria federale, nel 2008 lo SCOCI opera una serie di adeguamenti a livello della struttura del personale e della dotazione tecnica. L'infrastruttura informatica viene ammodernata e potenziata con hardware e software supplementari.

2009: integrazione nella Polizia giudiziaria federale

Dal 1° gennaio 2009 MELANI e SCOCI sono due entità separate. Lo SCOCI è integrato nella Polizia giudiziaria federale, mentre il settore di MELANI finora subordinato a fedpol passa al neocostituito Servizio delle attività informative della Confederazione (SIC). Con l'integrazione nella Polizia giudiziaria federale, lo SCOCI assume viepiù anche compiti operativi e di polizia, in particolare il coordinamento di indagini su scala nazionale e internazionale nonché lo scambio d'informazioni di polizia giudiziaria. La nuova impostazione comporta diversi adeguamenti sul piano organizzativo e del personale. Si decide inoltre di concentrare i commissariati Monitoring e Clearing, in precedenza gestiti separatamente, in un nuovo commissariato SCOCI.

2010–2011: potenziamento delle ricerche attive

Lo SCOCI potenzia le «ricerche attive» generando così un maggior numero di denunce trasmesse ai Cantoni. Tra i temi dominanti che occupano il Servizio nel 2010 vi è soprattutto quello delle cosiddette inchieste sotto copertura.

A partire dal 1° gennaio 2011, la maggior parte degli agenti di polizia cantonali non è più autorizzata a condurre in assenza di sospetti e a titolo preventivo indagini mascherate (i.e., sotto coperutra) in Internet nei confronti di pedocriminali, poiché le leggi cantonali di polizia non forniscono una base legale sufficiente. La lacuna nella legislazione dei Cantoni è stata generata dall'introduzione del nuovo Codice di procedura penale svizzero (CPP; RS *312.0*).

Alcuni Cantoni, tra cui Svitto, Argovia e Obvaldo, riconoscono tempestivamente la necessità di intervenire ed adeguano le rispettive leggi di polizia per consentire il perpetrarsi delle indagini mascherate. Il DFGP trova a sua volta, insieme alla CDDGP, una soluzione che consente allo SCOCI di ampliare, in conformità a una nuova base giuridica, le proprie attività di monitoraggio in Internet nel campo della pedocriminalità. Grazie a un accordo sottoscritto con il Dipartimento della sicurezza del Cantone di Svitto, a partire dal 1° gennaio 2011 lo SCOCI è autorizzato a condurre inchieste mascherate a titolo preventivo su mandato dei Cantoni permettendogli così di sorvegliare le chat room. Nel 2013 l'operato del Servizio nel campo delle indagini sotto copertura si basa ancora sul diritto di polizia e su un'autorizzazione del Tribunale delle misure coercitive del Cantone di Svitto. Questa soluzione consente di colmare un vuoto legislativo che avrebbe permesso ai pedocriminali di imperversare liberamente su Internet.

2011: Raccolta nazionale di file e valori hash

L'allora Gruppo di lavoro «Banca dati di immagini» (in seguito rinominato «Gruppo di lavoro NDHS[2]») si era già occupato negli anni precedenti della creazione di una banca dati nazionale di immagini e valori hash relativi al materiale pedopornografico sequestrato. Nel 2010 lo SCOCI rimette mano al progetto e nel 2011 i lavori registrano un notevole avanzamento con lo sviluppo della rinominata Raccolta nazionale di file e valori hash. Lo SCOCI provvede alla formazione degli agenti dei corpi di polizia cantonali e riceve le prime raccolte di immagini dai Cantoni.

2011–2012: Strategia nazionale per la Cyber Defense (futura Strategia nazionale per la protezione della Svizzera contro i cyber-rischi)

Dal mese di maggio 2011 lo SCOCI siede in seno al gruppo di progetto «Strategia nazionale per la Cyber Defense» e difende gli interessi delle autorità cantonali e federali di perseguimento penale anche nell'ambito dell'attuazione della strategia.

Il 27 giugno 2012 il Consiglio federale approva la rinominata «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi» (SNPC). Con questa strategia, il Consiglio federale in collaborazione con le autorità, gli esponenti del mondo economico e i gestori di infrastrutture critiche, intende ridurre i cyber-rischi che minacciano l'economia e il benessere svizzeri. La conclusione dei lavori di attuazione è prevista nel 2017.

Gennaio 2012: Convenzione del Consiglio d'Europa sulla cibercriminalità

[2] NDHS : Nationale Datei- und Hashweresammlung, ossia Raccolta nazionale di file e valori hash.

Con la ratifica della Convenzione del Consiglio d'Europa sulla cibercriminalità, la Svizzera partecipa alla sempre più intesa lotta internazionale contro la criminalità su Internet. In Svizzera, la Convenzione e i necessari adeguamenti legislativi del diritto interno entrano in vigore il 1° gennaio 2012.

Ottobre 2012: realizzazione della Raccolta nazionale di file e valori hash

Nel mese di ottobre 2012 entra in servizio la Raccolta nazionale di file e valori hash. Tutti i test e gli adeguamenti del sistema vengono conclusi con successo.

Dicembre 2012: adesione della Svizzera alla Global Alliance against Child Sexual Abuse Online

Alcuni collaboratori dello SCOCI accompagnano la consigliera federale Simonetta Sommaruga a Bruxelles in veste di esperti per l'adesione della Svizzera alla Global Alliance.

Gennaio 2013: European Cybercrime Center in seno a Europol

Dal 2011 lo SCOCI è membro attivo dei Focal Point[3] CYBORG e TWINS di Europol. I due Focal Point sono ora integrati all'European Cybercrime Center (EC3) operativo dal 1° gennaio 2013. Il centro specializzato nella lotta alla criminalità su Internet, con sede presso il quartier generale d'Europol all'Aia, coadiuva gli Stati membri dell'UE a livello operativo e mette a disposizione le proprie conoscenze nell'ambito di inchieste condotte su scala europea. Il lavoro dei suoi inquirenti si concentra sulla criminalità informatica organizzata, in particolare sulla lotta contro lo sfruttamento sessuale dei minori in Internet e sull'accertamento di reati finanziari. Gli inquirenti IT dell'UE esaminano inoltre gli attacchi alle infrastrutture critiche e ai sistemi d'informazione e svolgono anche attività di analisi e valutazione con lo scopo di individuare e contrastare tempestivamente eventuali minacce.

2013: avviata l'attuazione della SNPC

Nel contesto dell'attuazione della misura 6 della SNPC è previsto che il DFGP, in collaborazione con i Cantoni, presenti entro la fine del 2016 un documento programmatico per la gestione di una «Panoramica dei casi e coordinamento dei casi di portata intercantonale». Tale documento chiarirà le questioni in merito ai punti di contatto con altri attori coinvolti nell'ambito della riduzione dei rischi informatici, al coordinamento con i lavori per la rappresentazione della situazione nonché alle risorse e gli adeguamenti giuridici necessari a livello federale e cantonale. Nel 2013 è stata tracciata un'analisi di progetto dettagliata e stabilita la sua organizzazione.

Dicembre 2013: attivazione di un profilo su Facebook e Twitter

Con l'attivazione dei profili su Facebook e Twitter, dal 22 dicembre 2013 lo SCOCI dispone di due nuovi canali di comunicazione.

[3] I *Focal Point* sono divisioni di Europol sorte dai preesistenti «Analysis Workfiles» (AWF) e incaricate in modo specifico del coordinamento e delle analisi nell'ambito di casi complessi a carattere internazionale.

3. Lo SCOCI, punto di contatto nazionale

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet funge da punto di contatto nazionale per le persone che intendono segnalare la presenza di contenuti sospetti su Internet. Dopo un primo esame e dopo aver salvaguardato i dati, lo SCOCI trasmette le segnalazioni penalmente rilevanti alle autorità di perseguimento penale competenti in Svizzera o all'estero.

3.1. Segnalazioni pervenute

Nel periodo compreso tra il 1° gennaio e il 31 dicembre 2013 lo SCOCI ha ricevuto in totale 9208 segnalazioni tramite l'apposito modulo online disponibile sul sito www.cybercrime.ch, ossia l'11,7 per cento in più rispetto all'anno precedente (8242 segnalazioni).

L'evoluzione del numero di segnalazioni pervenute non consente di trarre conclusioni in merito allo sviluppo effettivo, reale della criminalità su Internet o ai contenuti illegali diffusi in rete. La quantità di segnalazioni pervenute rispecchia semplicemente l'atteggiamento della società riguardo nei confronti della criminalità su Internet e la predisposizione della popolazione a collaborare attivamente con le autorità segnalandole i contenuti sospetti.

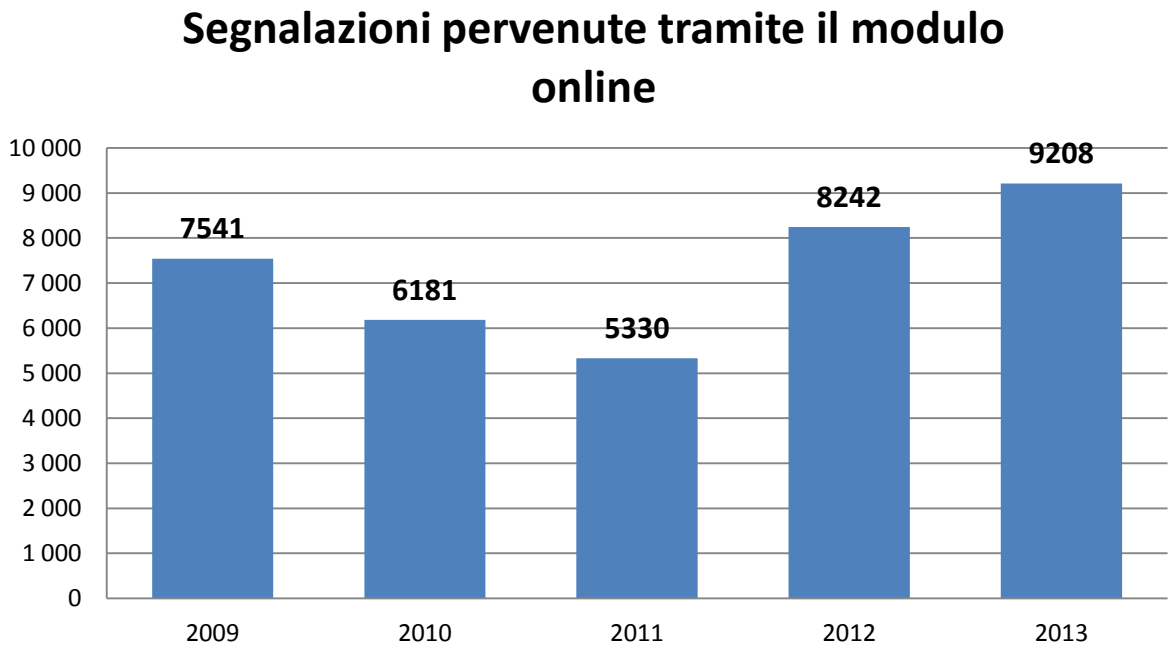


Grafico 1: Segnalazioni prevenute tramite www.cybercrime.ch – dati annuali

In media lo SCOCI ha ricevuto mensilmente 767 segnalazioni, con un picco massimo nel mese di maggio (1083 segnalazioni) e un minimo nel mese di settembre (585 segnalazioni). Le fluttuazioni registrate sono da ricondurre ad avvenimenti specifici e limitati nel tempo, come ad esempio la pubblicazione di un comunicato stampa da parte dello SCOCI.

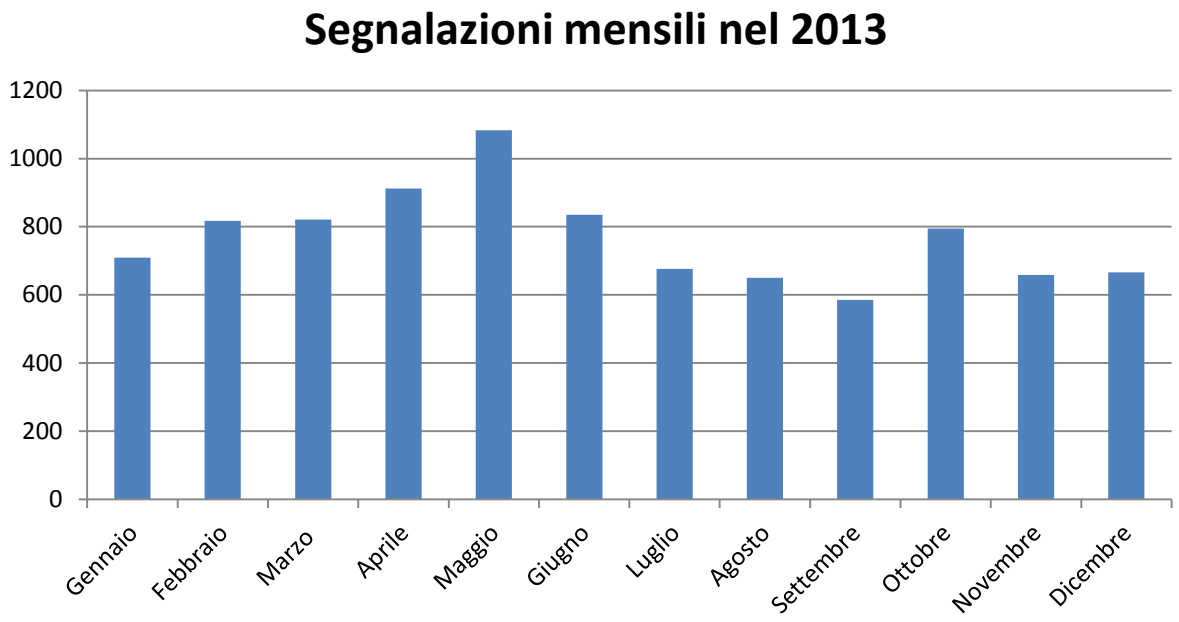


Grafico 2: Segnalazioni pervenute tramite www.cybercrime.ch – dati mensili (totale: 9208)

3.2. Contenuto delle segnalazioni

Nell'86 per cento delle segnalazioni ricevute (7910) è stata riscontrata una rilevanza penale. Le comunicazioni restanti riguardavano in particolare infrazioni alla LCSl[4] (290 segnalazioni), alla LDA[5] (24 segnalazioni), al CC[6] (40 segnalazioni), alla LStup[7] (14 segnalazioni) e alla LRD[8] (7 segnalazioni). Le segnalazioni risultate prive di rilevanza penale si aggirano attorno al dieci per cento.

I fatti segnalati possono essere suddivisi in due sottocategorie. La sottocategoria della criminalità su Internet in senso stretto che comprende i reati commessi con l'ausilio delle tecnologie di Internet o sfruttando le falle di queste. Ne fanno parte ad esempio i reati di *hacking*, gli attacchi DDoS (*Distributed Denial of Service*) o la creazione e la diffusione di software nocivi (*malware*). La criminalità su Internet in senso lato sfrutta invece le possibilità offerte da Internet, quali la posta elettronica o i server per lo scambio di dati, al fine di commettere dei reati. Rientrano ad esempio in questa sottocategoria l'invio di spam, i metodi di truffa utilizzati su piattaforme di annunci o la diffusione di materiale pornografico illegale.

Un numero elevato di segnalazioni riguardava fattispecie non perseguibili d'ufficio ma soltanto a querela di parte. In questi casi lo SCOCI indirizza l'autore della segnalazione alle competenti forze cantonali di polizia.

Il tendenziale aumento delle segnalazioni riguardanti reati contro il patrimonio si riconferma anche nel 2013. Complessivamente, il 60,7 per cento delle segnalazioni

[4] Legge federale del 19 dicembre 1986 contro la concorrenza sleale (LCSl; RS *241*).
[5] Legge federale del 9 ottobre 1992 sul diritto d'autore e sui diritti di protezione affini (LDA; RS *231.1*).
[6] Codice civile svizzero del 10 dicembre 1907 (CC; RS *210*).
[7] Legge federale del 3 ottobre 1951 sugli stupefacenti e sulle sostanze psicotrope (LStup; RS *812.121*).
[8] Legge federale del 10 ottobre 1997 relativa alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo nel settore finanziario (LRD; RS *955.0*).

pervenute riguardava questo titolo del Codice penale (art. 137–172ter CP). Al secondo posto, con il 20 per cento delle segnalazioni, seguono i reati contro l'integrità sessuale (art. 187–212 CP) che registrano dunque un netto calo, pari al 40,3 per cento, rispetto all'anno precedente.

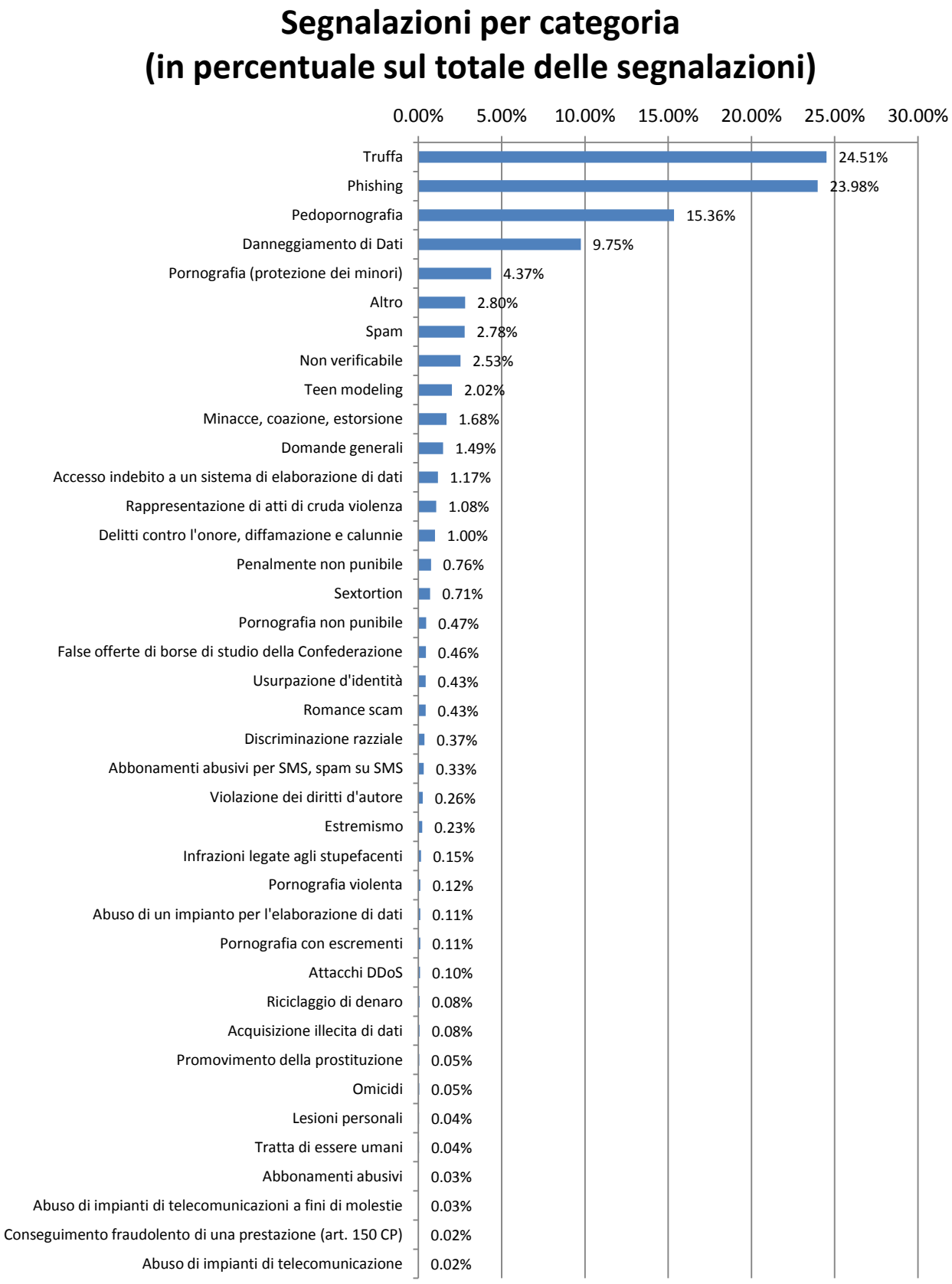


Grafico 3: Segnalazioni pervenute nel 2013 suddivise per categoria

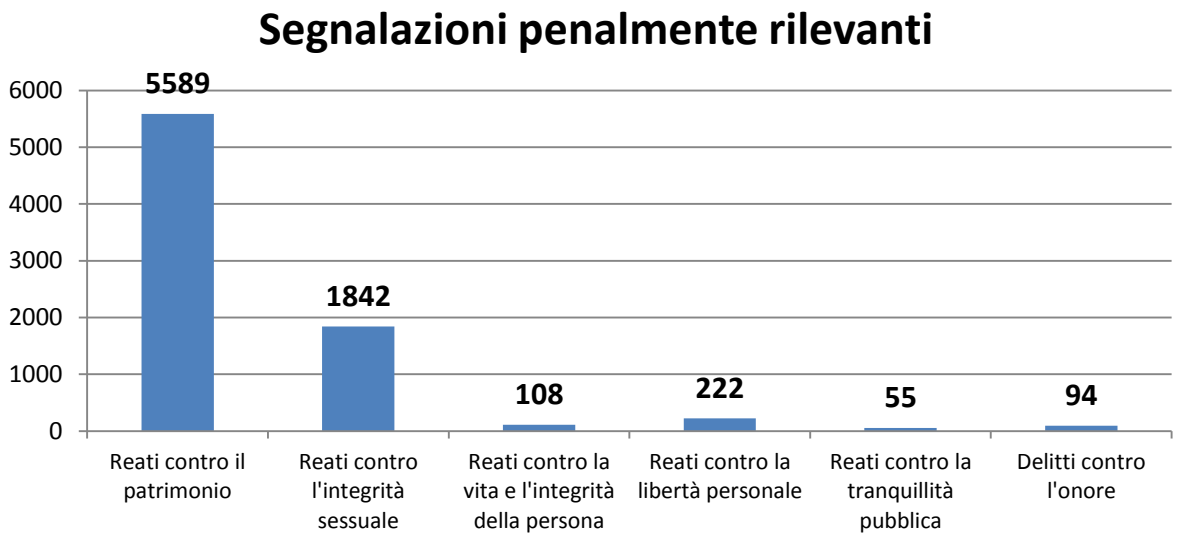


Grafico 4: Segnalazioni penalmente rilevanti pervenute nel 2013 (totale: 7910)

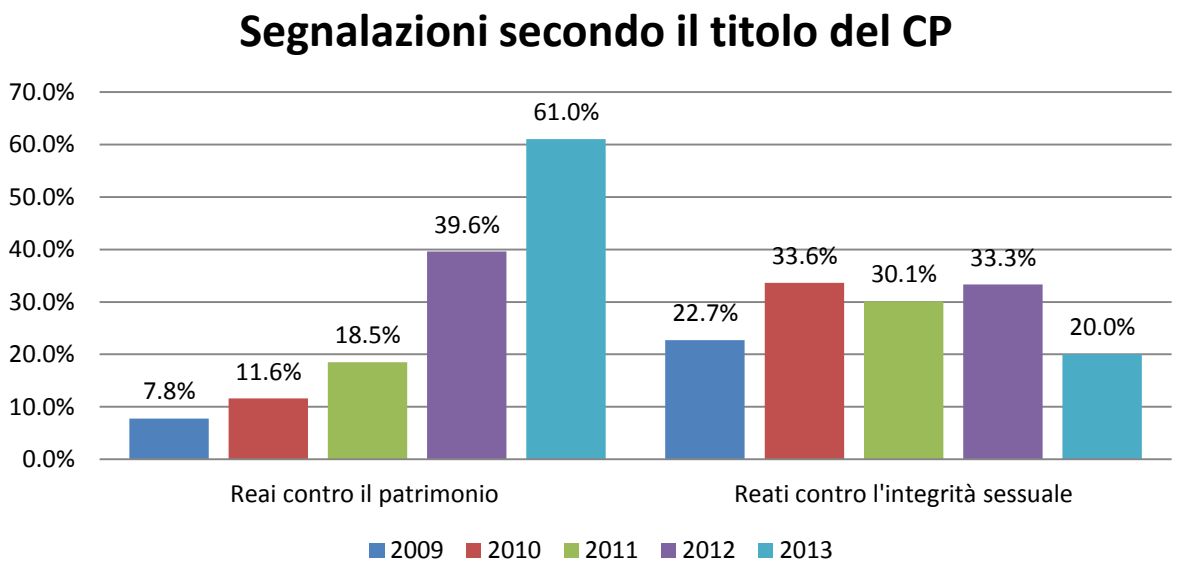


Grafico 5: Percentuale delle segnalazioni secondo il titolo del CP, 2009–2013

3.2.1. Reati contro il patrimonio

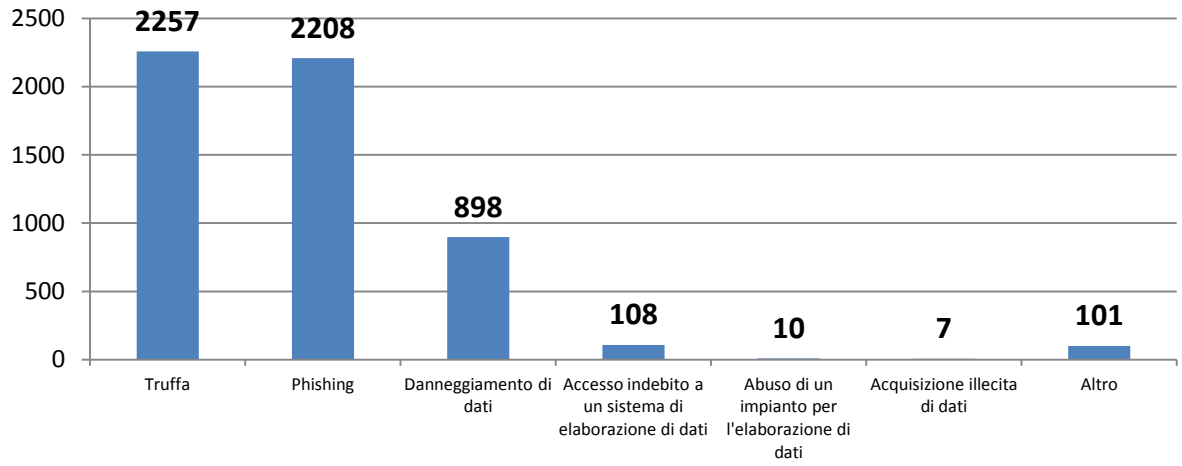


Grafico 6: Segnalazioni concernenti i reati contro il patrimonio pervenute nel 2013 (totale: 5589)

Nell'anno in rassegna la maggior parte delle segnalazioni riguardava reati contro il patrimonio che rappresentano il 60,7 per cento dei casi segnalati (5589). Con 2257 segnalazioni, la sottocategoria della truffa rappresenta il 25 per cento di tutte le comunicazioni pervenute. La gamma delle truffe segnalate è alquanto varia.

Sono aumentate in particolare le segnalazioni riguardanti tentativi di truffa sulle piattaforme di aste online e piccoli annunci, diretti tanto contro i potenziali interessati quanto contro gli inserzionisti. Si è inoltre constatato che i malintenzionati moltiplicano gli sforzi per conferire ai loro tentativi di truffa una maggiore credibilità. Creano ad esempio interi siti Internet per aziende di spedizione fittizie, con tanto di sistemi di localizzazione delle spedizioni inducendo così le vittime a credere il più a lungo possibile che la merce ordinata sia stata effettivamente spedita o si trovi ancora in fase di trasporto. I truffatori sono anche perfettamente informati sulla situazione corrente in Svizzera e sfruttano queste conoscenze. Approfittano ad esempio dell'attuale penuria di alloggi negli agglomerati per indurre le persone in cerca di casa, con inserzioni falsificate che propongono abitazioni a prezzi moderati a Zurigo o Basilea, a versare depositi per l'affitto di immobili inesistenti.

Anche le segnalazioni di tentativi di phishing registrano un netto aumento. Nel 2013 hanno raggiunto quota 2208, aumentando più del triplo rispetto all'anno precedente (662 segnalazioni). La variante più frequente tra i casi segnalati consiste nel tentativo, mediante l'invio di massa e indistinto di e-mail recanti link a siti fittizi che imitano l'aspetto di noti servizi Internet, di indurre le potenziali vittime a indicare i propri dati di utente (nome utente, password). All'incirca un quinto dei casi di phishing segnalati riguardava tentativi di impadronirsi dei dati di accesso a servizi di istituti bancari svizzeri.

Sul fronte della criminalità su Internet in senso stretto si osserva un ulteriore aumento delle segnalazioni di oltre il 20 per cento rispetto all'anno precedente. Si constata in particolare un netto incremento delle segnalazioni concernenti il reato di danneggiamento di dati (898 segnalazioni, + 124 per cento).

Per quanto riguarda quest'ultimo reato, uno dei *modus operandi* ricorrenti consiste nell'introduzione pianificata di programmi nocivi in computer di privati o aziende. Tra questi casi figura ad esempio l'introduzione di *ransomware* (contrazione dei termini inglesi *ransom*, ossia riscatto, e *software*). Una volta contagiato il computer della vittima, il *ransomware* impedisce qualsiasi ulteriore attività. Per sbloccare il computer, è richiesto alla vittima di acquistare un buono presso un fornitore di servizi di pagamento anonimo e di trasmettere ai truffatori il rispettivo codice affinché essi possano riscuotere il buono comperato dalla vittima. Nel corso del secondo semestre si è inoltre registrato un aumento delle segnalazioni su nuove tipologie di *ransomware*, i cosiddetti *CryptoLocker*, che crittografano i dati sul computer della vittima rendendoli inutilizzabili. Il *malware* informa la vittima che deve pagare un riscatto per ottenere la chiave di decrittazione che consentirebbe, a detta degli autori, di riottenere i dati.

Vi è stato anche un incremento dei casi di danneggiamento di siti web o infrastrutture di telecomunicazione appartenenti a piccole e medie imprese (PMI). Alcuni autori sono penetrati indebitamente in delle infrastrutture telefoniche VoIP (voce tramite protocollo Internet) per effettuare chiamate in Paesi africani e dell'America centrale o del Sud. Queste chiamate occasionano alle aziende colpite ingenti costi, nell'ordine di decine di migliaia di franchi. Un altro obiettivo di questi attacchi sono i dati dei clienti, quali indirizzi e-mail, numeri telefonici o dati di fatturazione, che vengono sottratti tramite le lacune nei sistemi di sicurezza dei siti web aziendali. Sebbene questo tipo di attacchi non comporti un danno finanziario diretto, causa però considerevoli danni indiretti per le operazioni necessarie al ripristino di eventuali backup e la correzione delle falle nei sistemi di sicurezza. Spesso questi attacchi diffondono sovente la sfiducia tra i clienti, causando un danno finanziario difficile da quantificare. Inoltre, i dati sottratti vengono spesso utilizzati per commettere ulteriori truffe, ad esempio per costruire identità fittizie o impossessarsi di account di posta elettronica di cui servirsi per inviare richieste fraudolente (p. es. per la «truffa dell'anticipo»).

3.2.2. Reati contro l'integrità sessuale

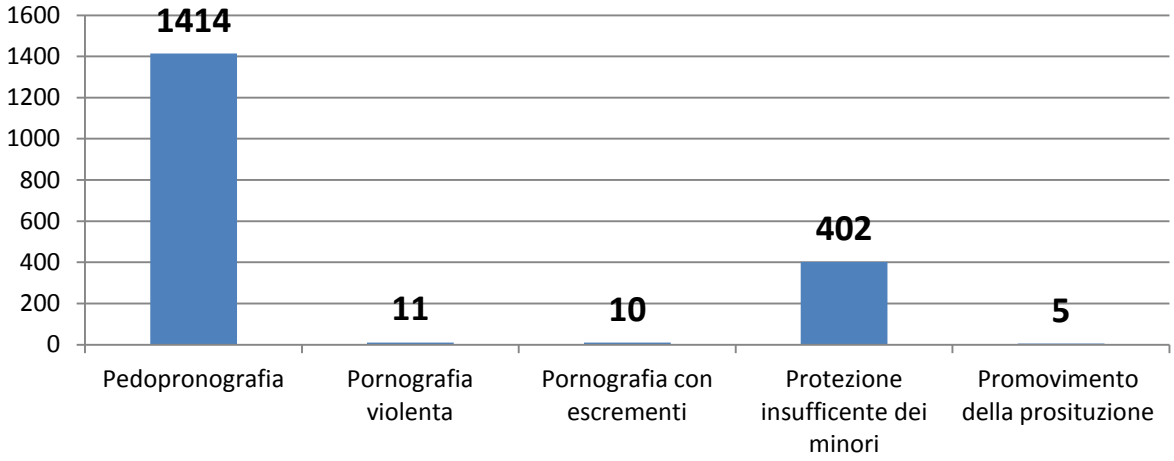


Grafico 7: Segnalazioni concernenti i reati contro l'integrità sessuale pervenute nel 2013 (totale: 1842)

Il numero di segnalazioni concernenti i reati contro l'integrità sessuale è diminuito quasi del 40 per cento, da 3083 nel 2012 a 1842 nell'anno in rassegna. Sono inoltre giunte 402 comunicazioni da parte di persone secondo cui determinati siti pornografici non bloccano in modo sufficiente l'accesso ai minori (l'anno precedente erano 307).

Il numero di segnalazioni relative a siti contenenti materiale pedopornografico ha registrato una netta flessione rispetto al 2012, passando da 2684 a 1414 segnalazioni (- 47 per cento).

3.2.3. Ulteriori reati

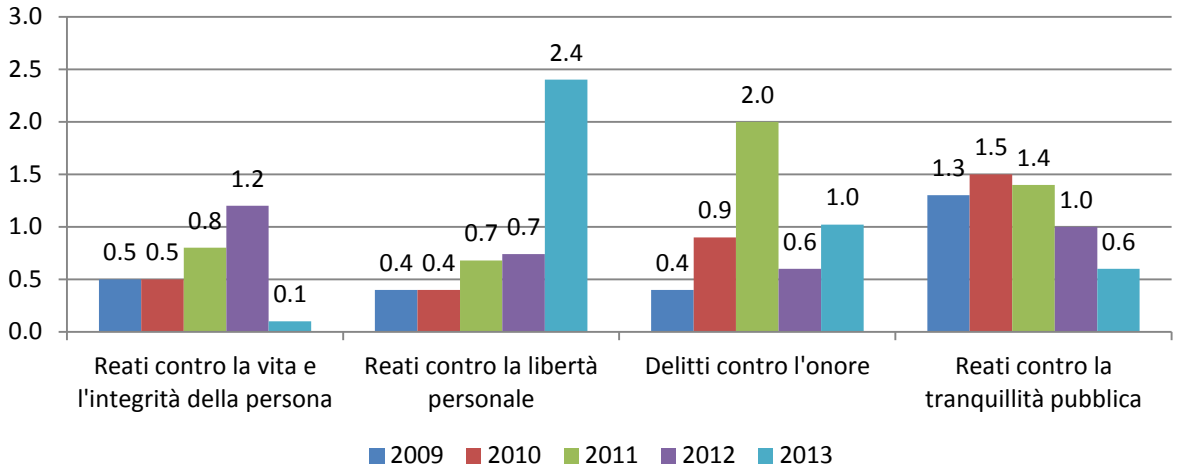


Grafico 8: Percentuale delle segnalazioni concernenti reati previsti in altri titoli del CP (2009–2013)

Circa il quattro per cento di tutte le segnalazioni pervenute riguarda reati contro la vita e l'integrità della persona, la libertà personale, la tranquillità pubblica e l'onore. Complessivamente, il 2,4 per cento delle segnalazioni concerneva reati contro la libertà personale. La maggior parte dei casi segnalati tratta di persone che attraverso siti di incontri o sui *social media* sono state indotte a compiere atti sessuali davanti alla webcam accesa. In seguito le vittime, perlopiù uomini, sono state contattate dagli autori e spinte a versare denaro sotto minaccia che in caso di mancato pagamento il filmato, registrato all'insaputa delle vittime, sarebbe stato diffuso su Internet. Anche quest'anno il numero di segnalazioni concernenti reati contro l'onore è relativamente modesto. Come nel 2012, in tale categoria non sembra pertanto esservi una tendenza all'aumento.

3.2.4. Conclusioni

Nel 2013 il numero di segnalazioni riguardanti reati contro il patrimonio è ancora aumentato di un terzo. Si conferma dunque la tendenza già osservata nel 2012. Al contempo, il numero di segnalazioni concernenti i reati contro l'integrità sessuale è diminuito di un terzo. Di conseguenza, nella graduatoria il numero complessivo delle segnalazioni concernenti le fattispecie contemplate dal titolo del CP sui reati contro l'integrità sessuale è ora superato dalle segnalazioni relative alle categorie di phishing e truffa.

3.3. Sviluppi

Sulla base delle segnalazioni trasmesse tramite l'apposito modulo online, lo SCOCI ha condotto diverse operazioni e adottato una serie di misure. Qui di seguito sono riportati i dati e le informazioni più significativi:

- tutte le 9208 segnalazioni pervenute sono state analizzate tempestivamente e valutate sotto il profilo della loro eventuale rilevanza penale;

- lo SCOCI ha risposto individualmente a 3457 segnalazioni su 9208;

- 35 segnalazioni sono state direttamente trasmesse, in virtù della loro rilevanza penale, al Cantone o all'autorità competente;

- 321 segnalazioni relative a siti Internet contenenti materiale penalmente rilevante sono state trasmesse alle autorità estere di perseguimento penale (tramite Interpol/Europol) o a organizzazioni attive nel settore della criminalità su Internet (p. es. all'associazione inhope);

- numerose segnalazioni sono state trasmesse all'interno di fedpol al commissariato Criminalità generale, organizzata e finanziaria e al commissariato Pedocriminalità/pornografia;

- i fenomeni oggetto di frequenti segnalazioni hanno determinato la pubblicazione di nove avvisi sul sito dello SCOCI www.cybercrime.ch. Grazie alla trasmissione degli avvisi a MELANI, alla «Prevenzione Svizzera della Criminalità» e ai media, il pubblico è stato messo in guardia dai pericoli attuali.

3.4. Casistica

Nel 2013 lo SCOCI è stato contattato da un provider svizzero di servizi *hosting* che aveva constatato che autori ignoti abusavano dei suoi servizi per gestire un commercio online di dati di carte di credito rubati. Il provider ha trasmesso volontariamente le informazioni rubate e i log file allo SCOCI che, a sua volta, ha inoltrato i dati a Europol. Lo European Cybercrime Center di Europol ha quindi eseguito l'analisi tecnica dei dati ricevuti e contattato gli istituti di credito interessati per far bloccare le carte coinvolte.

4. Ricerche attive da parte dello SCOCI (monitoring)

Lo SCOCI effettua anche ricerche in assenza di sospetti nelle aree di Internet meno accessibili al pubblico, nell'auspicio di ottenere così un effetto preventivo. Ogni anno il comitato direttivo dello SCOCI fissa un nuovo settore su cui incentrare le ricerche attive. Come negli anni precedenti, anche nel 2013 tali ricerche erano focalizzate sulla lotta alla pedocriminalità su Internet. Considerato l'ulteriore aumento delle segnalazioni in materia di reati economici, per il 2013 il comitato aveva espressamente dichiarato che nell'ambito delle sue ricerche lo SCOCI non doveva trascurare questo tipo di reati né la criminalità su Internet in senso stretto. Questa decisione ha avuto un impatto in particolare sull'attività di coordinamento e sulle indagini preliminari condotte dal Servizio (cfr. il capitolo 5.2).

Grazie alle ricerche attive, nel 2013 sono state allestite complessivamente 423 denunce. Questo dato registra una lieve flessione, pari al 6 per cento, rispetto all'anno precedente.

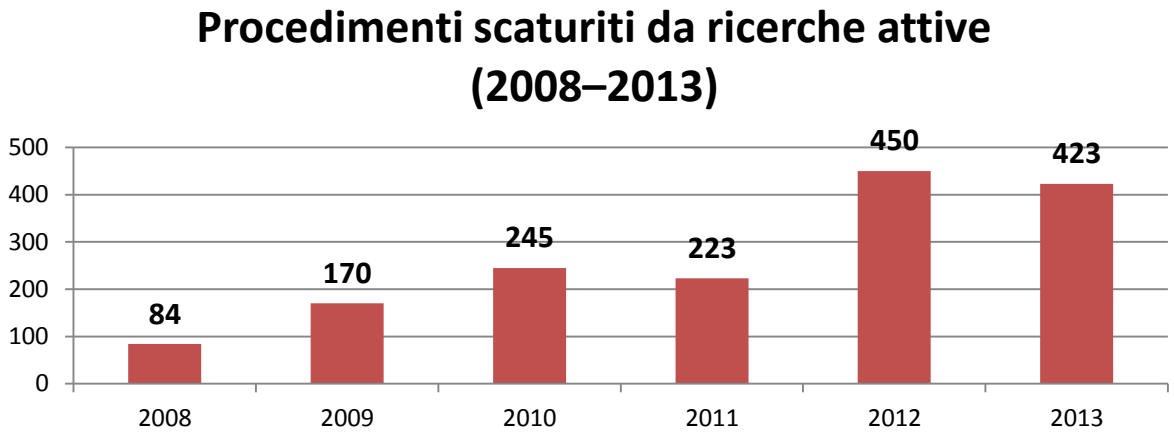


Grafico 9: Procedimenti penali scaturiti da ricerche attive (2008–2013)

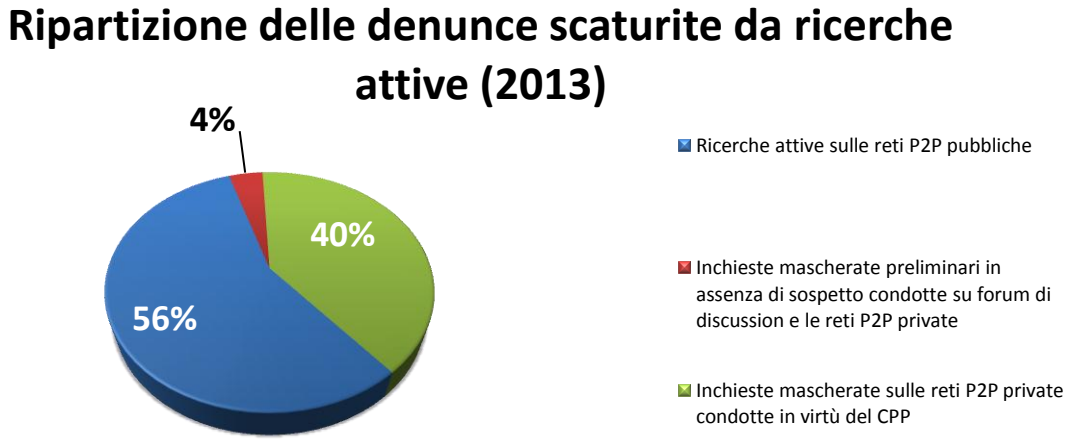


Grafico 10: Denunce suddivise in base al tipo di monitoraggio effettuato (totale: 423)

4.1. Ricerche attive nelle reti *peer to peer* (P2P)

Su 423 denunce, 238 sono scaturite dalle ricerche attive condotte dallo SCOCI in reti pubbliche *peer to peer* per la condivisione di file. Lo scopo delle denunce consiste nel giungere all'identificazione degli utenti Internet che condividono attivamente materiale a contenuto pedopornografico ai sensi dell'articolo 197 numero 3 e 3^{bis} CP. Rispetto all'anno precedente (450 denunce), il numero di casi segnalati è diminuito del 47,1 per cento. Il numero di denunce trasmesse ritorna dunque ai livelli del 2011, nonostante il monitoraggio sia stato condotto con la stessa intensità e gli stessi criteri del 2012.

Sebbene lo SCOCI focalizzi in modo specifico le proprie ricerche su utenti domiciliati in Svizzera, nell'anno in esame sono stati riscontrati, a causa di vincoli tecnici, anche reati commessi da dieci persone domiciliate all'estero. Lo SCOCI ha trasmesso i dati ottenuti via il canale Interpol agli Stati competenti.

4.2. Indagini preliminari sotto copertura svolte in assenza di sospetti

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 lo SCOCI, il Dipartimento della sicurezza del Cantone di Svitto e fedpol, disciplina le modalità secondo le quali i collaboratori dello SCOCI possono svolgere indagini preliminari mascherate per contrastare la pedocriminalità in rete[9]. In virtù di tale accordo i collaboratori dello SCOCI conducono inchieste preliminari mascherate esclusivamente su incarico e sotto l'egida della polizia cantonale di Svitto. In questo modo si garantisce che nel settore della pedocriminalità su Internet le ricerche attive (preliminari e non) possano continuare a essere svolte, oltre che dai Cantoni, da un servizio centrale nazionale.

Le indagini preliminari svolte sotto copertura dallo SCOCI hanno condotto nel 2013 all'allestimento e alla trasmissione di 17 denunce ai Cantoni competenti. Tre di queste sono scaturite da indagini condotte in alcune chat svizzere destinate in modo specifico ai minori. Nei tre casi, la fattispecie denunciata è di tentati atti sessuali con fanciulli ai sensi dell'articolo 187 CP.

Nei restanti 14 casi, le indagini preliminari sotto copertura che hanno portato alla denuncia sono state condotte su reti *private peer to peer* per la condivisione di file. Le reti di questo tipo si differenziano dalle reti *peer to peer* classiche per il fatto che i file vengono condivisi direttamente tra i computer coinvolti attraverso un collegamento diretto cifrato, invisibile al pubblico. La presa di contatto con tali utenti è pertanto disciplinata dalle disposizioni applicabili alle indagini preliminari sotto copertura. In questo tipo di indagini, la maggior parte delle denunce riguarda il possesso e la diffusione di materiale pornografico illegale ai sensi dell'articolo 197 numero 3 e 3^{bis} CP.

[9] Intervento ai sensi del § 9d dell'ordinanza del Cantone di Svitto del 22 marzo 2000 sulla polizia cantonale (PolV; SRSZ *520.110*).

4.3. Inchieste mascherate ai sensi del CPP

Per la prima volta dalla sua istituzione dieci anni fa, lo SCOCI è stato incaricato da alcuni pubblici ministeri cantonali di condurre inchieste mascherate ai sensi del Codice di procedura penale svizzero (CPP) nell'ambito di un procedimento cantonale. Le inchieste in questione, fondate sugli articoli 285*a* e seguenti CPP, si sono limitate esclusivamente a reti private *peer to peer*. In seguito alle inchieste condotte lo SCOCI ha allestito complessivamente 168 denunce, che sono state trasmesse alle autorità di polizia competenti in Svizzera come all'estero.

A causa dell'interconnessione globale delle comunità private *peer to peer* è difficile restringere il campo delle ricerche ai soli autori svizzeri. Lo SCOCI è quindi riuscito a identificare due autori svizzeri, mentre le restanti 166 denunce sono state trasmesse ad autorità di perseguimento penale estere nell'ambito dello scambio internazionale di informazioni in materia di polizia.

4.4. Riscontri dei Cantoni

Lo SCOCI trasmette ai Cantoni tutti i casi in cui sussiste un fondato sospetto di reato di loro competenza. Per disporre di una panoramica generale delle misure adottate dai Cantoni, invita questi ultimi a fornirgli informazioni sugli sviluppi dei casi che ha segnalato loro (misure di polizia adottate e/o esito di eventuali procedimenti giudiziari).

Per meglio illustrare gli sviluppi più recenti, i grafici seguenti considerano soltanto i riscontri pervenuti dai Cantoni nell'anno in rassegna. La stragrande maggioranza delle denunce (417) è scaturita dalle ricerche attive condotte nelle reti *peer to peer* nel 2012 e riguarda pertanto persone che hanno partecipato attivamente alla condivisione di materiale pedopornografico.

Grafico 11: Perquisizioni domiciliari nel 2013

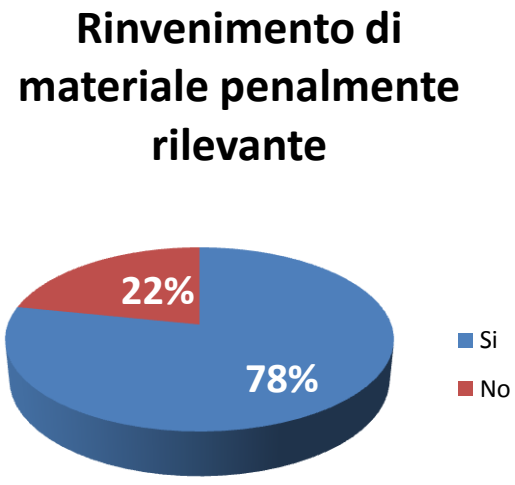


Grafico 12: Rinvenimento di materiale penalmente rilevante nel 2013

Come si evince dal grafico 11, nel 98 per cento dei casi le denunce trasmesse dallo SCOCI hanno indotto le autorità cantonali di polizia a effettuare una perquisizione domiciliare.

4.4.1. Riscontri da parte delle autorità cantonali di polizia

Nel 78 per cento dei casi, le perquisizioni domiciliari effettuate in seguito alle denunce trasmesse dallo SCOCI hanno portato al sequestro di materiale illegale. Negli altri casi, le cause del mancato sequestro di materiale sono molteplici. Per esempio, le reti *wireless* aperte e non protette o il trasferimento dei dati su servizi di *cloud computing* complicano l'acquisizione delle prove o l'identificazione precisa degli autori.

Nel 93 per cento dei casi il materiale di rilevanza penale sequestrato era di carattere pedopornografico. Questa percentuale elevata non sorprende, poiché le ricerche attive nelle reti *peer to peer* sono incentrate su questo tipo di reati e la maggior parte delle denunce deriva da queste ricerche. Occorre comunque rilevare che in più della metà dei casi sono state accertate anche altre forme di pornografia illegale (art. 197 CP; cfr. grafico 13). In oltre la metà delle perquisizioni domiciliari è stato sequestrato anche materiale pornografico raffigurante atti con animali.

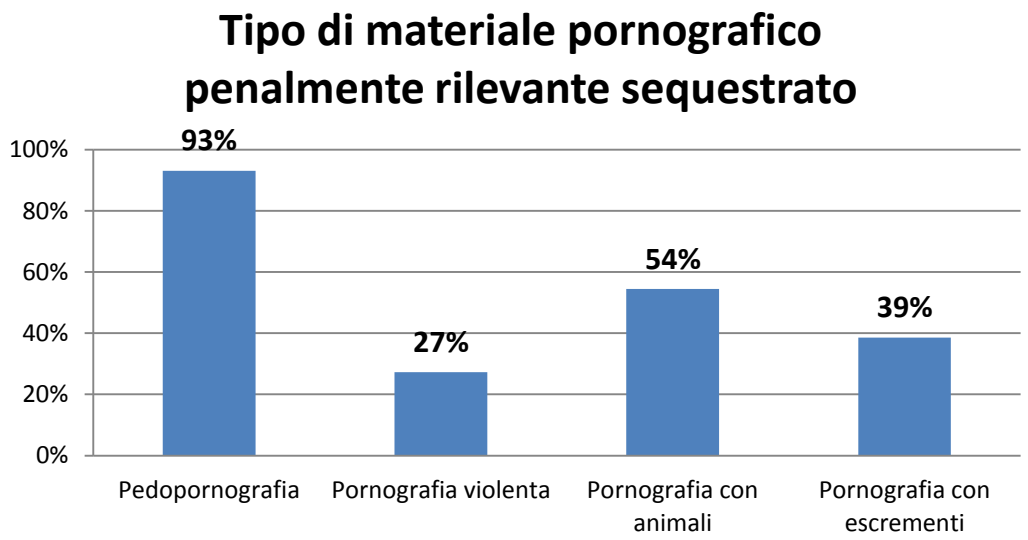
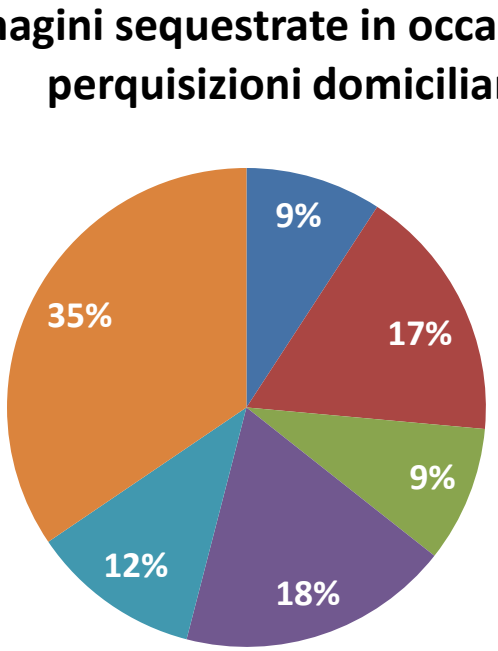
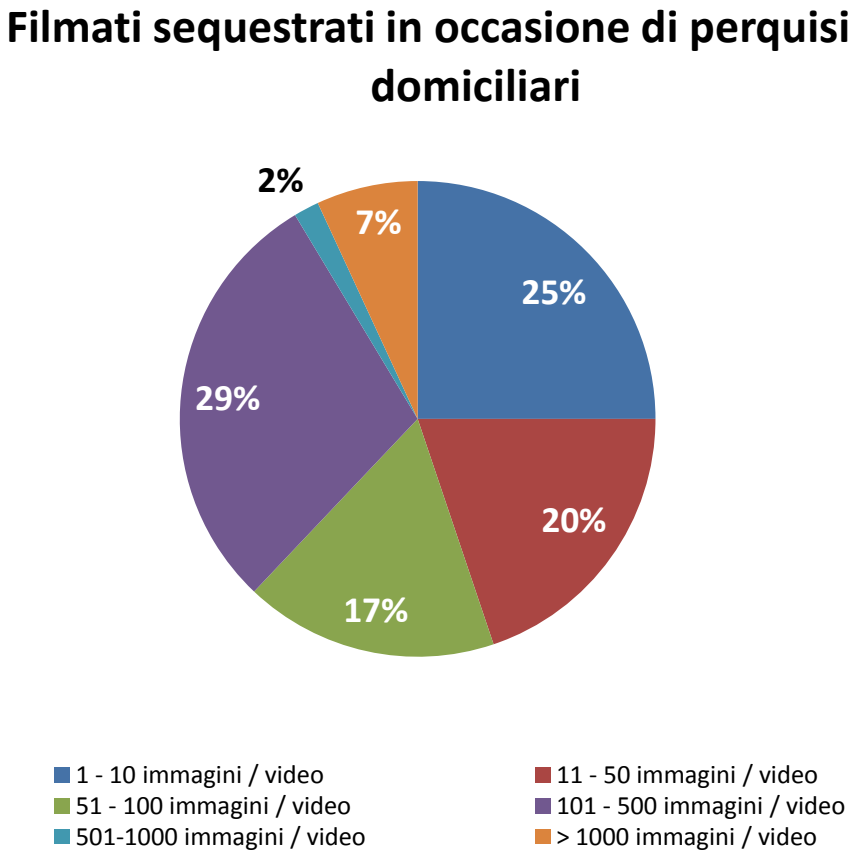


Grafico 13: Tipo di materiale pornografico penalmente rilevante sequestrato nel 2013 in occasione di perquisizioni domiciliari

Dai riscontri forniti dalle autorità cantonali di polizia emerge che le perquisizioni domiciliari andate a buon fine hanno portato nel 94 per cento dei casi al sequestro di filmati e nel 66 per cento dei casi al sequestro di materiale fotografico. In molti casi è stato scoperto e sequestrato materiale probatorio di entrambe le categorie. Nel complesso, le perquisizioni domiciliari hanno portato al sequestro di diversi milioni di filmati e immagini penalmente rilevanti.





Grafici 14 e 15: Panoramica delle immagini e filmati sequestrati

4.4.2. Riscontri delle autorità giudiziarie cantonali

Nel 91 per cento dei casi in cui le autorità giudiziarie cantonali hanno fornito un riscontro allo SCOCI, i procedimenti penali si sono conclusi con una condanna.

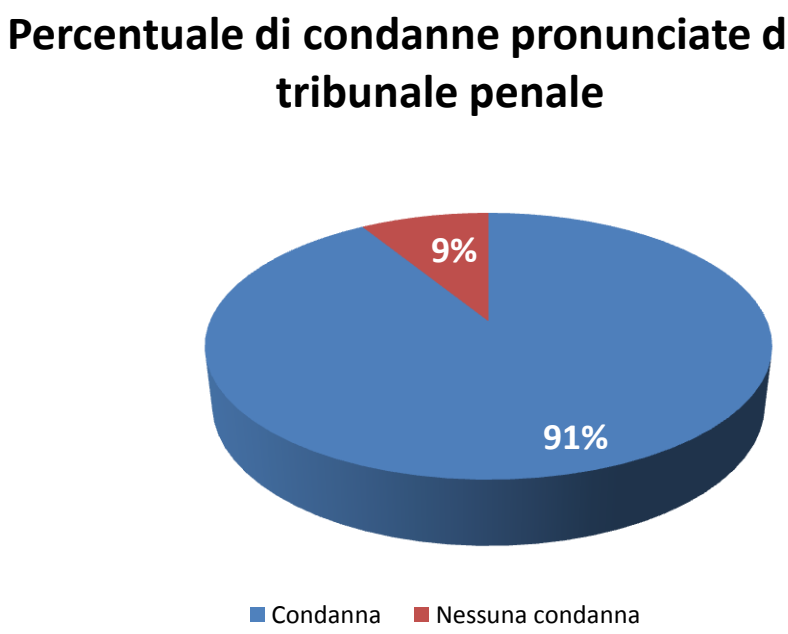


Grafico 16: Condanne penali pronunciate nel 2013

La maggior parte delle condanne è stata pronunciata per possesso di pornografia dura ai sensi del reato di pornografia previsto all'articolo 197 CP e in particolare alle fattispecie descritte ai numeri 3 e 3bis di tale disposizione.

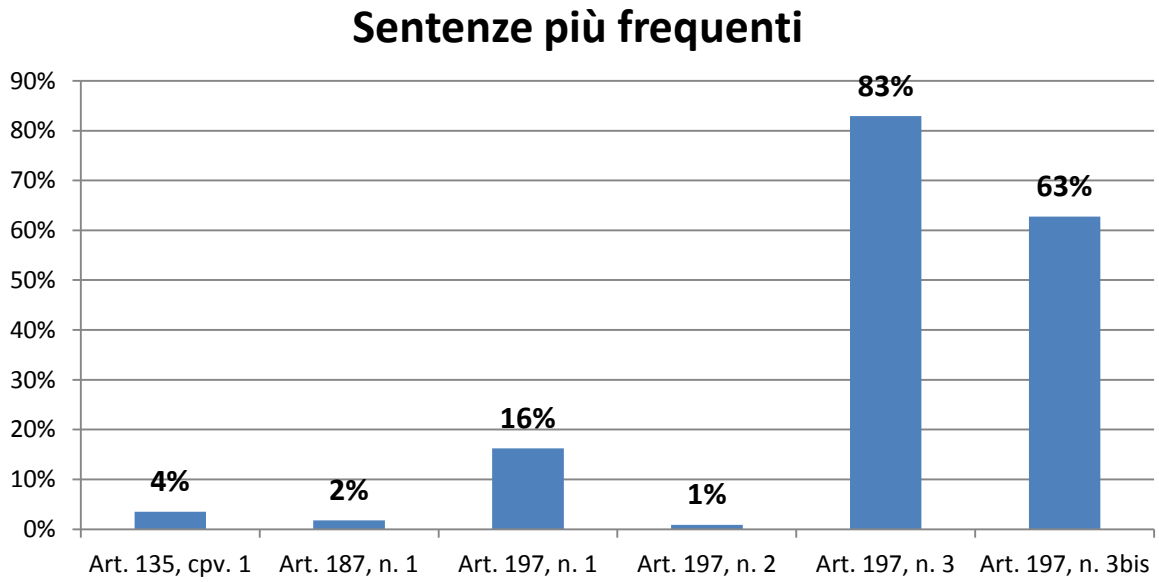


Grafico 17: Sentenze più frequenti nel 2013

Nell'85 per cento delle condanne comunicate nell'anno in rassegna è stata inflitta una pena pecuniaria (aliquota giornaliera), cumulata con una multa nel 77 per cento dei casi. Nel 91 per cento delle condanne la pena pecuniaria è stata pronunciata con la condizionale. Nel quattro per cento dei casi la condanna prevedeva un lavoro di pubblica utilità, una terapia, la privazione della libertà (detenzione), o una pena pecuniaria senza condizionale.

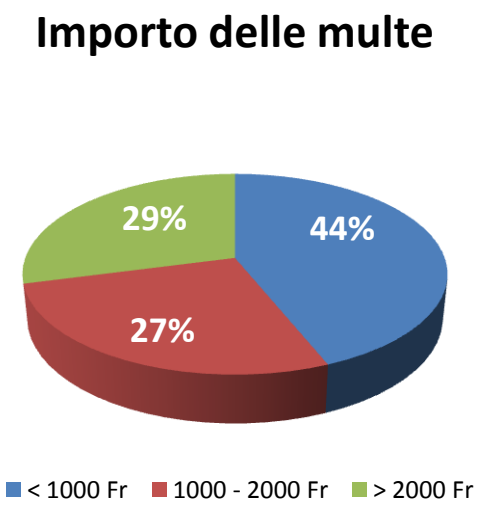


Grafico 18: Importo delle multe inflitte

Grafico 19: Numero di aliquote giornaliere inflitte

All'incirca nel 44 per cento dei casi l'importo della multa è inferiore ai 1000 franchi, nel 27 per cento dei casi è compreso tra 1000 e 2000 franchi e soltanto nel 29 per cento delle multe esso supera i 2000 franchi.

Il 29 per cento delle pene pecuniarie non supera le 50 aliquote giornaliere, nel 35 per cento dei casi la loro entità è compresa tra 51 e 100 aliquote e nel 36 per cento dei casi supera le 100 aliquote.

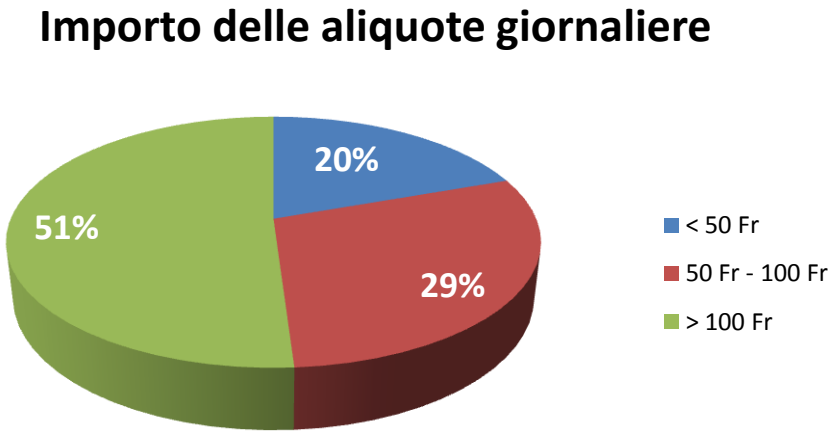


Grafico 20: Importo delle aliquote giornaliere inflitte

Infine, per quanto concerne l'importo delle aliquote giornaliere, nel 20 per cento dei casi, esso oscilla tra 1 e 50 franchi, nel 29 per cento dei casi tra 51 e 100 franchi e nel restante 51 per cento dei casi esso supera i 100 franchi.

Di norma le persone condannate devono inoltre assumersi le spese procedurali che in molti casi superano ampiamente la multa vera e propria.

4.5. Casistica

Complessivamente, nell'anno in rassegna sono stati identificati e arrestati tre individui che su chat destinate a bambini cercavano l'occasione di allacciare contatti sessuali con minori. In uno di questi casi, dopo pochi minuti di conversazione l'autore insisteva già per ottenere un incontro e manifestava la volontà di compiere degli atti sessuali con quella che in chat si descriveva come una tredicenne. Lo SCOCI ha trasmesso il caso alla polizia cantonale competente, la quale è riuscita ad arrestare il pedocriminale che si stava recando all'appuntamento con la sedicente tredicenne armato di un coltello. Questo caso mette in evidenza quanto sia elevato il pericolo che nelle chat rivolte a un pubblico minorile agiscano persone malintenzionate.

Nel campo delle ricerche attive sulle reti *peer to peer* si registra anche nel 2013 un caso di abuso attivo ai danni di un minore. A questo riguardo lo SCOCI ha trasmesso alla polizia cantonale competente diverse denunce per diffusione di materiale pornografico illegale su reti *peer to peer*. Dalle indagini è quindi emerso che l'indiziato, un padre di famiglia convivente con moglie e figli, aveva abusato sessualmente per vari mesi della propria figlia di tre anni. Prima della denuncia trasmessa dallo SCOCI l'autore risultava incensurato. Grazie alla proficua collaborazione tra lo SCOCI e la polizia cantonale e le minuziose indagini condotte successivamente dalla polizia, è stato possibile assicurare l'autore alla giustizia e proteggere la bambina da ulteriori abusi.

In un altro caso, le ricerche attive hanno messo lo SCOCI sulla pista di un cittadino tedesco attivamente coinvolto nella diffusione di materiale pedopornografico su reti *peer to peer*. Lo SCOCI ha trasmesso il caso via Interpol alle autorità tedesche. Come comunicato in seguito dal pubblico ministero competente, l'indiziato è risultato essere un quarantacinquenne a capo di un'associazione giovanile che si occupa di problematiche legate alla protezione dell'infanzia e della gioventù da violenza, pornografia, *cyber mobbing* e di software per la protezione dei minori. L'associazione era sovvenzionata dal Land tedesco in questione.

I casi descritti dimostrano quanto sia importante che le autorità cantonali si occupino sistematicamente delle denunce che lo SCOCI trasmette loro. Va tuttavia detto che alcuni Cantoni, a causa delle limitate risorse di cui dispongono, devono compiere grandi sforzi per trattare il numero sempre elevato di dossier trasmessi. In certi casi, i Cantoni, per riuscire a gestire in tempo utile l'enorme mole di lavoro supplementare generata da questi casi, devono compiere notevoli sforzi.

5. Scambio di informazioni di polizia giudiziaria

5.1. Segnalazioni ricevute e trasmesse

Con l'integrazione dello SCOCI nella Polizia giudiziaria federale, avvenuta nel 2009, e con la decisione del comitato direttivo di non trascurare le indagini sui reati economici e la criminalità su Internet in senso stretto, lo scambio di informazioni di polizia giudiziaria con le autorità in Svizzera e all'estero ha acquisito maggiore importanza. Lo SCOCI svolge oggi una funzione cardine per il flusso delle informazioni. In qualità di centro di competenza e di coordinamento, il Servizio fornisce sostegno ai Cantoni nelle loro indagini, non da ultimo grazie alla sua ampia rete di contatti con l'estero, i Cantoni stessi, l'economia privata e gli enti pubblici. Lo SCOCI funge inoltre da punto di contatto con Interpol ed Europol e in particolare con l'European Cybercrime Center (EC3).

Dall'entrata in vigore della Convenzione del Consiglio d'Europa sulla cibercriminalità il 1° gennaio 2012, sul piano internazionale la Svizzera è percepita come partner attivo nella lotta contro la criminalità su Internet. La crescente importanza del nostro Paese in questo contesto si manifesta in particolare nel netto aumento delle informazioni di polizia giudiziaria scambiate con le autorità estere su fattispecie che rientrano nel campo d'applicazione della Convenzione. Le cifre esposte in appresso rispecchiano chiaramente questa realtà.

Nel 2013 lo SCOCI ha ricevuto complessivamente 739 segnalazioni su fatti assoggettati alla Convenzione, ossia il 53 per cento in più rispetto al 2012. La stessa tendenza si registra sul fronte delle segnalazioni trasmesse alle autorità di perseguimento penale estere che aumentano di pari passo con le segnalazioni in entrata. Su incarico dei Cantoni o nell'ambito delle proprie competenze, nel 2013 lo SCOCI ha indirizzato alle autorità estere (Interpol ed Europol) un totale di 946 segnalazioni, ossia oltre il 68 per cento in più rispetto al 2012.

Grafico 21: Scambio di informazioni di polizia giudiziaria con le autorità estere nel 2013

La Convenzione del Consiglio d'Europa sulla cibercriminalità prevede la possibilità per le Parti di chiedere la conservazione rapida di dati informatici in relazione ai quali intendono presentare una domanda di assistenza giudiziaria (art. 29 segg.). A questo titolo lo SCOCI ha trasmesso ad autorità estere otto richieste dei Cantoni. A loro volta, le autorità estere hanno presentato quattro richieste.

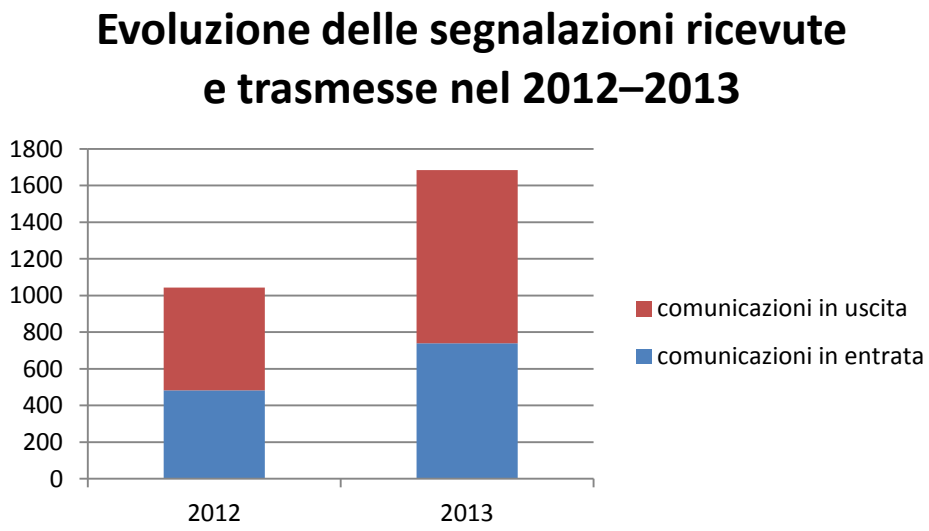


Grafico 22: Sviluppo dello scambio di informazioni di polizia giudiziaria nel 2012–2013

5.2. Coordinamento delle procedure sul piano nazionale e internazionale

Nell'ambito dello scambio d'informazioni di polizia giudiziaria sono state prese in 180 casi delle misure di coordinamento.

Il tipo di sostegno e il ruolo dello SCOCI variano di caso in caso a seconda del contesto. Il Servizio interviene come organo di coordinamento in particolare nell'ambito di procedure investigative internazionali. In questi casi funge da referente nazionale per le autorità di perseguimento penale svizzere ed estere e per i servizi e le persone che partecipano al procedimento. In altri casi, e in particolare in quelli di competenza cantonale, lo SCOCI appoggia i servizi competenti con analisi, pareri tecnici e perizie legali oppure con l'intervento di agenti sotto copertura.

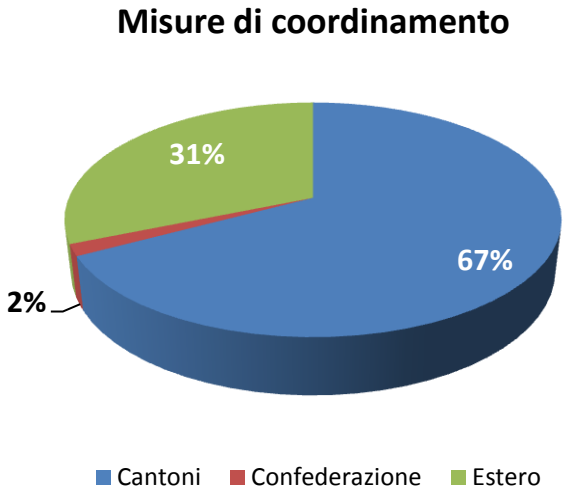


Grafico 23: Ripartizione delle misure di coordinamento, percentuali

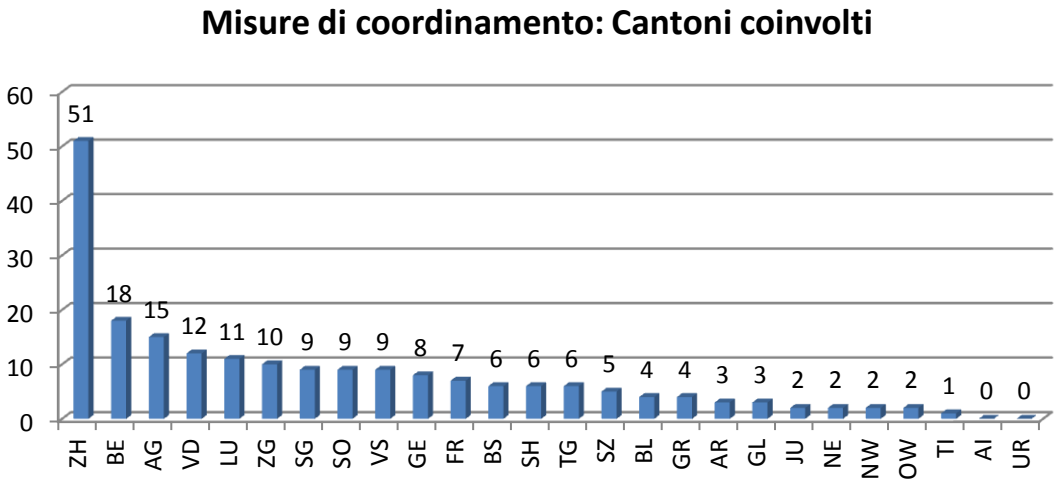


Grafico 24: Numero di misure di coordinamento secondo i Cantoni

Il Cantone di Zurigo è stato toccato da un numero di misure di coordinamento eccezionalmente elevato. Da un esame più attento emergono soprattutto due spiegazioni fondamentali a questo fenomeno. Anzitutto, come polo economico Zurigo è anche sede di molte società importanti attive nel campo dell'informazione e della comunicazione. In secondo luogo, con la costituzione di un centro di competenza cantonale per la criminalità su Internet, il Cantone ha creato premesse ideali che gli consentono di svolgere indagini nello spazio virtuale e dare un contributo alle indagini condotte sul piano internazionale.

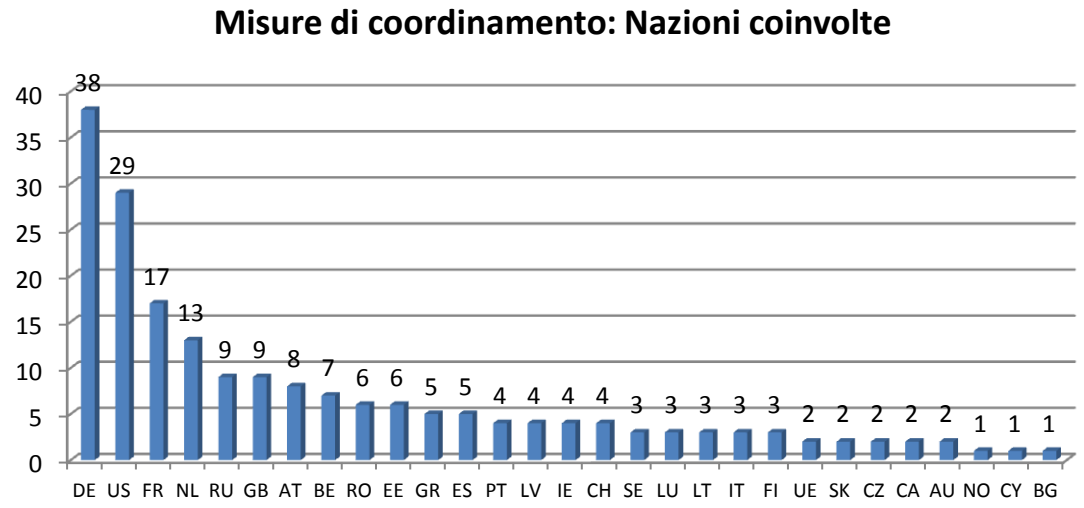


Grafico 25: Numero di misure di coordinamento secondo le Nazioni coinvolte.

Nelle indagini internazionali lo SCOCI funge da referente centrale e da unità di collegamento tra autorità inquirenti nazionali e internazionali. Il Servizio garantisce pertanto alla Svizzera una panoramica generale sui casi e sulle informazioni e le consente di adottare le necessarie misure su scala nazionale e internazionale.

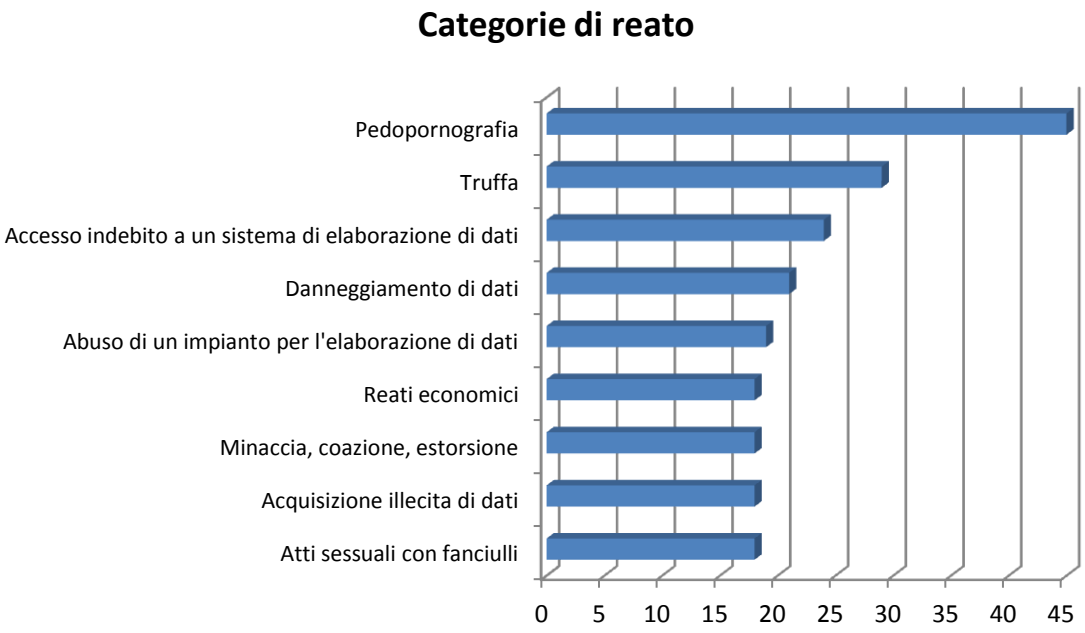


Grafico 26: Ripartizione delle misure di coordinamento nel 2013 in base alle categorie di reato

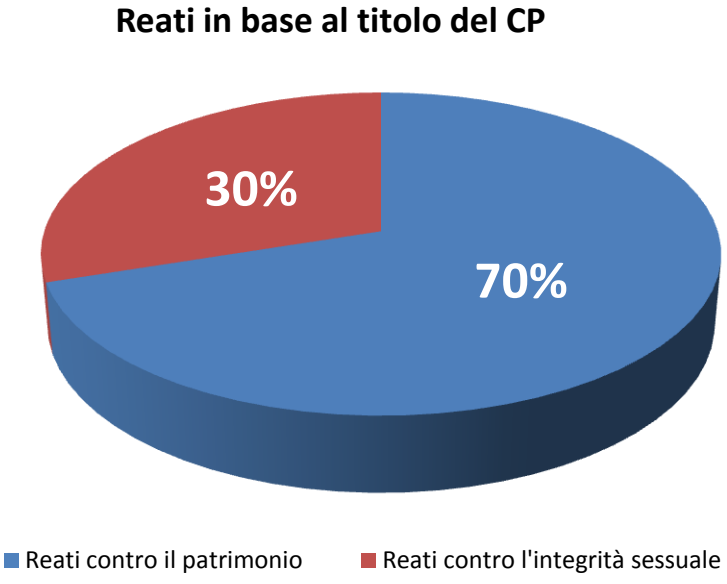
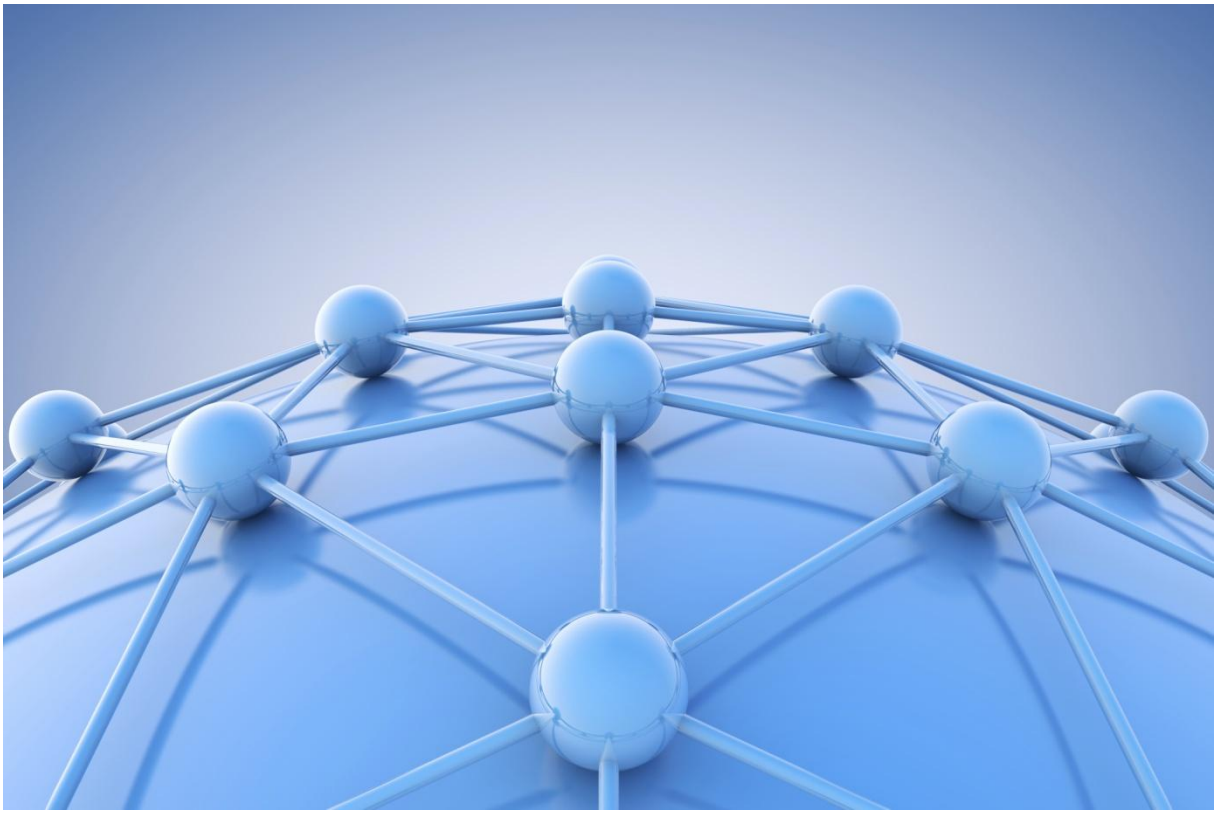


Grafico 27: Ripartizione delle misure di coordinamento nel 2013 in base al titolo del CP

5.3. Casistica

L'Ufficio anticrimine tedesco (Bundeskriminalamt) di Wiesbaden ha informato lo SCOCI che ignoti erano penetrati nei sistemi informatici di una delle principali società di telecomunicazione tedesche e stavano trasferendo i dati rubati tramite un server localizzato nel Canton Zurigo. Nel giro di poche ore lo SCOCI si è messo in contatto con il centro di competenza Cybercrime di Zurigo e ha predisposto, a norma dell'articolo 29 della Convenzione del Consiglio d'Europa sulla cibercriminalità, la conservazione rapida dei dati relativi al traffico informatico e al contenuto. Una prima analisi ha permesso di risalire a degli autori in Germania. D'intesa con l'autorità inquirente, due giorni dopo il server in questione è stato nuovamente sottoposto a delle procedure di conservazione e di analisi del contenuto, dalle quali è risultato che i criminali avevano già fatto sparire quasi tutte le prove. Se le misure di conservazione fossero state adottate soltanto in quel momento, sarebbe stato praticamente impossibile identificare gli autori del reato.



Lo SCOCI contribuisce anche al coordinamento delle attività necessarie all'esecuzione delle domande di assistenza giudiziaria provenienti dall'estero. Un caso illustrativo è quello della chiusura della banca digitale Liberty Reserve imposta dall'US Secret Service (USSS) del Dipartimento di giustizia statunitense. Lo SCOCI è intervenuto come organo di coordinamento tra l'Ufficio federale di giustizia, l'USSS, il Ministero pubblico della Confederazione e la Polizia giudiziaria federale. L'USSS si era rivolto allo SCOCI già in precedenza chiedendo di essere messo in contatto con i servizi interessati e che fossero condotti accertamenti preliminari, poiché altrimenti il tempo necessario tra la ricezione della domanda di assistenza giudiziaria all'Ufficio federale di giustizia e la prevista esecuzione delle misure sarebbe stato troppo grande comportando così il rischio di scomparsa delle prove. Grazie all'attività di coordinamento svolta dallo SCOCI nell'ambito di questa vicenda, le autorità interessate hanno potuto, durante la preparazione dell'inchiesta, concentrarsi sui loro compiti

fondamentali e in seguito sequestrare il server in questione come auspicato nella domanda di assistenza giudiziaria.

6. Progetti

6.1. Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)

Il 27 giugno 2012 il Consiglio federale ha approvato la SNPC. Con la nuova Strategia il Consiglio federale intende ridurre, in collaborazione con le autorità, il mondo dell'economia e i gestori di infrastrutture critiche, i rischi informatici ai quali tali ambienti sono esposti quotidianamente. La SNPC considera i rischi informatici anzitutto come fenomeno direttamente collegato ai processi esistenti e alle responsabilità degli attori coinvolti. Occorre pertanto integrare nei processi di gestione dei rischi già in uso anche queste nuove tipologie di rischi. In primo luogo, i responsabili devono acquisire una base di conoscenze sui cyber-rischi e sviluppare una certa sensibilità a questo riguardo.

A tale scopo il Consiglio federale ha incaricato i dipartimenti di avviare al loro interno l'attuazione delle 16 misure previste dalla SNPC coinvolgendo le autorità cantonali e il mondo dell'economia. Le misure previste spaziano dall'analisi dei rischi delle infrastrutture critiche a una difesa più assidua degli interessi della Svizzera in questo campo sul piano internazionale.

La misura 6 prevede la gestione di una panoramica possibilmente esaustiva casi (casi penali) a livello nazionale e la garanzia del coordinamento dei casi di portata intercantonale. Le informazioni ottenute devono confluire in una rappresentazione globale della situazione. Il DFGP, in collaborazione con i Cantoni, dovrà sottoporre entro la fine del 2016 il documento programmatico che chiarirà le questioni concernenti i punti di contatto con gli altri attori coinvolti nell'ambito della riduzione dei rischi informatici, il coordinamento con i lavori per la rappresentazione della situazione nonché le risorse e gli adeguamenti giuridici necessari a livello federale e cantonale. Sulla base della decisione del comitato direttivo dello SCOCI e della direzione di fedpol, lo SCOCI garantisce per conto di fedpol il coordinamento e l'adempimento del mandato in relazione ai lavori di attuazione della SNPC. La direzione del progetto è invece assunta dal capo della Polizia giudiziaria federale.

Nelle prossime tappe di attuazione della SNPC, occorrerà in particolare chiarire le questioni organizzative, tecniche, giuridiche e inerenti ai mezzi (p. es. le risorse in materia di personale, infrastruttura, informatica ecc). Come prima mossa si è già provveduto a elaborare un'analisi dettagliata del mandato e a definire l'organizzazione del progetto, composta di rappresentanti di fedpol, della CDDGP, della CCPCS, della CPS (ex CAIS), di Swiss Police ICT (in qualità di gruppo d'interesse), del Ministero pubblico della Confederazione e dell'Ufficio federale di giustizia (come gruppo d'interesse). Nel 2014 il progetto verrà sottoposto a due consultazioni presso i Cantoni e i servizi interessati.

6.2. Presenza dello SCOCI nei social media

In qualità di punto di contatto, lo SCOCI è tenuto a confrontarsi in permanenza con gli ultimi sviluppi relativi a Internet. I progressi della tecnica inducono cambiamenti nelle possibilità di comunicazione e di conseguenza anche nell'utilizzo dei media. Aumentano inoltre anche le segnalazioni allo SCOCI su contenuti o comportamenti potenzialmente perseguibili inerenti a Facebook.

Alla luce di queste considerazioni, il Servizio ha sollecitato il comitato direttivo affinché definisse una serie di misure per migliorare il dialogo con gli utenti. Il comitato ha quindi deciso di dotare lo SCOCI di un proprio profilo su Facebook e Twitter e di attivare i nuovi canali di comunicazione nel quadro del decimo anniversario del Servizio. I nuovi profili[10] sono stati attivati in versione trilingue il 22 dicembre 2013 e da allora sono a disposizione della popolazione.

[10] www.facebook.com/cybercrime.ch e, su Twitter, @KOBIK_Schweiz

7. Gruppi di lavoro, cooperazione e contatti

7.1. Raccolta nazionale di file e valori hash

La Raccolta nazionale di file e valori hash è entrata in funzione nell'ottobre 2012 e da allora è a disposizione dei servizi specializzati di Cantoni e città. Affinché la raccolta possa essere utilizzata in modo efficiente, è necessario classificare un numero sufficiente di immagini conosciute e creare i corrispondenti valori hash. La classificazione di materiale visivo richiede molto tempo e date le limitate risorse di cui dispone lo SCOCI può essere garantita soltanto grazie al sostegno dei Cantoni.

7.2. Gruppi di lavoro nazionali

Nel 2013 lo SCOCI ha fatto parte di diversi gruppi di lavoro nazionali.

In collaborazione con il commissariato Pedocriminalità/pornografia della Polizia giudiziaria federale, lo SCOCI ha organizzato l'incontro annuale del gruppo di lavoro «Kindsmissbrauch» (abusi sui fanciulli). Il gruppo di lavoro, che conta anche rappresentanti di organizzazioni di pubblica utilità, dei Cantoni e della «Prevenzione Svizzera della Criminalità», affronta temi d'attualità legati alla problematica degli abusi sui fanciulli e alla lotta contro tali abusi.

Come negli anni precedenti, lo SCOCI ha partecipato anche nel 2013 ai lavori del programma nazionale «Protezione della gioventù dai rischi dei media e competenze mediali», sia in seno al comitato direttivo, incaricato dell'elaborazione del programma, sia nel gruppo esecutivo di accompagnamento. Il programma intende aiutare bambini e giovani a utilizzare i media moderni in modo sicuro, responsabile e adeguato alla loro età.

Dal 2011 lo 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 in seguito l'attuazione.

Lo SCOCI ha inoltre partecipato all'attuazione del piano «Sicurezza e fiducia», diretto dall'Ufficio federale delle comunicazioni (UFCOM). Il piano illustra le misure da adottare per promuovere la sicurezza e la fiducia della popolazione nei confronti delle nuove tecnologie dell'informazione e della comunicazione (TIC).

7.3. Collaborazione con i servizi della Confederazione

Anche nell'anno in esame, lo SCOCI ha lavorato a stretto contatto con diversi servizi della Confederazione sul fronte della lotta contro la criminalità su Internet. In seno a fedpol, il Servizio ha collaborato intensamente soprattutto con i commissariati Pedocriminalità/pornografia, Indagini Tecnologie dell'informazione e Inchieste mascherate della Polizia giudiziaria federale nonché con la divisione principale Cooperazione internazionale di polizia (CIP). Considerata la convergenza degli ambiti di attività, lo SCOCI collabora con particolare intensità con il commissariato Pedocriminali-

tà/pornografia. Inoltre lo SCOCI ha sviluppato e approfondito vari contatti con diversi servizi collocati in altri dipartimenti federali, 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 dell'informatica e della telecomunicazione (UFIT), l'Ufficio federale delle assicurazioni sociali (UFAS), l'Ufficio federale delle comunicazioni (UFCOM), la Commissione federale contro il razzismo (CFR), l'Amministrazione federale delle dogane (AFD), la Regìa federale degli alcool (RFA), l'Autorità federale di vigilanza sui mercati finanziari (FINMA), l'Istituto federale della proprietà intellettuale (IPI) e la Commissione federale delle case da gioco (CFCG).

7.4. Scambio di esperienze con i Cantoni

Nell'anno in esame, lo SCOCI ha intrattenuto diversi contatti con rappresentanti di vari corpi di polizia e pubblici ministeri cantonali.

Un aspetto particolarmente importante in questo contesto è costituito dalla collaborazione e dallo scambio di esperienze con il centro di competenza Cybercrime del Cantone di Zurigo, che ha iniziato la sua attività nel 2013. La chiara definizione delle strutture orientate a contrastare la criminalità su Internet e degli interlocutori presso il pubblico ministero e la polizia ha consentito in varie occasioni di impedire la distruzione delle prove o addirittura l'apertura di un procedimento.

Oltre al consueto scambio di esperienze con i Cantoni, si sono tenute diverse riunioni di lavoro, in particolare nell'ambito di indagini preliminari sotto copertura (cfr. n. 4) e del progetto relativo alla Raccolta nazionale di file e valori hash (cfr. n. 7.1).

Il 19 novembre 2013 si è inoltre tenuto il secondo «*Forum Cybercrime Staatsanwaltschaften - KOBIK*» (forum sulla collaborazione tra i pubblici ministeri e lo SCOCI in materia di cibercriminalità). Esperti ed esponenti degli ambienti scientifici e in materia di perseguimento penale hanno fornito ai partecipanti un'immagine concreta della lotta internazionale contro la criminalità su Internet. I partecipanti hanno potuto farsi un'idea delle indagini in corso contro i *botnet* e delle attività di riciclaggio in rapporto alle valute virtuali. Inoltre, i rappresentanti di Europol hanno informato in merito ai poteri di coordinamento di cui è dotato lo European Cybercrime Center EC3 dell'Aia. Al forum di quest'anno hanno partecipato un centinaio di procuratori pubblici, con un'affluenza che testimonia dell'importanza di questo genere di proposta formativa. La partecipazione alla tavola rotonda del consigliere agli Stati Luc Recordon, del consigliere nazionale Daniel Jositsch e di Christian Schwarzenegger, professore di diritto penale all'università di Zurigo, ha inoltre consentito uno scambio diretto con esponenti della politica e del mondo accademico sulle difficoltà concrete riscontrate dai pubblici ministeri.

7.5. Collaborazione con organizzazioni non governative (ONG)

Da diversi anni lo SCOCI collabora strettamente con l'ONG Action Innocence (AIG) nella lotta contro la pedopornografia. Grazie al sostegno offerto da AIG, negli ultimi anni è stato possibile proseguire e approfondire il progetto per il monitoraggio delle reti *peer to peer*. La collaborazione con AIG assume un'importanza ancora maggiore, se si considera che la maggior parte delle ricerche attive condotte dallo SCOCI sono

rese possibili dal software messo a disposizione da AIG. Quest'ultima sostiene inoltre lo SCOCI sviluppando ulteriori progetti nell'ambito della lotta alla pedocriminalità.

La Fondazione svizzera per la protezione dell'infanzia e ECPAT Svizzera si adoperano in particolare a favore della protezione dei minori e della prevenzione della violenza nei confronti dei fanciulli su Internet. Gli incontri periodici con queste organizzazioni consentono di sfruttare le possibili sinergie e di unire le forze nella lotta contro gli abusi di minori.

Nell'anno in rassegna, all'incontro del gruppo di lavoro « Kindsmissbrauch» è stata invitata anche Pro Juventute, con la quale è stata avviata una collaborazione più stretta.

7.6. Collaborazione con i provider svizzeri di accesso a Internet

Dal 2007 lo SCOCI coadiuva i principali provider svizzeri nel blocco dei siti contenenti materiale pedopornografico. Il blocco interessa esclusivamente i siti esteri che offrono il download di materiale raffigurante atti sessuali con fanciulli ai sensi dell'articolo 197 numero 3 CP. Lo SCOCI mette a disposizione dei provider una lista aggiornata di siti Internet (circa 200-300 siti) con contenuti di questo genere. I provider bloccano l'accesso a questi siti in virtù della loro etica aziendale e delle condizioni generali di contratto e deviano gli utenti verso una cosiddetta *stop page*.

Nell'ambito di questo progetto lo SCOCI collabora strettamente con Interpol. La lista allestita in Svizzera alimenta con un consistente apporto la lista «Worst-Of» di Interpol, sulla quale figurano i siti Internet che propongono materiale pedopornografico. Lo SCOCI si impegna ogni giorno nella ricerca di nuovi siti Internet contenenti materiale pedopornografico e foraggia costantemente la lista di Interpol, che è gestita in collaborazione con diversi servizi di polizia internazionali.

7.7. Cooperazione internazionale

Dal 2011 lo SCOCI è membro del Focal Point (FP) CYBORG di Europol, specializzato nella lotta alla criminalità transfrontaliera su Internet e in particolare ai fenomeni di phishing, *botnet* e *hacking*. Nel 2012 lo SCOCI ha inoltre aderito al FP TWINS incentrato sulla lotta contro la pedocriminalità. Entrambi i Focal Point sono stati integrati all'European Cybercrime Center.

Il centro per la lotta contro la criminalità su Internet EC3 fornisce sostegno operativo agli Stati dell'UE e mette a disposizione le proprie conoscenze specialistiche nelle indagini comuni a livello europeo. Lo SCOCI intrattiene stretti contatti con l'EC3 e in diverse occasioni ha già contribuito attivamente a delle operazioni nell'ambito delle reti anonime.

A partire dal 2013 lo SCOCI rappresenta inoltre la Svizzera in seno all'European Union Cybercrime Task Force (EUCTF). Il gruppo di esperti, formato da rappresentanti di Europol, di Eurojust e della Commissione europea, è stato costituito nel 2010 per agevolare e ottimizzare la lotta contro la criminalità su Internet nello spazio europeo in collaborazione con i responsabili delle unità Cybercrime nazionali. L'EUCTF contribuisce allo sviluppo e alla promozione di un progetto europeo armonizzato per

contrastare la criminalità su Internet nonché alla soluzione dei problemi derivanti dall'impiego delle cibertecnologie per la commissione di reati. L'Unione europea attribuisce un'estrema importanza alla lotta contro la criminalità su Internet anche nell'ambito della piattaforma European Multidisciplinary Platform Against Criminal Threats (EMPACT) e ha inserito la lotta alla cibercriminalità tra le otto priorità del proprio ciclo programmatico per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale. Lo SCOCI affianca gli sforzi dell'Unione europea e rappresenta attivamente gli interessi della Svizzera nell'ambito dei dibattiti.

Lo SCOCI collabora anche al progetto CIRCAMP, promosso dall'European Chief of Police Task Force (EPCTF) al fine di combattere la diffusione di materiale pedopornografico su Internet. Come negli anni precedenti, nel 2013 lo SCOCI ha preso parte all'European Financial Coalition (EFC), cofinanziata dall'UE e composta di attori responsabili del perseguimento penale e di operatori del settore privato accomunati dall'obiettivo di contrastare lo sfruttamento sessuale di minori per scopi commerciali su Internet.

Persegue obiettivi analoghi anche la Global Alliance Against Child Sexual Abuse Online, iniziativa contro la pedocriminalità online lanciata a Bruxelles dagli Stati europei e alla quale la Svizzera ha aderito il 5 dicembre 2012. In occasione della firma dell'iniziativa, la Consigliera federale Simonetta Sommaruga ha sottolineato l'importanza che la Svizzera attribuisce alla cooperazione internazionale nel campo della lotta contro la pedocriminalità e la necessità di promuovere ulteriormente tale cooperazione. Una delle tappe definite dallo SCOCI nell'ambito della cooperazione con la Global Alliance riguarda l'adesione della Svizzera alla Virtual Global Taskforce (VGT). La VGT è un'alleanza internazionale tra autorità di perseguimento penale, organizzazioni non governative e industria privata finalizzata a proteggere i minori dagli abusi su Internet. L'alleanza intende rendere Internet uno spazio più sicuro, individuare e localizzare gli abusi, aiutare i minori in difficoltà e assicurare il perseguimento efficace dei criminali che abusano di minori. La VGT conta attualmente dodici membri a pieno titolo e diversi partner (cfr. www.virtualglobaltaskforce.com).Nell'anno in rassegna la richiesta di adesione presentata dalla Svizzera è stata approvata all'unanimità dal consiglio amministrativo. Lo SCOCI rappresenterà dunque il nostro Paese come nuovo Stato membro in occasione del prossimo incontro della VGT, in programma a Bruxelles nel maggio 2014.

8. Presenza nei mass media, attività didattica e conferenze

8.1. Presenza nei mass media

Nel 2013, le attività dello SCOCI hanno trovato ampia risonanza nei media. Gli avvisi allestiti dal Servizio per segnalare pericoli legati a fenomeni criminali su Internet sono stati diramati anche dai media.

Va menzionata in particolare la partecipazione dello SCOCI al reportage «*Chronik eines Missbrauchs*» trasmesso dal canale svizzero tedesco della SSR nell'ambito della serie di documentari «*Schweizer Verbrechen im Visier*».

8.2. Social media

I riscontri ricevuti dagli utenti di Facebook e Twitter sui nuovi profili nei *social media* dello SCOCI (www.facebook.com/cybercrime.ch e Twitter sotto @KOBIK_Schweiz) sono assolutamente positivi.

8.3. Attività didattica e conferenze

Nell'anno in esame i collaboratori dello SCOCI hanno partecipato a numerose conferenze, convegni internazionali e corsi di formazione e colto l'occasione per rinsaldare i contatti con partner ed esperti.

Alcuni collaboratori hanno inoltre partecipato a diversi seminari in veste di formatori. L'Istituto Svizzero di Polizia (ISP), ad esempio, ha di nuovo organizzato una serie di workshop sulla cooperazione internazionale in materia di polizia nel campo della criminalità informatica. Inoltre, nell'ambito del corso di aggiornamento degli inquirenti IT del Concordato di polizia della Svizzera nord-occidentale i collaboratori dello SCOCI hanno tenuto una serie di conferenze sull'economia clandestina legata alla criminalità informatica. Oltre a queste attività, nel 2013 lo SCOCI ha tenuto conferenze o partecipato a tavole rotonde in più di 50 occasioni.

9. Interventi politici a livello federale

Interpellanza 13.3229: Portata della minaccia e misure di lotta contro la guerra e la criminalità cibernetiche - Recordon Luc; Gruppo dei Verdi

Interpellanza 13.3986: Richieste alle reti sociali. Perché la Svizzera ottiene così poche informazioni?- Vogler Karl; Gruppo PPD-PEV

Mozione 13.3490: Centro di competenza per la sicurezza in ambito TIC - Gruppo BD

Interrogazione 13.5380: Insuffisance des instruments de lutte contre la cybercriminalité - Reimann Maximilian; Gruppo dell'Unione democratica di Centro (non disponibile in italiano)

Interrogazione 13.5356: Commande de drogues sur le site web Silk Road - Geissbühler Andrea Martina; Gruppo dell'Unione democratica di Centro (non disponibile in italiano)

Interrogazione 13.5321: La Suisse fait-elle aussi l'objet d'espionnage économique par la NSA? - Leutenegger Oberholzer Susanne; Gruppo socialista (non disponibile in italiano)

Interrogazione 13.5281: Activités des services secrets américains en Suisse - Vischer Daniel; Gruppo dei Verdi (non disponibile in italiano)

Interrogazione 13.5059: Responsabilité des fournisseurs d'hébergement et des services de blogs et de forums - Glättli Balthasar; Gruppo dei Verdi (non disponibile in italiano)

Interrogazione 13.5224: Cyberactivités des services secrets américains en Suisse - Reimann Maximilian; Gruppo dell'Unione democratica di Centro (non disponibile in italiano)

Interpellanza 13.4077: Spionaggio di dati e sicurezza su Internet - Clottu Raymond; Gruppo dell'Unione democratica di Centro

Iniziativa parlamentare 13.442: Grooming con minorenni – Commissione degli affari giuridici CN

Postulato 13.3707: Strategia globale per il ciberspazio al passo con i tempi - Gruppo BD

Interpellanza 13.3773: Legge sulle telecomunicazioni al passo con i tempi. Una strategia globale per il ciberspazio – Gruppo liberale radicale

Interpellanza 13.3033: Come proteggere i dati personali di cittadini svizzeri in possesso di imprese americane? - Schwaab Jean Christophe; Gruppo socialista

Interpellanza 13.3726: Usurpazione d'identità. Una lacuna penale da colmare? - Schwaab Jean Christophe; Gruppo socialista

Postulato 13.3687: Valutare i rischi della moneta virtuale Bitcoin - Schwaab Jean Christophe, Gruppo socialista

10. Potenziali sviluppi e minacce per il 2014

Il numero di segnalazioni pervenute allo SCOCI non permette di trarre conclusioni dirette o concrete in merito allo sviluppo effettivo della criminalità su Internet o dei contenuti illegali diffusi in rete. Le cifre rispecchiano soltanto le tendenze relative alla propensione della popolazione a segnalare eventuali casi di cibercriminalità e al modo in cui la società percepisce la criminalità su Internet. Le affermazioni seguenti si basano sull'interpretazione personale dello SCOCI di ricerche effettuate nelle fonti pubbliche e sulle conoscenze di cui dispone a livello operativo.

Incremento dei tentativi di truffa riusciti

Alla luce delle truffe segnalate si è constatato che nel corso dell'anno è aumentato il grado di professionalità con cui sono compiuti questi reati. La professionalità è aumentata sia in merito alla qualità dei testi sia a livello di grafica. Questa tendenza riguarda pressoché ogni tipo di tentativo di truffa: dall'invio di messaggi di phishing, all'allestimento di inserzioni e risposte fraudolente su piattaforme di annunci fino alla schermata di blocco dei *ransomware*. Vi è da temere che questa tendenza si confermerà anche negli anni venturi. Per gli utenti di Internet potrebbe quindi diventare sempre più difficile riconoscere un tentativo di truffa. Per le autorità penali risulta molto arduo contrastare questi fenomeni di truffa visto che hanno spesso origine in Paesi del Nordafrica e dell'Africa occidentale e che i criminali possono contare su una rete di *money mules*[11] che si estende nel mondo intero e che sanno sfruttare a proprio vantaggio gli ostacoli legali che impediscono il perseguimento penale. Bisogna pertanto puntare maggiormente sulla prevenzione e sull'adozione di misure tecniche da parte dei gestori di piattaforme.

Sviluppo dell'economia clandestina legata alla cibercriminalità

Negli ultimi anni attorno alla criminalità su Internet in senso lato e in senso stretto si è sviluppata una vera e propria economia clandestina. Su Internet si possono acquistare in tutta tranquillità, velocemente e sotto anonimato, servizi come la produzione mirata di *malware*, l'invio di e-mail di massa, l'esecuzione attacchi DDoS e falsi profili su reti sociali. Per il pagamento di tali servizi si ricorre esclusivamente a valute elettroniche quasi anonime, ad esempio Bitcoin, oppure a piattaforme per il loro scambio. Viene fatto ricorso frequentemente anche a servizi di trasferimento che al di fuori dei confini europei possono essere utilizzati spesso senza indicare la propria vera identità. Di conseguenza, seguire questi movimenti finanziari è ormai praticamente impossibile.

Considerata la situazione economica che affligge l'Europa, occorre prevedere un aumento degli attori in questa economia clandestina. I mezzi investigativi convenzionali non consentono di combattere efficacemente questo fenomeno. Occorre invece puntare maggiormente sulle inchieste mascherate nell'ambito di una cooperazione internazionale, in modo da disporre di un quadro globale dello stato di questa economia e di riuscire a identificarne i principali attori. Per la Svizzera questo significa che verosimilmente il singolo Cantone non sarà in grado di perseguire con successo gli autori di tale tipo di reati. Una soluzione più efficiente consisterebbe nel coordinare le operazioni in base a una panoramica dei casi a livello nazionale, come previsto

[11] Agenti reclutati per il riciclaggio di denaro

dalla SNPC. I procedimenti potrebbero dunque essere condotti da gruppi di lavoro congiunti sotto la direzione di un Cantone o della Confederazione.

Piccole medie imprese (PMI) sempre più spesso nel mirino

Considerati lo scambio di "know-how" che ha luogo nei mercati clandestini e la grande diffusione di *malware,* occorre presumere che le PMI saranno sempre più spesso preda di furti di dati. Per i cibercriminali, le PMI sono un bersaglio lucrativo poiché le raccolte di dati da esse gestite (consistenti in indirizzi di posta elettronica, password, recapiti e indirizzi postali) hanno un grande valore nell'economia clandestina che ruota attorno alla criminalità informatica. In aggiunta, le infrastrutture di queste ditte non dispongono di dispositivi di sicurezza paragonabili ad esempio a quelli delle grandi banche. Sembrano inoltre in aumento anche i tentativi di ricatto preceduti da un furto di dati e da attacchi DDoS ai danni di siti Internet di imprese locali. In particolare, si prevede un aumento dei ricatti esercitati con l'ausilio di cosiddetti *CryptoLocker* (cfr. capitolo 3.2.1).

Furto di certificati

Nell'anno in esame lo SCOCI aveva già ricevuto da importanti enti certificatori segnalazioni riguardanti la perdita di certificati[12] che in seguito erano stati utilizzati da cibercriminali per firmare *malware* e aggirare così i dispositivi di sicurezza quali ad esempio le scansioni antivirus. Questo fenomeno potrebbe far vacillare uno dei principali pilastri della sicurezza su Internet, ossia la catena di fiducia garantita dagli enti certificatori. Per gli utenti finali, il crollo di questo pilastro significherebbe che i criminali avrebbero la possibilità di intercettare senza essere notati collegamenti considerati sicuri con determinati web server e leggere, deviare e modificare per fini illeciti i dati scambiati. Il browser continuerebbe tuttavia a segnalare all'internauta il collegamento con un server munito di certificato correttamente firmato, quindi sicuro. Questa situazione potrebbe avere gravi ripercussioni ad esempio per i servizi e-banking, per il trasferimento dei dati nell'ambito di acquisti online e per altre applicazioni critiche dal profilo della sicurezza.

Probabile incremento di *malware* diretto contro dispositivi mobili

Il trasferimento del principale utilizzo di Internet su terminali mobili potrebbe accelerare la diffusione di varianti di *malware* per telefoni cellulari, smartphone e tablet. Con la diffusione dei meccanismi di autenticazione per i sistemi di e-banking che richiedono l'esistenza di un dispositivo di comunicazione supplementare, ad esempio di un telefono cellulare o uno smartphone, non si può escludere l'aumento del numero di attacchi contro i sistemi di questo tipo per mezzo di *malware* per dispositivi mobili. Il gran numero di dispositivi in circolazione, i vari tipi di modelli, le conoscenze occorrenti e il numero crescente di specialisti necessari metterà i corpi di polizia cantonali che dispongono di divisioni informatiche di dimensioni ridotte di fronte a difficoltà difficili da superare, sia sul piano forense sia sul piano finanziario.

[12] Un certificato è un'identità digitale rilasciata e autenticata da enti autorizzati (enti certificatori, «Certificate Authorities»). La firma dei certificati di identità elettroniche, anzitutto per i web server, equivale al rilascio di un passaporto per una persona fisica.

11. Glossario

Adult check	Sistema per la protezione della gioventù che consente di 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, indispensabili per la fluidità del sistema.
Peer to peer	Modello di rete informatica per la condivisione di file tra utenti di stesso livello (*peer*).
Pornografia dura	Rappresentazione di atti sessuali con fanciulli (pedopornografia), animali, escrementi umani o atti violenti (art. 197 n. 3 CP).
Valore hash	Valore attribuibile in modo univoco a un'immagine (impronta digitale).
Phishing	(unione tra i termini inglesi *phreaking* [utilizzo di dati di accesso falsi] e *fishing*) Metodo utilizzato per ottenere in modo fraudolento i dati d'accesso a servizi online, soprattutto tramite l'invio di e-mail di massa da parte di mittenti fittizi che chiedono i la «verifica» dei dati dei clienti.
Proxy	(ingl. *proxy* = mandatario) Un *proxy* è un server che funge da tramite tra un client (l'utente) e un server (il sito web che s'intende consultare).
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 in diretta di dati audio e video che non necessita il *download* per intero sul disco rigido. I dati sono riprodotti man mano che giungono a destinazione.
URL	*(Uniform Resource Locator*) sequenza di caratteri utilizzata per indirizzare gli utenti verso le risorse del web (indirizzo web).