Sistema di esplorazione delle comunicazioni via satellite del Dipartimento federale della difesa, della protezione della popolazione e dello sport (progetto «Onyx»)

Rapporto della Delegazione delle Commissioni della gestione delle Camere federali

del 10 novembre 2003

«The King has note of all that they intend,
By interception which they dream not of.»

«Il re però è informato di tutto,
avendo intercettato i lor messaggi,
e sa, come nemmeno essi si sognano,
d'ogni loro segreto intendimento.»

William Shakespeare, Enrico V, atto secondo, scena 2

Rapporto

1 Introduzione

Seguendo l'esempio di diversi Stati, il Consiglio federale ha deciso nel 1997 di sviluppare un progetto di esplorazione delle comunicazioni via satellite. Il sistema, denominato Onyx (ex SATOS-3), permette di intercettare le comunicazioni internazionali civili e militari che transitano via satellite. Esso fornisce alle massime autorità della Confederazione informazioni importanti per analisi e decisioni in materia di politica di sicurezza. L'attività di Onyx è basata principalmente sull'articolo 99 della legge federale del 3 febbraio 1995 sull'esercito e sull'amministrazione militare (LM; RS *510.10*) che disciplina i compiti del servizio informazioni estero della Confederazione.

Il sistema Onyx è entrato in funzione nell'aprile 2000 e attualmente è nella fase sperimentale. Passerà alla fase operativa nel corso del 2004 e alla piena operatività alla fine del 2005/all'inizio del 2006.

Il sistema Onyx offre già ora numerose funzioni e possibilità di raccolta di informazioni al Servizio informazioni strategico (SIS) del Dipartimento della difesa, della protezione della popolazione e dello sport (DDPS), che è il suo principale utente. In misura minore serve anche al Servizio di analisi e prevenzione (SAP) del Dipartimento federale di giustizia e polizia (DFGP).

Onyx consente la sorveglianza di massa delle comunicazioni. Semplifica e moltiplica le capacità dei servizi d'informazioni di raccogliere informazioni utili, ad esempio, nella lotta contro la proliferazione delle armi di distruzione di massa (WDM = Weapons of Mass Destruction) o contro il terrorismo internazionale.

Il sistema non offre solo vantaggi. Può anche presentare, se non è strettamente inquadrato in una cornice giuridica e politica, rischi importanti per quanto riguarda i diritti fondamentali, in particolare il diritto alla protezione della sfera privata e il rispetto del segreto delle telecomunicazioni. Tale diritto è garantito dall'articolo 13 della Costituzione federale della Confederazione Svizzera del 18 aprile 1999 (Cost.; RS *101*). Nel diritto internazionale, la sfera privata è protetta dall'articolo 8 della Convenzione europea del 4 novembre 1950 dei diritti dell'uomo (CEDU; RS *0.101*) e dall'articolo 17 del Patto internazionale relativo ai diritti civili e politici del 16 dicembre 1966 (Patto ONU II; RS *0.103.2*).

Dopo il caso delle schedature negli anni Novanta, il Parlamento è molto sensibile ai rischi che le misure di sorveglianza adottate dallo Stato rappresentano per i diritti fondamentali. Le intercettazioni, per la loro natura segreta, suscitano fondati timori e sollevano legittime obiezioni.

Per questo motivo, sin dall'inizio la Delegazione delle Commissioni della gestione (DCG) ha seguito da vicino la realizzazione del progetto Onyx, con l'obiettivo di esaminare se il sistema rispetta, a livello di struttura e di esercizio, l'ordinamento giuridico svizzero e in particolare i diritti fondamentali. La Delegazione ha anche provveduto a far correggere man mano i punti più critici del progetto prima che il sistema raggiunga la fase operativa.

Nel presente rapporto si espongono le differenti constatazioni fatte dalla Delegazione e le misure adottate dal DDPS e dal Consiglio federale; si illustra anche la valuta-

zione generale della Delegazione, si propongono diverse raccomandazioni e si presenta la situazione alla fine di ottobre 2003.

2 Metodo di lavoro

2.1 Mandato generale della Delegazione delle Commissioni della gestione

La DCG esercita, su incarico delle Camere federali, l'alta vigilanza sull'attività della Confederazione nel settore della protezione dello Stato e dei servizi d'informazione (art. 47quinquies cpv. 2 LRC; RS *171.11*).

Per «protezione dello Stato», si intendono tutte le attività della Confederazione che hanno carattere repressivo o preventivo e che contribuiscono a garantire la «sicurezza interna» della Svizzera. Si tratta in particolare della lotta contro il terrorismo, contro i gruppi violenti di estremisti, contro il crimine organizzato, contro lo spionaggio e contro la proliferazione delle armi di distruzione di massa.

Il termine «servizio informazioni» copre tutte le attività che permettono alla Confederazione di raccogliere e utilizzare informazioni dall'estero, con l'obiettivo di garantire la «sicurezza esterna» della Svizzera.

L'alta vigilanza è esercitata in primo luogo sotto l'aspetto dei principi della legalità, dell'opportunità e dell'efficienza.

La DCG sottopone le attività segrete della Confederazione a un controllo continuo e approfondito per scoprire per tempo i punti che giustificano un intervento politico. In questo contesto, la DCG attribuisce grande importanza al riconoscimento precoce dei problemi e contribuisce a correggere le insufficienze e le disfunzioni constatate.

Per svolgere il suo compito, la DCG dispone, in virtù della Costituzione e della legge, di diritti di informazione particolarmente ampi. Né il segreto d'ufficio, né il segreto militare sono opponibili alla DCG (art. 169 cpv. 2. Cost.).

2.2 Definizione dell'oggetto e dei limiti dell'inchiesta

La realizzazione del progetto Onyx solleva tutta una serie di domande: chi viene intercettato? Con quali obiettivi? In quali settori? Chi affida i mandati di esplorazione e secondo quali procedimenti? Chi controlla i risultati delle intercettazioni? Chi li archivia? Chi ha accesso ai documenti? Chi li utilizza? Che cosa succede di informazioni raccolte casualmente? L'esplorazione radio via satellite è un'attività esclusivamente nazionale oppure la Svizzera coopera a un sistema di intercettazione internazionale? Ecc.

Queste domande sollevano importanti problemi di ordine giuridico e politico.

La Delegazione si è data il mandato seguente:

- esaminare e commentare il sistema di esplorazione Onyx,
- descrivere i processi di assegnazione dei mandati di esplorazione e di raccolta di informazioni,
- valutare il contesto giuridico a livello nazionale e internazionale,

– situare il progetto Onyx nel contesto internazionale,
– valutare i sistemi di controllo impiegati,
– formulare eventualmente raccomandazioni politiche e legislative.

La Delegazione ha deciso di concentrare, in un primo tempo, la sua analisi sulla legalità delle intercettazioni. In occasione di una prossima verifica, esaminerà anche l'efficienza del sistema, come pure la sua affidabilità e il suo rendimento.

Occorre rilevare che il sistema Onyx comprende unicamente le intercettazioni amministrative svolte per scopi di informazione. Non concerne le misure di sorveglianza telefonica adottate nell'ambito di procedure penali a livello federale e cantonale, nonché in materia di assistenza giudiziaria internazionale in materia penale. Queste misure sono applicate in un quadro giuridico preciso stabilito dalla legge federale del 6 ottobre 2002 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT; RS *780.1*). Di regola devono essere approvate da un giudice e possono essere oggetto di un ricorso al Tribunale federale.

Le misure di sorveglianza telefonica nell'ambito di procedure penali non sono oggetto del presente rapporto, limitato alle intercettazioni destinate a servizi d'informazione. Questi due generi di intercettazione sono rigorosamente distinti per quanto riguarda la loro finalità e il loro contesto legale ed è molto importante non confonderli.

Il presente rapporto si occupa unicamente delle intercettazioni satellitari effettuate mediante Onyx. La sorveglianza di collegamenti radio a onde corte e l'esplorazione radio a livello operativo o tattico, in particolare nel caso di un impiego dell'esercito in Svizzera o all'estero, non sono trattate.

2.3 Svolgimento dei lavori

La DCG si occupa della messa in opera del progetto Onyx da gennaio 1999. Tra questa data e la fine di ottobre 2003, ha dedicato al progetto 17 sedute nel corso delle quali ha sentito le persone[1] e i servizi seguenti, di cui alcune/i più volte:

– il capo del DDPS (12.11.99, 14.3.2001, 18.9.2001, 12.11.2001, 19.5.2003);
– il relatore del capo del DDPS per compiti speciali (15.9.2000, 5.7.2002);
– il coordinatore dei servizi d'informazione e/o il suo sostituto (26.3.2001, 12.11.2001, 5.7.2002, 28.1.2003, 19.5.2003);
– il capo dello Stato maggiore generale (15.9.2000, 19.5.2003);
– il capo dell'Ispettorato del DDPS e un esperto (8.2.2002);
– rappresentanti del Gruppo dell'aiuto alla condotta di Stato maggiore generale e in particolare della Divisione della condotta della guerra elettronica (CGE) (26.3.2001, 28/29.5.2001, 12.11.2001, 8.2.2002, 5.7.2002, 28.1.2003, 19.5.2003);
– il sottocapo di stato maggiore del Servizio informazioni (28.1.1999) e il suo sostituto (15.9.2000);

[1] Cfr. elenco delle persone sentite, allegato 2.

– rappresentanti del SIS (29./30.1.2001, 26.3.2001, 12.11.2001, 8.2.2002, 5.7.2002, 7.10.2002);
– rappresentanti del servizio dell'Ispettorato e compiti speciali della Segreteria generale del DFGP (28./29.5.2001);
– rappresentanti dell'Ufficio federale di polizia e del SAP (4.7.2001, 12.11.2001, 22.11.2001, 22.1.2002, 5.7.2002, 19.5.2003);
– un rappresentante del Segretariato di Stato dell'economia (Commercio mondiale, 5.7.2002).

La Delegazione ha anche effettuato due visite agli impianti di esplorazione di Onyx, di cui una inaspettata. Nell'occasione, ha discusso con i responsabili molte domande relative al funzionamento, alla sicurezza, al finanziamento e ai mandati affidati a Onyx nonché alle relazioni fra il DDPS e Swisscom. La Delegazione si è anche recata alla sede del SIS per incontrarvi i collaboratori incaricati dell'elaborazione degli ordini di esplorazione.

La Delegazione ha avuto anche diversi scambi di corrispondenza con il Consiglio federale, con la Delegazione del Consiglio federale per la sicurezza, con il capo del DDPS e con il capo del DFGP. Nelle lettere sono stati trattati i temi seguenti: compiti e legalità dell'esplorazione elettronica, controllo dei mandati di esplorazione, trattamento e protezione dei dati personali, collaborazione con l'estero, vigilanza politica del Consiglio federale e dei dipartimenti interessati (DDPS, DFGP) sulle intercettazioni.

La DCG ha trattato diversi rapporti, di cui uno dell'ispettorato del DDPS, datato del 9 maggio 2001, dedicato a un'ispezione effettuata presso la CGE. Ha anche esaminato un rapporto di revisione del Controllo federale delle finanze (CDF) sul finanziamento del progetto, datato del 15 agosto 2003. La Delegazione ha anche interrogato i servizi del SIS e del Controllo federale delle finanze su alcuni aspetti relativi all'impiego dei crediti per il finanziamento di Onyx. La Delegazione ha anche preso conoscenza dei differenti interventi parlamentari relativi alle intercettazioni di comunicazioni[2].

Nelle sue riflessioni, la DCG ha approfittato dei lavori effettuati da altri Parlamenti europei. La Delegazione ha in particolare studiato differenti rapporti allestiti dal

2 98.5085 Domanda. Spionaggio informatico su vasta scala con Echelon, del 15.6.1998 (Boll. Uff. **1998** N 1162); 99.3416 Interpellanza. Sorveglianza elettronica su incarico dei servizi informazioni, del 31.8.1999 (Boll. Uff. **2000** N 736); 00.3629 Interpellanza. Stazione terrestre per satelliti a Leuk, del 28.11.2000 (Boll. Uff. **2001** N 365); 00.5144 Ora delle domande. Satos 3. Controllo parlamentare, del 25 settembre 2000 (Boll. Uff. **2000** N 958); 01.3189 Postulato. Satos 3. Vendita di terreno a Leuk da parte di Swisscom, del 23.3.2001 (tolto di ruolo dopo due anni senza essere trattato); 01.3601 Interpellanza. Sicurezza dei dati. Situazione, del 5.10.2001 (Boll. Uff. **2002** N 467); 01.5095 Ora delle domande. Sistema d'intercettazione globale Echelon, del 18.6.2001 (Boll. Uff. **2001** N 757); 03.1046 Interrogazione ordinaria. Spionaggio economico su territorio svizzero a vantaggio degli Stati Uniti, dell'8.5.2003 (Boll. Uff. **2003** N 1758).

Parlamento francese, da quello europeo e da quello belga[3] sulle reti di sorveglianza e di esplorazione elettronica. Questi rapporti concernono principalmente la rete Echelon, una rete di sorveglianza mondiale delle telecomunicazioni concepita e coordinata dall'Agenzia americana per la sicurezza nazionale (*National Security Agency*, NSA). La Delegazione ha anche ricevuto due rapporti sul sistema Echelon: il primo elaborato dal SAP nel febbraio 2000 e il secondo dai servizi del coordinatore dei servizi d'informazione nel febbraio 2001.

I lavori della Delegazione sono stati coordinati con quelli della Commissione della politica di sicurezza del Consiglio nazionale (CPS-N) che si è occupata anch'essa del dispositivo Onyx. In virtù di un accordo concluso fra la Delegazione e la CPS-N, è stato convenuto che a occuparsi della sorveglianza del sistema Onyx sarebbe stata la Delegazione, non essendo la CPS-N autorizzata a intervenire nei settori segreti della Confederazione[4].

La Delegazione ha informato regolarmente le Commissioni della gestione (CdG) sullo stato di avanzamento dei lavori. Ha anche pubblicato due comunicati stampa rispettivamente il 19 settembre 2000 e il 27 marzo 2001 e ha descritto le sue attività nei rapporti annuali delle CdG[5].

In base alle informazioni ottenute durante i suoi lavori, la Delegazione ha elaborato un progetto di rapporto e ha trasmesso le relative conclusioni provvisorie al Consiglio federale il 16 ottobre 2003. Quest'ultimo ha preso posizione in un parere del 29 ottobre 2003. Il rapporto finale tiene conto delle osservazioni del Consiglio federale.

La Delegazione ha sottoposto il suo rapporto finale alle Commissioni della gestione il 21 novembre 2003. Le CdG hanno deciso all'unanimità di pubblicarlo.

La DCG ci tiene a rilevare che ha potuto svolgere i suoi lavori in piena indipendenza e che non è mai stata ostacolata nelle sue attività. Ha avuto accesso a tutte le informazioni necessarie per svolgere il suo compito. La Delegazione desidera ringraziare in questa sede tutti i servizi interessati per la loro collaborazione attiva e costruttiva.

3 Rapport de la Commission de la défense nationale et des forces armées de l'Assemblée nationale française su les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, dell'11.10.2000 (rapporto informativo di Arthur Paecht) (qui di seguito: rapporto francese); rapporto della Commissione temporanea del Parlamento europeo sull'esistenza di un sistema d'intercettazione globale delle comunicazioni private e economiche (sistema d'intercettazione ECHELON)(2001/2098(INI)), dell'11.7.2001 (qui di seguito: rapporto europeo); rapport de la Commission chargée du suivi du comité permanent de contrôle des services de renseignements et de sécurité et de la Commission spéciale chargée de l'accompagnement parlementaire du comité permanent de contrôles des services de police du Sénat et de la Chambre des représentants de Belgique consacré a l'existence éventuelle d'un réseau d'interception des communications, nommé «ECHELON», del 25.2.2002 (qui di seguito: rapporto belga).

4 Cfr. comunicato stampa della CPS-N, del 10.4.2001.

5 Cfr. il rapporto annuale 2000/2001 delle Commissioni della gestione e della Delegazione delle Commissioni della gestione delle Camere federali, del 22.5.2001 (FF **2001** 5027) e il rapporto annuale 2001/2002 delle Commissioni della gestione e della Delegazione delle Commissioni della gestione delle Camere federali, del 17.5.2002 (FF **2002** 5297).

2.4 Mantenimento del segreto

Il principio della Delegazione è di informare con la massima trasparenza e di pubblicare i risultati dei suoi lavori. Per raggiungere l'obiettivo, la Delegazione deve talvolta rinunciare a dare indicazioni dettagliate su determinate questioni soggette all'obbligo del segreto. Per godere della fiducia del Parlamento, la Delegazione deve dare molte informazioni; per conquistare la fiducia dei servizi sorvegliati, deve dare prova di riservatezza. La Delegazione opera al confine tra trasparenza e segretezza e deve fare in modo di tenere adeguatamente conto dell'una e dell'altra.

Come già detto, la Delegazione ha avuto acceso a tutte le informazioni utili allo svolgimento del suo mandato di controllo su Onyx. Certe informazioni sono classificate come segrete e non possono essere pubblicate. Nell'elaborare il presente rapporto, la Delegazione ha pertanto dovuto conciliare il rapporto fra l'obbligo di informare il Parlamento e l'opinione pubblica nel modo più completo possibile e l'obbligo di mantenere il segreto necessario al funzionamento di determinati servizi dello Stato.

La DCG ha deciso di non dare nel suo rapporto indicazioni dettagliate sulle capacità, sui costi e sul rendimento del sistema Onyx. Ritiene infatti che la pubblicazione di queste informazioni non sia indispensabile e non serva alla comprensione del soggetto. La Delegazione pensa anche che la divulgazione di queste informazioni potrebbe danneggiare le relazioni estere della Svizzera e compromettere l'applicazione di misure destinate a proteggere la sicurezza interna e esterna del Paese. In certi casi, si tratta anche di tutelare la sfera privata di terzi.

Per la Delegazione, è importante non confondere riservatezza e silenzio totale. Se su determinate questioni mantiene un certo riserbo, la DCG non lo fa per coprire attività criticabili o azioni illegali, ma per proteggere i mezzi, le fonti e le procedure di raccolta di informazioni della Confederazione. Limitandosi a mantenere segrete le informazioni la cui comunicazione potrebbe pregiudicare interessi pubblici o privati preponderanti, la Delegazione vuole anche far risaltare l'importanza del segreto quando è necessario.

La Delegazione è consapevole che questa restrizione non è del tutto soddisfacente, ma è solo a questo prezzo che il presente rapporto può essere pubblicato.

3 Osservazioni generali e situazione all'estero

3.1 Definizioni

Tutti gli Stati del mondo dispongono di servizi di informazione più o meno sviluppati per la raccolta e l'analisi di informazioni destinate agli organi decisionali militari e politici.

Questi servizi possono perseguire diversi obiettivi. All'origine, servivano soprattutto a raccogliere informazioni di natura militare o diplomatica. Successivamente, con l'aumento degli scambi, l'interesse si è allargato ad altri tipi di informazioni relative alla sicurezza (terrorismo, crimine organizzato, proliferazione delle armi ecc.), ma anche, in certi casi, alla tecnologia, alle scienze e al commercio.

I servizi di informazione – la Svizzera non costituisce un'eccezione – utilizzano diverse forme di raccolta di informazioni, che si completano a vicenda.

Le principali fonti di informazioni sono[6]:

- la raccolta di informazioni attraverso fonti aperte (open source intelligence, OSINT) come le banche dati, le pubblicazioni scientifiche, la letteratura specializzata, Internet ecc.;
- la raccolta di informazioni attraverso fonti umane (human intelligence, HUMINT) comunicate da addetti alla difesa e agenti (informatori, spie, agenti segreti ecc.);
- lo scambio di informazioni con altri servizi partner e con fonti terze;
- la raccolta di informazioni attraverso mezzi elettronici (signals intelligence, SIGINT). Questa tecnica permette di raccogliere informazioni per mezzo dell'ascolto di sistemi di trasmissione o dell'intercettazione di altre emissioni elettromagnetiche.

La raccolta elettronica di informazioni si suddivide in due grandi categorie:

- l'esplorazione radio o la raccolta di messaggi di comunicazione (communications intelligence, COMINT);
- l'esplorazione elettronica o la raccolta di segnali non di comunicazione (electronic intelligence, ELINT).

In altri termini, COMINT si occupa dell'intercettazione, dell'analisi e della trasmissione di emissioni radio che possono essere tradotte in linguaggio umano (come morse o le comunicazioni radio) o in forma di grafici. ELINT concentra la sua ricerca sui segnali elettronici che non servono alla comunicazione e che sono emessi da radar e da altri sistemi di armi nonché sull'analisi dei loro parametri tecnici (frequenza, modulazione, polarizzazione ecc.)[7].

Il sistema Onyx è una fonte di informazioni di tipo COMINT.

3.2 Panoramica dei sistemi di esplorazione negli altri Paesi

Negli ultimi anni diversi Stati hanno sviluppato sistemi di esplorazione delle comunicazioni. Nella maggior parte dei casi, questi sistemi sono a destinazione militare. In realtà sono pochi gli Stati che dispongono di sistemi strategici che permettono di intercettare su vasta scala comunicazioni militari, diplomatiche, commerciali o private. Secondo certe fonti, una trentina di Stati sarebbe in possesso di una capacità di esplorazione importante[8].

Non vi sono dati precisi in questo ambito; spesso, ci si deve accontentare di supposizioni e non si può affermare niente con certezza. Per evidenti ragioni, le informazioni su questi sistemi sono nella maggior parte dei casi tenute segrete dalle autorità dei Paesi interessati. Le fonti di informazioni aperte, invece, non sono sempre attendibili e talvolta addirittura si contraddicono. Dati di fatto e informazioni non verificate, se non addirittura inventate formano spesso un tutt'uno.

6 Cfr. l'opuscolo pubblicato dal DDPS e dal DFGP: «Die Nachrichtendienste der Schweiz», 1ª edizione, 2003, pag. 14 segg.

7 Cfr. la documentazione dell'esercito svizzero: «Le combat moderne en Europe», documentation 52.15f, valida dal 1º luglio 1999, pag. 99 segg.

8 Rapporto belga, pag. 17; rapporto dell'Ufficio federale di polizia, febbraio 2000, pag. 1 (non pubblicato).

Nel presente caso, la Delegazione si è basata su un numero limitato di fonti aperte, e in particolare sui rapporti del Parlamento francese, di quello belga e di quello europeo nonché su altre fonti pubbliche disponibili[9]. Si è fondata anche su un rapporto dell'Ufficio federale di polizia, datato del febbraio 2000, dedicato allo spionaggio economico e all'intercettazione delle comunicazioni, nonché su un rapporto realizzato nel febbraio 2001 dai servizi del coordinatore dei servizi d'informazione.

Gli Stati Uniti sono il Paese che dispone delle capacità più sviluppate in materia di servizio di informazione elettronica. L'organismo centrale responsabile delle intercettazioni è la *National Security Agency* (NSA) presso la quale lavorano quasi 40 000 collaboratori negli Stati Uniti e nel mondo e che dispone di un budget annuale nell'ordine di 4 miliardi di franchi. La NSA è il più grande ufficio di informazione degli Stati Uniti prima ancora della CIA (*Central Intelligence Agency*) e del FBI (*Federal Bureau of Investigations*). Si basa su una rete globale di esplorazione delle comunicazioni che comprende, oltre a satelliti di esplorazione, stazioni di ascolto dei satelliti di comunicazione, reti di radiocomunicazione terrestri nonché reti via cavo[10].

Secondo molte fonti, la NSA eserciterebbe anche, in collaborazione con la Gran Bretagna, il Canada, l'Australia e la Nuova Zelanda, una rete multinazionale di ascolto: la rete Echelon. Questo sistema sarebbe in grado di intercettare tutte le comunicazioni via satellite e di filtrarle grazie all'impiego di computer molto potenti, di parole chiave predefinite e di tecniche di riconoscimento della voce. Secondo certe fonti, Echelon ascolterebbe anche le comunicazioni trasmesse attraverso reti via cavo terrestri o sottomarine o ponti radio. In Gran Bretagna, è il *Government Communications Headquarters* (GCHQ) che è ufficialmente incaricato delle intercettazioni e disporrebbe di stazioni di ascolto in Belize, a Gibraltar, a Cipro, in Oman, in Turchia e in Australia.

La collaborazione fra gli Stati Uniti, la Gran Bretagna, il Canada, l'Australia e la Nuova Zelanda sarebbe formalizzata in un accordo segreto, denominato UKUSA. Questo accordo sarebbe stato firmato, alla fine degli anni 40, dagli Stati Uniti e dalla

9 Cfr. Nicky Hager, «Secret Power. New Zealand's Role in the International Spy Network», Craig Potton Publishing, Nelson, Nuova Zelanda, 1996. Cfr. anche il rapporto realizzato per l'Ufficio per la valutazione delle scelte scientifiche e tecnologiche (Science and Technology Options Assessment Panel, STOA) del Parlamento europeo: Steve Wright, «An appraisal of technologies of political control», Omega Foundation, studio ad interim, Lussemburgo, aprile 1997, PE 166.499 e i cinque rapporti su «Development of Surveillance Technology and Risk of Abuse of Economic Information», pubblicati da Dick Holdsworth per lo STOA: Peggy Becker, «Data protection and human rights in the European Union and the role of the European Parliament», Lussemburgo, ottobre 1999, PE.168.184, volume 1/5; Duncan Campbell, «The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition», Lussemburgo, ottobre 1999, PE 168.184, volume 2/5 (qui di seguito: rapporto Campbell); Franck Leprevost, «Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues», Lussemburgo, novembre 1999, PE 168.184, volume 3/5; Chris Elliot, «The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law», Lussemburgo, ottobre 1999, PE 168.184, volume 4/5; Nikos Bogolikos, «The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception», Lussemburgo, ottobre 1999, PE 168.184, volume 5/5.

10 Cfr. in particolare James Bamford, «Body of secrets. Anatomy of the ultra-secret National Security Agency», Doubleday, New York, 2001.

Gran Bretagna, poi ampliato al Canada che avrebbe concluso un accordo bilaterale con gli Stati Uniti (accordo CANUSA). L'Australia e la Nuova Zelanda sarebbero venute ad aggiungersi dopo. Secondo le fonti à disposizione, altri Paesi parteciperebbero indirettamente al sistema Echelon ospitando stazioni di esplorazione sul loro territorio o ricevendo informazioni da Echelon. Si tratterebbe in particolare della Germania, della Corea del Sud, del Giappone, della Norvegia, della Turchia[11] e di Cipro. Echelon costituirebbe il solo sistema multilaterale di esplorazione delle comunicazioni al mondo. Finora i Governi americani, britannici e canadesi non hanno mai riconosciuto l'esistenza dell'accordo UKUSA. Il governo neozelandese e il direttore australiano del servizio delle intercettazioni della difesa (*Defence Signals Directorate* [DSD]) hanno invece ammesso l'esistenza di questo accordo.

Inizialmente sviluppato per scopi militari, secondo certe fonti Echelon sarebbe sempre più spesso utilizzato per scopi di spionaggio economico e di sorveglianza della concorrenza al fine di promuovere gli interessi delle imprese americane e di aumentare la loro quota di partecipazione al mercato. Gli Stati Uniti non negano di fare dello spionaggio economico, ma – affermano – unicamente per lottare contro le imprese che non rispettano gli embargo internazionali, che sviluppano tecnologie a doppio uso, civile e militare, o che pagano Commissioni per «strappare» contratti[12]. Sinora, nessuna impresa ha fatto ricorso, in Europa o negli Stati Uniti, per eventuali danni provocati da intercettazioni elettroniche.

Echelon pone anche una serie di problemi giuridici e politici in seno all'Unione europea (UE) a causa della doppia appartenenza del Regno Unito all'UE e all'accordo UKUSA e delle distorsioni della concorrenza che eventuali intercettazioni economiche potrebbero provocare.

Anche se numerosi lavori e rapporti ufficiali sono stati dedicati a Echelon, sono poche le informazioni attendibili a disposizione sugli obiettivi e sulle capacità reali del sistema. I rapporti ufficiali si riferiscono molto spesso alle stesse fonti e presentano le stesse informazioni. Secondo il rapporto dell'Assemblea nazionale francese, questa «somiglianza delle informazioni e il fatto che esse non si prestino all'analisi possono testimoniare di una volontà deliberata di orientare il dibattito sulle intercettazioni delle comunicazioni in una direzione precisa, volontà alla quale la comunità dei servizi d'informazione non sarebbe del tutto estranea»[13]. Del resto stupisce l'improvviso interesse dell'opinione pubblica per Echelon dopo la fine degli anni Novanta, visto che questo sistema era conosciuto dagli specialisti da molto tempo.

Il rapporto del Parlamento europeo costituisce con ogni probabilità l'analisi più dettagliata delle possibilità e dei limiti del sistema Echelon. Secondo il rapporto l'esistenza di questo sistema mondiale di esplorazione delle comunicazioni è fuor di dubbio[14] e la NSA collabora con altri servizi nel settore COMINT[15]. Il rapporto precisa tuttavia anche che le possibilità del sistema non sono così grandi come

11 Secondo la *Free Congress Research and Education Foundation* con sede a Washington D.C., citata da Jacques Isnard, «La CIA et la NSA justifient les missions du réseau d'espionnage Echelon», in: *Le Monde*, 10.3.2000, pag. 5.

12 Cfr. le dichiarazioni fatte dall'ex direttore della CIA, James Woolsey, al *Foreign Press Center* di Washington D.C. il 7.3.2000 e il suo articolo «Why we spy on our allies», in: *The Wall Street Journal*, 17.3.2000, pag. A18.

13 Rapporto francese, pag. 25.

14 Rapporto europeo, pag. 17.

15 Rapporto europeo, pag. 71.

supposto. Le conclusioni del rapporto del Parlamento europeo sono condivise dal Consiglio federale[16].

Il rapporto francese e quello belga sono più espliciti e considerano l'esistenza di Echelon come sicura.

Anche se altri Paesi possiedono capacità di spionaggio elettronico, nessuno può rivaleggiare con le capacità di esplorazione degli Stati Uniti. Secondo il rapporto del Parlamento europeo e di altre fonti non ufficiali[17], anche la Francia disporrebbe di una rete di ascolto globale. Questa rete sarebbe stata realizzata negli ultimi dieci anni dal servizio d'informazione estero, la *Direction générale de la sécurité extérieure* (DGSE). Comprenderebbe basi di esplorazione, satellitari o altre, in Francia, ma anche negli Emirati Arabi Uniti[18], a Kourou (Guyana francese) nonché sull'isola francese di Mayotte (Comores) nell'Oceano indiano. Queste due ultime basi sarebbero gestite in comune con il servizio di informazione estera tedesco, il *Bundesnachrichtendienst* (BND). Grazie alla vasta copertura geografica delle stazioni terrestri, la Francia sarebbe in grado di intercettare comunicazioni via satellite dappertutto nel mondo. Secondo un rapporto ufficiale dell'Assemblea nazionale francese, l'intercettazione di telecomunicazioni via satelliti continua a restare una priorità della DGSE[19]. Anche la Francia dispone di satelliti di spionaggio nonché, sul piano operativo, di capacità di ascolto della Marina e dell'Aviazione, che possono essere impiegate nelle zone d'intervento.

Secondo il rapporto del Parlamento europeo, anche la Russia disporrebbe, senza che sia possibile confermarlo, di un sistema di esplorazione di portata mondiale con stazioni di ascolto terrestri a Cuba e nel Vietnam[20].

Sembra che anche altri Stati dell'Unione europea dispongano di capacità di informazione elettronica, tuttavia più limitate. È il caso della Danimarca, della Finlandia, della Germania, dei Paesi Bassi, della Spagna, della Svezia e della Gran Bretagna[21]. Secondo il rapporto del Parlamento belga, che cita un giornalista, la Germania disporrebbe di una base nella Repubblica popolare di Cina, a Taiwan e – in collaborazione con la Francia – nella Guyana francese[22].

Nel resto del mondo, anche la Cina, l'India, Israele e il Pakistan disporrebbero di capacità SIGINT di una certa entità[23].

16 Cfr. la risposta del Consiglio federale del 15.3.2002 all'interpellanza 01.3601 Sicurezza dei dati. Stato della situazione (Boll. Uff. **2002** N 468).
17 Jacques Isnard, «Le Royaume-Uni au cœur du dispositif en Europe», in: *Le Monde*, 23.2.2000, pag. 2. Cfr. anche Vincent Jauvert, «Espionnage, comment la France écoute le monde», in: *Le Nouvel Observateur*, n. 1900, 5.4.2001, pag. 14 segg.
18 Rapporto dell'Ufficio federale di polizia, febbraio 2000, pag. 9 (non pubblicato).
19 Rapport fait au nom de la Commission des finances, de l'économie générale et du plan de l'Assemblée nationale sur le projet de loi des finances pour 2003, del 10.10.2002, rapporto n. 256, allegato n. 36, Secrétariat général de la défense nationale et renseignement, relatore speciale: Bernard Carayon, pag. 11.
20 Rapporto europeo, pag. 13 e pag. 85 segg.
21 Rapporto europeo, allegato IV.
22 Rapporto belga, pag. 37.
23 Rapporto Campbell, pag. 1, cap. 7.

4 Descrizione del sistema Onyx

4.1 Introduzione

Onyx è un sistema COMINT di esplorazione delle comunicazioni militari e civili che transitano via satelliti (COMSAT). Permette di captare le trasmissioni e i trasferimenti di dati quali le chiamate telefoniche, le telecopie, i telex, le e-mail e i dati informatici. Questo sistema completa l'ascolto dei segnali radio a onde corte, che sono stati, a lungo, la sola forma di informazione elettronica utilizzata dalle autorità svizzere.

La decisione di realizzare Onyx è stata presa dal Consiglio federale il 13 agosto 1997 su proposta del DDPS. L'obiettivo che si vuole raggiungere con il sistema è di intercettare le comunicazioni relative al terrorismo internazionale, all'estremismo violento, al crimine organizzato, allo spionaggio e alla proliferazione delle armi nonché tutte le altre informazioni concernenti la politica di sicurezza. Le informazioni acquisite devono migliorare le possibilità del Consiglio federale di riconoscere per tempo, e indipendentemente dall'estero, le minacce e i rischi nel settore della politica di sicurezza.

Il sistema Onyx può essere utilizzato solo per intercettazioni al di fuori delle frontiere del Paese.

Dopo la fase di sviluppo, il sistema Onyx è stato messo in funzione nell'aprile 2000. Da aprile 2001, il sistema è nella fase di esercizio pilota. Durante questa fase, l'accento è posto soprattutto sull'intercettazione di comunicazioni concernenti le armi di distruzione di massa.

Il sistema passerà alla fase operativa nel corso del 2004 sui siti di Zimmerwald, Heimenschwand e di Leuk. La piena operatività è prevista per la fine del 2005/l'inizio del 2006. Nel frattempo, il numero di antenne deve essere raddoppiato.

Il finanziamento del sistema Onyx è assicurato dal budget ordinario del materiale d'armamento dell'Aggruppamento dell'armamento che è esaminato annualmente dalle Commissioni delle finanze e approvato dalle Camere federali (rubriche 540.3210.001[24] e 540.3220.001[25]). Il finanziamento delle relative costruzioni è stato approvato con decreto federale del 9 dicembre 1999 sugli immobili militari 2000[26] e iscritto nel budget dello Stato maggiore generale (rubrica 510.3200.001). Il personale supplementare necessario è messo a disposizione dallo Stato maggiore generale.

La DCG e la Delegazione delle finanze hanno preso atto dei costi d'investimento e delle spese d'esercizio annuali dell'impianto. Questi dati non sono indicati qui per motivi di segretezza.

24 Rubrica «Progettazione, prove e preparativi degli acquisti di materiale d'armamento»[in tedesco: «Projektierung, Erprobung und Beschaffungsvorbereitung von Rüstungsmaterial (PEB)»].

25 Rubrica «equipaggiamento personale e bisogni d'ammodernamento» [in tedesco: «Ausrüstung und Erneuerungsbedarf (AEB)»].

26 Cfr. il messaggio del Consiglio federale sugli immobili militari 2000, del 18.8.1999, FF **1999** 7431.

4.2 Basi legali

L'esercizio del sistema Onyx è basato principalmente sull'articolo 99 LM[27]. Questo articolo costituisce la base legale delle attività di servizio d'informazione della Confederazione all'estero:

Art. 99 LM Servizio informazioni

1 Il servizio informazioni ha il compito di raccogliere, valutare e diffondere informazioni concernenti l'estero rilevanti sotto il profilo della politica di sicurezza.

2 Ha facoltà di trattare dati personali, compresi quelli particolarmente degni di protezione e profili della personalità, se del caso anche all'insaputa della persona interessata, sempreché e finché i suoi compiti lo esigano. In singoli casi può trasmettere dati personali all'estero, in deroga alle disposizioni in materia di protezione dei dati.

2bis Può trasmettere all'Ufficio federale di polizia informazioni su persone in Svizzera risultanti dalla propria attività di cui al capoverso 1 e che possono essere rilevanti per la sicurezza interna e il perseguimento penale.

3 Il Consiglio federale disciplina:

a. i compiti in dettaglio e l'organizzazione del servizio informazioni, nonché la protezione dei dati;

b. l'attività del servizio informazioni nel servizio di promovimento della pace, nel servizio d'appoggio e nel servizio attivo;

c. la collaborazione del servizio informazioni con i servizi interessati della Confederazione e dei Cantoni nonché con i servizi esteri;

d. le eccezioni alle prescrizioni concernenti la registrazione di collezioni di dati, quando queste pregiudicassero la raccolta d'informazioni.

4 La tutela delle fonti dev'essere in ogni caso garantita.

5 Il servizio informazioni è direttamente subordinato al capo del Dipartimento della difesa, della protezione della popolazione e dello sport.

L'articolo è completato dall'ordinanza del 4 dicembre 2000 sul servizio informazioni del Dipartimento federale della difesa, della protezione della popolazione e dello sport (Ordinanza sul servizio informazioni, OSINF; RS *510.291*). Questa ordinanza precisa in particolare che il SIS «assicura in permanenza il servizio informazioni concernente l'estero» e che «in stretta collaborazione con altri organi federali, raccoglie, per la direzione politica e militare, le informazioni rilevanti per la sicurezza della Confederazione» (art. 2 OSINF).

Le attività di Onyx per il SAP risultano dall'incarico di garantire la sicurezza interna e sono basate sulla legislazione relativa alla protezione preventiva dello Stato, in primo luogo sulla legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI; RS *120*). L'articolo 14 LMSI descrive in maniera esaustiva le informazioni che il SAP può cercare nell'esercizio del suo mandato legale:

27 Con modifica del 4 ottobre 2002; l'art. 99 cpv. 2bis, cpv. 3 lett. b e c, cpv. 4 e cpv. 5 entrerà in vigore il 1° gennaio 2004.

Art. 14 LMSI Ricerca di informazioni

1 Gli organi di sicurezza federali e cantonali raccolgono le informazioni necessarie all'adempimento dei compiti secondo la presente legge. Essi possono ricercare tali informazioni anche all'insaputa della persona interessata.

2 I dati personali possono essere raccolti con:

a. valutazione delle fonti accessibili al pubblico;

b. richiesta di informazioni;

c. consultazione di fascicoli ufficiali;

d. ricezione e valutazione di comunicazioni;

e. ricerca dell'identità o del soggiorno delle persone;

f. osservazione dei fatti in luoghi pubblici e liberamente accessibili, anche ricorrendo a registrazioni di immagini e suoni;

g. accertamento dei movimenti e contatti delle persone.

3 L'impiego di misure coercitive procedurali penali è ammissibile soltanto nel quadro di una procedura delle indagini preliminari della polizia giudiziaria o di un'istruzione preparatoria. Lo stesso dicasi per l'osservazione di fatti in ambienti privati.

La LM e la LMSI fissano i principi e le competenze in materia di raccolta di informazioni da parte dei servizi di informazione. I dettagli dell'esplorazione radio sono disciplinati nell'ordinanza concernente la condotta della guerra elettronica (OCGE), che il Consiglio federale ha adottato il 15 ottobre 2003 (RU *2003* 3971)[28]. Questa ordinanza è entrata in vigore il 1° novembre 2003.

La LM e l'OCGE disciplinano anche gli scambi di informazioni quando indicazioni relative alla sicurezza interna o ad attività criminali in Svizzera sono rilevate involontariamente[29]. Di regola queste informazioni concernenti la Svizzera non sono trasmesse al SIS, che non è autorizzato a procedere ad attività di esplorazione nel Paese. L'articolo 99 capoverso 2bis LM prevede la possibilità, per gli agenti della CGE, di trasmettere le informazioni concernenti la Svizzera o utenti svizzeri direttamente all'Ufficio federale di polizia, che a sua volta può trasmetterle alle autorità penali competenti.

La collaborazione fra il SIS e il SAP è disciplinata in una direttiva dei capi del DDPS e del DFGP del 19 marzo 1997 e in una convenzione fra il SIS e il SAP del 6 febbraio 2003.

28 Cfr. comunicato stampa del DDPS, del 15.10.2003.
29 L'OCGE parla, in simili casi, di «sottoprodotti»; cfr. art. 5 cpv. 3 OCGE.

4.3 Ciclo dei servizi d'informazione

Onyx è uno strumento di raccolta di informazioni. La sua attività si svolge in un ciclo di cui costituisce una tappa[30]:

- la prima fase – *la fase di pianificazione e condotta* – consiste nel determinare i bisogni di informazioni e nel pianificarne la raccolta. Questo compito spetta al SIS e al SAP sulla base dei compiti generali assegnati loro rispettivamente dalla legge e dall'ordinanza oppure per mandato delle autorità politiche responsabili (Delegazione del Consiglio federale per la sicurezza, capi del DDPS e del DFGP).
- La seconda fase – *la fase di raccolta* vera e propria – ha per obiettivo la raccolta di informazioni presso le fonti. Vi prendono parte diversi attori e differenti servizi. Nel corso di questa fase Onyx funge da strumento di raccolta. I procedimenti e i metodi di raccolta, sia elettronici che umani, sono generalmente tra i segreti meglio custoditi dai servizi di informazione.
- La terza fase – *la fase di analisi* – è la parte del ciclo che consiste nell'analisi e nell'interpretazione delle informazioni raccolte. È nel corso di questa fase che le informazioni diventano messaggi. Questa fase è assicurata dai servizi di analisi del SIS e del SAP.
- La quarta e ultima fase si chiama *la fase di diffusione;* nel corso di questa fase le informazioni sono istradate in forma di rapporti verso gli organi richiedenti. Questa fase è sottomessa a severe regole in materia di segretezza per evitare che i destinatari si impadroniscano delle procedure di raccolta di informazioni e possano identificarne le fonti.

4.4 Esercizio

Onyx è esercitato dalla Divisione della condotta della guerra elettronica (CGE) che fa parte del Gruppo dell'aiuto alla condotta dello Stato maggiore generale. Il sistema intercetta le comunicazioni che transitano via satellite mediante collegamenti elettromagnetici fra i satelliti di comunicazione – generalmente in orbita geostazionaria – e le stazioni terrestri[31] (cfr. schema 1).

Vi sono diversi tipi di satelliti di comunicazione (Intelsat, Inmarsat, Eutelsat, PanAmSat, Arabsat, Gorizont ecc.), che offrono alla loro clientela differenti tipi di prestazioni. Ad esempio, la rete Intelsat propone servizi nell'ambito delle comunicazioni fra reti terrestri fisse («fixed satellite services»). Attualmente dispone di 24 satelliti che servono il continente americano, l'Africa, l'Europa, l'Asia nonché il Pacifico. Il sistema Inmarsat, che ha le stesse zone di copertura di Intelsat, offre prestazioni satellitari fra una rete telefonica terrestre e utenti mobili come aerei, navi, piattaforme offshore («mobile satellite services»).

L'intercettazione delle comunicazioni attraverso Onyx si svolge per mezzo di antenne paraboliche che hanno un diametro fra 4 e 18 metri. Tutte le antenne del sistema

30 Cfr. Jacques Baud, «Encyclopédie du renseignement et des services secrets», Lavauzelle, Parigi, 2002, pag. 196.

31 Per maggiori informazioni sugli aspetti tecnici dell'intercettazione delle comunicazioni e sulla tecnica delle comunicazioni satellitari, si consiglia di leggere i capitolo 3 e 4 del rapporto del Parlamento europeo, pag. 32 segg.

Onyx sono situate sul territorio svizzero. Ricevono i fasci di onde che i satelliti di comunicazioni inviano verso la terra («downlinks»).

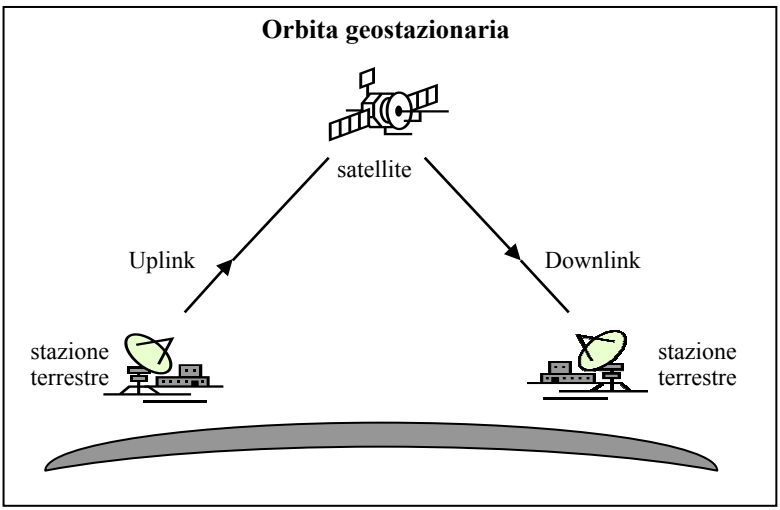
In generale, i fasci di onde inviati verso la terra non sono focalizzati in una zona geografica precisa, ma distribuiti su più Paesi («footprint»). Questa zona può rappresentare fino al 50 per cento della superficie terrestre se il segnale non è concentrato. In Europa, ad esempio, le zone di copertura di Intelsat e Inmarsat si estendono generalmente a tutta l'Europa. Basta dunque disporre di una stazione ricevente in Svizzera per intercettare le comunicazioni via satellite di tutta l'Europa. Di regola occorre un'antenna per ogni satellite che si intende intercettare.

L'intercettazione è limitata alle comunicazioni internazionali civili e militari. L'intercettazione e l'analisi di comunicazioni civili che hanno luogo in Svizzera sono vietate.

Il sistema Onyx funziona 24 ore su 24, 365 giorni all'anno.

Schema 1

Comunicazioni via satellite (Schema semplificato)



4.5 Mandati di esplorazione

La CGE svolge intercettazioni solo su mandato dei servizi debitamente autorizzati (designati qui di seguito mandanti). Per il momento, secondo una decisione presa dalla Delegazione del Consiglio federale per la sicurezza il 10 giugno 2002[32], solo il SIS e il SAP hanno la qualità di mandante per quanto riguarda le intercettazioni satellitari. È previsto che il capo del DDPS possa allargare la qualità di mandanti ad

32 n. 3.2. del mandato di base del Servizio informazioni strategico, del 10.6.2002 (non pubblicato).

altri servizi a condizione che dispongano di basi legali sufficienti (ad esempio: il servizio informazioni militare e il servizio informazioni delle Forze aeree). Ci si può anche immaginare l'impiego di Onyx quale servizio di assistenza dell'esercito (ad esempio, per assicurare la sicurezza del *World Economic Forum* di Davos). Una simile decisione dovrebbe essere presa dal Consiglio federale e dal Parlamento.

I principi della collaborazione fra la CGE e i mandanti sono fissati nell'OCGE nonché in convenzioni quadro concluse con ogni mandante. Le convenzioni quadro devono obbligatoriamente rivestire la forma scritta (art. 3 cpv. 2 OCGE). Fissano inoltre le relative responsabilità, gli standard di sicurezza da adottare, i processi di gestione e la definizione dei prodotti attesi.

Finora sono state stipulate una convenzione quadro fra la CGE e il SIS, il 3 ottobre 2001 e una convenzione quadro fra il Gruppo dell'aiuto alla condotta dello Stato maggiore generale (da cui dipende la CGE) e il SAP, il 1º aprile 1998.

Sulla base delle convenzioni quadro, i mandanti fissano i mandati di esplorazione individuali che devono essere oggetto di una convenzione scritta sulle prestazioni fra il mandante e la CGE (art. 3 cpv. 3 OCGE). Le convenzioni sulle prestazioni precisano i punti importanti dell'esplorazione in funzione di zone geografiche o di temi precisi legati alla politica di sicurezza della Svizzera. Per ogni tema e per ogni regione geografica di interesse deve essere stipulata una convenzione di prestazioni propria.

Le convenzioni sulle prestazioni contengono tutti gli elementi necessari all'esecuzione dei mandati e al loro controllo. Comprendono in particolare gli oggetti di esplorazione cercati (nomi di persone, di organizzazioni o di imprese, elementi di indirizzo ecc.) nonché la lista delle parole chiave (*key words*) che il mandante si attende che figurino nelle comunicazioni intercettate. Tutte queste informazioni sono necessarie per l'elaborazione dei sistemi di filtraggio automatico delle comunicazioni. A seconda dei mandati, vi possono essere fra 5 e diverse centinaia di parole chiave. Ad esempio, nel settore della lotta contro la proliferazione delle armi, la lista delle parole chiave conta più di dieci pagine, con 25 termini per pagina.

Quanto più le parole chiave sono precise, tanto più pertinenti sono le informazioni ricevute. Termini come «terrorismo», «bomba» o «antracite» non fanno al caso perché non compaiono praticamente mai in questa forma in una comunicazione fra due utenti.

Le liste degli elementi d'indirizzo o di parole chiave non devono contenere nessuna indicazione relativa a utenti svizzeri. I numeri di telefono o di telefax con, ad esempio, l'indicativo internazionale per la Svizzera (0041) sono vietati a meno che non sia tecnicamente provato che l'apparecchio si trova all'estero. È il caso in particolare di certi tipi di telefonini.

Spetta ai mandanti assicurarsi della legalità e della proporzionalità dei mandati di esplorazione affidati alla CGE (art. 14 OCGE). Un'istanza di controllo indipendente (ICI), composta di rappresentanti di differenti dipartimenti, verifica i mandati di esplorazione (art. 15 OCGE). L'ICI verifica ogni mandato e l'aggiunta di nuovi oggetti dell'esplorazione radio ai mandati esistenti. Essa verifica anche l'acquisizione dei risultati delle esplorazioni radio nonché la loro trasmissione ed elaborazione ulteriore presso il mandante (art. 15 cpv. 2 OCGE). L'ICI può, se necessario, chiedere al dipartimento del mandante la sospensione di mandati di esplorazione

radio che non soddisfano o non soddisfano più i principi della legalità e della proporzionalità.

Sul piano teorico, sarebbe possibile definire un numero illimitato di convenzioni sulle prestazioni. Sul piano tecnico, le possibilità sono limitate. Si devono dunque fissare priorità nella ricerca delle informazioni. Queste priorità sono stabilite dai mandanti.

Attualmente vi sono una trentina di mandati di prestazioni fra il SIS e le CGE e un mandato di prestazioni fra il SAP e il Gruppo dell'aiuto alla condotta dello Stato maggiore generale. Questi mandati riguardano la lotta contro la proliferazione delle armi, il controspionaggio, la criminalità organizzata e la lotta contro il terrorismo nonché la situazione nel Golfo.

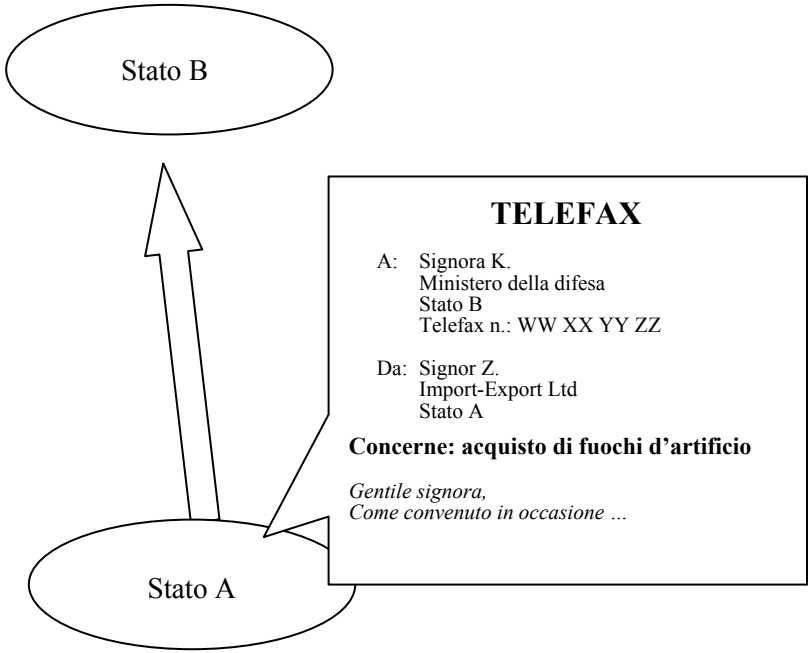
La Delegazione conosce le convenzioni quadro concluse fra il SIS e la CGE da una parte e fra il SAP e la CGE dall'altra. Ha accesso anche a tutte le convenzioni sulle prestazioni.

4.6 Raccolta di informazioni

In base alle convenzioni sulle prestazioni, la CGE effettua la raccolta delle informazioni provenienti da sistemi di telecomunicazione all'estero.

A tal fine, Onyx deve prima di tutto accedere al canale di trasmissione e identificarlo. Si tratta durante questa fase di rilevare solo le comunicazioni potenzialmente interessanti e di eliminare tutto ciò che concerne il settore pubblico, per esempio i programmi della radio e della televisione che transitano via satellite. La seconda fase consiste nell'analizzare automaticamente il contenuto decifrabile della comunicazione per filtrarlo automaticamente. Il filtraggio si effettua mediante sistemi d'intelligenza artificiale. Questi sistemi confrontano il contenuto del messaggio con gli elementi d'indirizzo e le parole chiave predefinite (cfr. schema 2). I messaggi che non rispondono a nessuno di questi criteri sono eliminati automaticamente.

Esempio di esplorazione di una comunicazione per telefax fra due utenti all'estero



Commento allo schema 2:

Se il *numero di chiamata* del destinatario del telefax (nell'esempio: *«WW XX YY ZZ»*) è contenuto in una convenzione sulle prestazioni, Onyx può intercettare tutti i telefax spediti al Ministero della difesa dello Stato B, a condizione tuttavia che la comunicazione transiti via satellite. Se la quantità delle comunicazioni è elevata, è possibile fissare nella convenzione sulle prestazioni *parole chiave* destinate a filtrare maggiormente le informazioni (ad esempio: *«fuochi d'artificio»*).

La procedura di filtraggio è relativamente semplice se i messaggi sono trasmessi in forma di testo come è il caso delle e-mail o dei telex. È invece molto più complessa se il sistema deve leggere messaggi stampati o manoscritti, in quanto occorre un'operazione di riconoscimento ottico dei caratteri, o se deve utilizzare un sistema di riconoscimento della voce, nel caso di comunicazioni vocali. I sistemi automatici di riconoscimento della voce sono ancora poco affidabili, in particolare se le voci degli interlocutori non sono conosciute o se non sono chiare.

Uno degli altri limiti fondamentali dell'esercizio è il fatto che il filtraggio automatico deve funzionare per comunicazioni in una moltitudine di alfabeti e di lingue con pronunce diverse. Il filtraggio deve inoltre essere effettuato in tempo reale per evitare il sovraccarico delle unità di immagazzinamento dati e permettere che l'informazione giunga rapidamente al suo destinatario.

Da quanto precede risulta che la sorveglianza specifica o generale delle comunicazioni via satelliti è possibile solo per una piccola parte del traffico. Si può illustrare quanto affermato mediante statistiche in materia di esplorazione (cfr. riquadro). Queste cifre mostrano che le informazioni veramente interessanti si perdono in un mare di dettagli insignificanti e che le informazioni preziose da trasmettere al più alto livello dello Stato sono estremamente rare.

Statistiche in materia di esplorazione

Capacità di esplorazione del BND tedesco: dei 10 milioni di comunicazioni internazionali effettuate ogni giorno da e verso la Germania, 800 000 (l'8 per cento) circa sono svolte via satellite. Meno del 10 per cento di esse (75 000 comunicazioni) sono filtrate da un motore di ricerca[33]. Di queste comunicazioni, solo 700 presentano informazioni che hanno a che fare con la sicurezza del Paese e 15 di esse possono essere oggetto di un esame approfondito[34]. Il rapporto è dunque di 15 su 10 milioni (0,00015 per cento).

Altro esempio: la NSA americana intercetta un milione di conversazioni via satelliti ogni mezz'ora. Di questo milione di comunicazioni, 6500 sono separate mediante filtraggio, 1000 corrispondono ai criteri predefiniti, 10 sono selezionate dagli analisti e su tale base[35] viene quindi allestito un solo rapporto. La proporzione è qui di 1 su 1 milione, cioè dello 0.0001 per cento.

Le informazioni grezze (*raw intelligence*) che sono passate attraverso differenti filtri sono selezionate manualmente da un operatore della CGE e ricomposte in funzione di differenti criteri. Sono quindi trasmesse, munite di un commento dell'operatore o di una breve traduzione, al rispettivo mandante. Nessuna informazione è trasmessa al mandante senza essere stata esaminata prima da un collaboratore della CGE (controllo).

Le informazioni ricevute sono comunicate ai servizi di analisi del SIS o del SAP. Questi le analizzano, le traducono e le interpretano per allestire rapporti o sintesi (*finished intelligence*).

Il SIS o il SAP non trasmettono nessuna informazione grezza proveniente dall'esplorazione elettronica ad altri servizi, salvo in casi eccezionali. Capita invece spesso che i rapporti di analisi dei servizi di informazione svizzeri siano forniti, senza indicazione delle fonti, ad altri organi della Confederazione e dei Cantoni o a servizi

33 Dichiarazioni fatte dal coordinatore tedesco dei servizi di informazione davanti alla commissione temporanea del Parlamento europeo il 21.11.2000 (cfr. il rapporto europeo, pag. 38).

34 Jochen Bittner, «Bedingt abhörbereit. Der BND hat zu viele elektronische Quellen und zu wenige kundige Auswerter», in: *Die Zeit*, n. 40, 27.9.2001, pag. 2.

35 Dichiarazione rilasciata dall'ammiraglio William O. Studeman, ex direttore della NSA (1988–1992), citata da James Bamford, «Body of secrets. Anatomy of the ultra-secret National Security Agency», Doubleday, New York, 2001, pag. 411 e nota pag. 671.

di informazione o di sicurezza all'estero, conformemente alle procedure previste nelle leggi e ordinanze corrispondenti[36]. La lista dei Paesi con i quali i servizi di informazione svizzeri sono autorizzati a scambiare informazioni è definita dal Consiglio federale. Anche la Delegazione ne ha conoscenza ed effettua regolarmente controlli puntuali.

Le informazioni grezze ricevute dal sistema Onyx sono esclusivamente informazioni dei servizi d'informazione. Esse non possono, allo stato attuale del diritto, essere utilizzate come mezzi di prova in una procedura penale.

I mandanti sono responsabili che i dati loro trasmessi siano trattati e archiviati in modo conforme alle disposizioni legali. La CGE non archivia nessun dato personale e distrugge man mano gli archivi informatici. Essa non conserva che i dati di collegamento provenienti dall'attività di esplorazione radio utili all'identificazione degli oggetti dell'esplorazione radio (art. 6 cpv. 2 OCGE). I dati di collegamento comprendono le informazioni sulle circostanze delle comunicazioni e non il contenuto delle comunicazioni (allegato all'OCGE, n. 3).

Onyx lavora attualmente nella misura di quasi il 92 per cento per il SIS (compresi i risultati trasmessi al Servizio informazioni delle Forze aeree) e nella misura dell'8 per cento circa per il SAP. Oltre a questi due servizi, non vi sono altri beneficiari delle prestazioni.

4.7 Condizioni poste alla raccolta di informazioni

Diverse condizioni cumulative sono poste alla raccolta di informazione con Onyx. Queste condizioni figurano nell'OCGE e nelle convenzioni quadro.

Si tratta delle condizioni seguenti:

- solo i servizi designati dal capo del DDPS sono autorizzati ad assegnare mandati di esplorazione a Onyx (art. 2 cpv. 3 OCGE).
- La raccolta di informazioni non è autorizzata che sulla base di mandati di esplorazione scritti (art. 3 cpv. 3 OCGE). Senza mandato, niente ricerca.
- I mandati possono essere assegnati soltanto al fine di acquisire informazioni rilevanti in materia di politica di sicurezza (art. 2 cpv. 2 OCGE). Onyx non ha pertanto il diritto di svolgere sorveglianza economica, tecnologica o scientifica, a meno che non serva alla sicurezza della Svizzera.
- I mandati di esplorazione radio si riferiscono esclusivamente a oggetti dell'esplorazione radio all'estero – o considerati tali – e non possono comprendere utenti svizzeri (art. 5 cpv. 1 OCGE). La CGE è pertanto autorizzata a intercettare le comunicazioni fra due utenti all'estero, nonché le comunicazioni fra un utente all'estero e un utente in Svizzera, a condizione che l'utente all'estero costituisca oggetto di esplorazione. È per contro vietato utilizzare Onyx per fini di sicurezza interna. Per questo motivo l'intercettazione di conversazioni fra due utenti in Svizzera, qualunque sia la loro nazionalità, è vietata (cfr. tabella 1). L'OCGE parte dunque

[36] Cfr., per il SIS, art. 6 cpv. 2 OSINF. Cfr., per il SAP, art. 17 LMSI, art. 6 cpv. 1 dell'ordinanza del 27 giugno 2001 sulle misure per la salvaguardia della sicurezza interna (OMSI), (RS **120.2**) e n. 26 delle direttive del 9 settembre 1992 del Dipartimento federale di giustizia e polizia sull'attuazione della protezione dello Stato (FF **1992** VI 149).

nazionalità, è vietata (cfr. tabella 1). L'OCGE parte dunque essenzialmente da una logica territoriale e non dalla nazionalità degli utenti.

– In linea di principio, la CGE non ha il diritto di trasmettere al SIS informazioni concernenti utenti svizzeri che sono state rilevate involontariamente (art. 5 cpv. 2 OCGE). Se queste informazioni fortuite – l'ordinanza parla di «sottoprodotti» (art. 5 cpv. 3 OCGE) – sono necessarie per l'esecuzione del mandato del SIS, i dati relativi agli utenti in Svizzera devono essere cancellati interamente o parzialmente. Lo stesso vale per gli utenti all'estero chiaramente identificati come svizzeri. I dettagli sono disciplinati in un documento allegato alla convenzione quadro fra il SIS e la CGE del 3 ottobre 2001, chiamato «allegato 4»[37]. L'allegato 4 prevede in particolare che le informazioni trasmesse al SIS in simili casi devono essere oggetto di un verbale allestito dal SIS e dalla CGE. I verbali possono essere controllati, in particolare dalla DCG.

– I sottoprodotti che concernono utenti svizzeri e possono essere rilevanti per la sicurezza interna possono essere comunicati direttamente al SAP, conformemente all'articolo 99 cpv. 2bis LM. Le informazioni possono essere trasmesse integralmente, cioè con le indicazioni necessarie sugli utenti svizzeri.

Tabella 1

Intercettazioni autorizzate o vietate, secondo il territorio

		Obiettivo dell'esplorazione	
		in Svizzera	all'estero
Ubicazione dell'altro utente	in Svizzera	intercettazione vietata	intercettazione autorizzata
	all'estero	intercettazione vietata	intercettazione autorizzata

37 Beilage 4: Richtlinien zur Verarbeitung von Erfassungsresultaten mit Bezug zu CH-Personen bzw -Firmen, Produktedefinition SAT, Anhang B1 zur Rahmenvereinbarung zwischen dem Strategischen Nachrichtendienst und der COMINT Organisation betreffend ND Führung, vom 3.10.2001 (solo in tedesco, non pubblicato). Secondo questo allegato sono considerati utenti svizzeri (a) tutti i cittadini svizzeri, (b) tutti gli stranieri con domicilio permanente in Svizzera, (c) tutte le persone giuridiche registrate in Svizzera (compresi aerei e navi battenti bandiera svizzera) e (d) tutti i gruppi e tutte le associazioni non registrati, composti prevalentemente da membri che rispondono ai criteri fissati alle lettere (a)–(c).

5 Constatazioni della Delegazione e valutazione

5.1 Legalità delle intercettazioni effettuate mediante Onyx

5.1.1 Legalità dei mandati di esplorazione in materia di sicurezza esterna

La Delegazione ritiene che la base legale su cui si fondano i mandati di esplorazione del SIS sia sufficiente, in quanto l'articolo 99 LM e l'OSINF danno al SIS esplicitamente la competenza di raccogliere attivamente informazioni concernenti l'estero. La legge precisa che le attività di raccolta di informazioni sono limitate alle questioni relative alla politica di sicurezza della Svizzera e dunque alle minacce provenienti dall'esterno[38]. La raccolta e l'analisi di informazioni relative alla Svizzera e l'intercettazione di comunicazioni fra utenti in Svizzera sono vietate.

Il divieto di svolgere intercettazioni di comunicazioni di utenti in Svizzera si deduce del resto dal Codice penale, secondo cui sono punibili le infrazioni effettuate contro la sfera privata e le violazioni del segreto delle telecomunicazioni. Non sono considerate punibili unicamente le misure ufficiali di sorveglianza approvate da un giudice che mirano a perseguire o prevenire i crimini e i reati di una certa gravità[39]. Le intercettazioni della CGE non rientrano in questa categoria e sono dunque punibili se riguardano volutamente utenti in Svizzera.

Anche se giudica sufficiente l'attuale dispositivo legislativo sulle misure di intercettazione ordinate dal SIS, la Delegazione ritiene che esso dovrebbe essere chiarito e reso più preciso a livello di legge.

Occorre anche constatare che il tenore dell'articolo 99 LM è, per quanto riguarda le intercettazioni di comunicazioni, molto generico, in particolare rispetto alle disposizioni estremamente chiare e precise in materia di sicurezza interna (LMSI) o di sorveglianza telefonica nell'ambito penale (LSCPT). La Delegazione dubita pertanto che persone non specializzate nelle questioni di informazioni siano coscienti delle attività di intercettazione svolte sulla base dell'articolo 99 LM. Tali attività non sono menzionate del resto nel messaggio del 1993 relativo alla LM. Il messaggio a sostegno della revisione della legislazione militare del 2001[40] non fornisce maggiori informazioni.

La Delegazione ritiene che l'intercettazione delle comunicazioni dovrebbe essere menzionata più chiaramente nella LM, la quale dovrebbe indicare esplicitamente che le intercettazioni possono riguardare solo comunicazioni all'estero nonché rinviare alle disposizioni del Codice penale secondo cui l'intercettazione di comunicazioni di utenti in Svizzera è punibile.

38 Cfr. a questo merito il messaggio dell'8 settembre 1993 del Consiglio federale a sostegno della legge federale sull'esercito e l'amministrazione militare e del decreto federale sull'organizzazione dell'esercito (FF **1993** IV 1).

39 Cfr. gli art. 179bis–179^{novies}, in particolare l'art. 179^{octies}, e l'art. 321ter del Codice penale del 21 dicembre 1937 (CP; RS **311.0**). Cfr. anche art. 43, 44 e 50 della legge federale del 30 aprile 1997 sulle telecomunicazioni (LTC; RS **784.10**). Secondo la LSCPT che disciplina la sorveglianza telefonica in materia penale, le conversazioni possono essere ascoltate unicamente se esiste il forte sospetto di reato grave, per una certa categoria di reati e su decisione di un giudice, la cui decisione deve essere confermata da un'istanza giudiziaria superiore. Cfr. anche l'allegato 1.

40 Messaggio del 24 ottobre 2001 del Consiglio federale concernente la riforma Esercito XXI e la revisione della legislazione militare (FF **2002** 768).

Per la Delegazione è inoltre paradossale dover constatare che le sorveglianze di comunicazioni telefoniche effettuate dalle autorità svizzere sul proprio territorio sono limitate da un quadro legale molto severo, con controlli giudiziari e vie di ricorso, mentre le intercettazioni all'estero godono – la DCG non vuol dire intenzionalmente – di un quadro regolamentare piuttosto vago. Pertanto, le persone all'estero non beneficiano di nessuna protezione giuridica nel diritto svizzero in caso di intercettazioni.

Chiedendo di fissare esplicitamente nella LM le intercettazioni di comunicazioni, la DCG persegue un obiettivo di trasparenza. Questa esigenza è meno giustificata sul piano interno, poiché l'intercettazione di utenti in Svizzera è vietata, che non rispetto al diritto internazionale, in particolare alla CEDU[41]. L'articolo 8 CEDU non autorizza le ingerenze nella vita privata se non per preservare la sicurezza nazionale e se sono soddisfatte diverse condizioni come esistenza e accessibilità della base legale, proporzionalità ecc. In numerose decisioni, la Corte europea dei diritti dell'uomo di Strasburgo ha rilevato che le leggi che disciplinano gli ascolti amministrativi o giudiziari devono essere accessibili al pubblico e redatti in modo sufficientemente preciso e dettagliato affinché i cittadini possano reagirvi con un comportamento adeguato[42].

In questo contesto, la Delegazione approva l'iniziativa presa recentemente dal Consiglio federale di fissare con precisione nell'OCGE i compiti e le competenze in materia di intercettazione delle comunicazioni. Questo modo di procedere contribuisce a rendere più trasparente la legislazione in materia e va nel senso auspicato dalla Delegazione.

Nonostante questa prima misura, la Delegazione ritiene che l'esistenza di intercettazioni delle comunicazioni dovrebbe essere menzionata più chiaramente nella LM. Essa dovrebbe indicare esplicitamente che le intercettazioni possono riguardare solo comunicazioni all'estero nonché rinviare alle disposizioni del Codice penale secondo cui l'intercettazione di comunicazioni di utenti in Svizzera è punibile.

41 Secondo numerosi autori, la CEDU è lo strumento più efficace a livello internazionale in materia di protezione della vita privata.

42 Cfr. decisione del 24 aprile 1990 della Corte europea dei diritti dell'uomo in casu Kruslin contro Francia, nella quale, al paragrafo 33, si precisa che le intercettazioni e altre forme ai ascolto delle conversazioni telefoniche costituiscono una grave lesione al rispetto della vita privata e della corrispondenza e pertanto devono essere basate su una «legge» particolarmente precisa. L'esistenza di regole chiare e dettagliate in materia è indispensabile, tanto più che i procedimenti tecnici utilizzabili continuano ad essere perfezionati. Cfr. anche le decisioni del 2 agosto 1984 Malone contro Regno Unito (§ 67), Huvig contro Francia del 24 aprile 1990 (§ 29) e Amann contro Svizzera del 16 febbraio 2000 (§ 58). Per il momento, la giurisprudenza della Corte si riferisce a misure di sorveglianza telefonica giudiziarie o amministrative realizzate da autorità contro cittadini sottoposti alla loro giurisdizione. Secondo le conoscenze della DCG, la Corte non ha ancora dovuto pronunciarsi su intercettazioni svolte da un membro firmatario della CEDU sul territorio di un altro Paese.

Raccomandazione n. 1

La Delegazione delle Commissioni della gestione raccomanda al Consiglio federale di esaminare l'opportunità di introdurre nella LM un riferimento esplicito alle intercettazioni di comunicazioni all'estero. Il riferimento dovrebbe indicare esplicitamente che le intercettazioni possono riguardare solo comunicazioni all'estero nonché rinviare alle disposizioni del Codice penale secondo cui l'intercettazione di comunicazioni di utenti in Svizzera è punibile.

Raccomandazione n. 2

La Delegazione delle Commissioni della gestione raccomanda al Consiglio federale di esaminare la conformità alla CEDU della legislazione relativa alle attività di intercettazione delle comunicazioni all'estero e, in caso di bisogno, di apportarvi gli adeguamenti necessari.

5.1.2 Legalità dei mandati di esplorazione in materia di sicurezza interna

L'articolo 14 LMSI disciplina in maniera dettagliata e esaustiva i mezzi che le autorità di protezione dello Stato sono autorizzate a impiegare in materia di ricerca di informazioni. La legge precisa che i dati personali possono essere raccolti con:

- valutazione delle fonti accessibili al pubblico;
- richiesta di informazioni;
- consultazione di fascicoli ufficiali;
- ricezione e valutazione di comunicazioni;
- ricerca dell'identità o del soggiorno delle persone;
- osservazione dei fatti in luoghi pubblici e liberamente accessibili, anche ricorrendo a registrazioni di immagini e suoni;
- accertamento dei movimenti e contatti delle persone.

Pur precisando che si possono ricercare informazioni anche all'insaputa della persona interessata (art. 14 cpv. 1 LMSI), la legge non prevede che il SAP possa intercettare o dare l'incarico di intercettare comunicazioni private all'estero. La legge vieta inoltre alle autorità di sicurezza dello Stato l'impiego di misure coercitive (art. 14 cpv. 3 LMSI). Per la Delegazione è indubbio che qualsiasi intercettazione di comunicazioni comporta una coercizione non appena costituisce un'ingerenza nel diritto alla tutela della vita privata. Questo genere di ingerenza è vietato al SAP nel diritto interno e niente lascia supporre che il legislatore sia disposto ad autorizzarlo oltre le frontiere.

Le intercettazioni realizzate all'estero su mandato del SAP non possono essere desunte neanche dalla «clausola generale di polizia», che permette al Consiglio federale di ordinare misure di sicurezza basandosi direttamente sulla Costituzione

federale. Tali misure possono essere prese solo dal Governo e solo in caso di «pericolo grave, immediato e non altrimenti evitabile» (art. 36 cpv. 1 Cost.) o di «gravi turbamenti, esistenti o imminenti, dell'ordine pubblico o della sicurezza interna o esterna» (art. 185 cpv. 3 Cost.). I mandati affidati dal SAP alla CGE non soddisfano queste condizioni.

Per la Delegazione, le attività svolte mediante Onyx su mandato del SAP non poggiano, attualmente, su una base legale formale sufficientemente solida. Questa valutazione è condivisa anche dall'Ufficio federale di giustizia in una perizia legale del mese di aprile 2003 richiesta dallo Stato maggiore generale.

In una lettera del 23 maggio 2003, la Delegazione ha esposto al capo del DFGP i problemi legali sollevati dai mandati di esplorazione del SAP. Nella sua presa di posizione del 23 giugno 2003, il capo del DFGP ha ammesso la debolezza della base legale e sostenuto che la situazione giuridica doveva essere corretta. Il capo del DFGP ha comunicato la sua intenzione di procedere in due tempi: in una prima fase, il DFGP ha previsto la revisione parziale dell'OMSI con l'OCGE; nella seconda, il Dipartimento presenterà una modifica della legge nell'ambito della seconda revisione della LMSI. Nella sua lettera alla Delegazione, il capo del DFGP ha insistito affinché il SAP possa continuare ad assegnare mandati di esplorazione a Onyx. Ha sottolineato anche che le informazioni fornite dal sistema, contrariamente alle sorveglianze telefoniche effettuate nelle procedure penali, non possono essere utilizzate in un processo e che esse servono unicamente per scopi di informazione.

In occasione della sua seduta del 15 ottobre 2003, il Consiglio federale ha deciso di correggere parzialmente il problema nel senso auspicato dal capo del DFGP. Approvando l'OCGE, il Consiglio federale ha deciso di modificare l'OMSI in modo da conferire al SAP una competenza esplicita che lo autorizza ad assegnare mandati di esplorazione all'estero (art. 9bis OMSI). Parallelamente, il Consiglio federale ha deciso di istituire l'ICI, che assicurerà il controllo della legalità e della proporzionalità dei mandati di esplorazione del SAP.

La Delegazione ritiene che la modifica dell'OMSI sia un netto progresso rispetto alla situazione precedente. La modifica rappresenta una soluzione provvisoria politicamente accettabile per la DCG e giuridicamente sostenibile da parte dell'Ufficio federale di giustizia. La creazione dell'ICI costituisce anche una misura che permette di compensare l'attuale deficit in materia di legalità.

Il vuoto giuridico comunque non è ancora completamente colmato. In effetti anche se può sembrare logico regolamentare una materia prima mediante un'ordinanza e solo dopo con una legge in senso formale, non si devono dimenticare le condizioni poste dalla Costituzione federale. Quest'ultima esige infatti che le restrizioni gravi dei diritti fondamentali, nella fattispecie la tutela della sfera privata, devono essere previste almeno da una legge in senso formale (art. 36 Cost.). Nel presente caso, il Consiglio federale ha preferito, per ragioni del tutto comprensibili, invertire la gerarchia delle norme, anticipando tuttavia così il legislatore.

I mandati del SAP sono meno numerosi di quelli del SIS. Quantitativamente, infatti, non rappresentano che l'8 per cento delle informazioni intercettate mediante Onyx. Sul piano qualitativo e politico, tuttavia, la loro importanza è nettamente superiore.

La Delegazione ritiene che spetti al Parlamento dare rapidamente una base legale formale ai mandati di esplorazione del SAP, e precisamente prima dell'inizio della

fase di piena operatività del sistema Onyx, prevista alla fine del 2005/all'inizio del 2006.

Formulando questa esigenza, la Delegazione vuole conferire ai mandati di esplorazione del SAP una base formale che sia allo stesso livello normativo di quello in vigore per il SIS. La Delegazione vuole anche evitare che la fase sperimentale — che si svolge in un quadro legislativo molto vago – crei una situazione che il legislatore non potrà più modificare e costituisca un precedente per ulteriori e più limitative misure nel settore della protezione preventiva dello Stato.

Raccomandazione n. 3

La Delegazione delle Commissioni della gestione raccomanda al Consiglio federale di presentare, nel suo secondo progetto di revisione della LMSI, una disposizione legale che disciplini i mandati di esplorazione che il SAP effettua o incarica di effettuare in materia di sicurezza interna. Il progetto dovrà essere presentato al Parlamento prima della fase di piena operatività di Onyx.

In questo contesto, la Delegazione ci tiene a rilevare che non ha trovato elementi che in base ai quali si possa presumere che il vuoto giuridico attuale abbia consentito al SAP di raccogliere informazioni per scopi diversi da quelli previsti dalla legge.

5.1.3 Legalità dei trasferimenti di informazioni dal CGE al SAP in materia di sicurezza interna

L'articolo 99 cpv. 2bis LM disciplina chiaramente le competenze quando informazioni fortuite[43], provenienti dall'esplorazione radio all'estero, concernono la Svizzera e utenti svizzeri.

È ancora troppo presto per procedere alla valutazione di questa nuova disposizione che entrerà in vigore solo all'inizio del 2004. La Delegazione provvederà a sorvegliare strettamente gli scambi di informazioni che verranno svolti sulla base di questa disposizione. Essa si assicurerà in particolare che vengano fornite all'UFP solo informazioni potenzialmente significative per la sicurezza interna o per il perseguimento penale. Inoltre domanderà alle autorità in questione di disciplinare per scritto le procedure e di tenere un controllo preciso della natura e del contenuto delle informazioni trasmesse. Una simile procedura è del resto prevista all'articolo 5 cpv. 3 OCGE.

Attualmente, per quanto riguarda i mandati affidati dal SIS, la percentuale di informazioni che ha un riferimento con utenti svizzeri è molto bassa (lo 0,5%). Ciò significa che su mille informazioni intercettate mediante Onyx su mandato del SIS, cinque comprendono informazioni relative alla Svizzera. Per la Delegazione, si tratta di un risultato molto buono. Per il SAP, questo tasso sale al 15 per cento, ciò che è logico considerato il suo mandato legale.

43 L'OCGE parla, in questo caso, di «sottoprodotti», art. 5 cpv. 3 OCGE.

5.1.4 La compatibilità delle intercettazioni rispetto al diritto internazionale

Le intercettazioni di comunicazioni all'estero sollevano questioni fondamentali di diritto internazionale generale, e precisamente in merito ai principi della territorialità e della tutela della sfera privata in virtù del diritto internazionale.

Per la DCG, le intercettazioni effettuate mediante Onyx delle comunicazioni all'estero sono problematiche sotto diversi aspetti. Esse concernono in effetti utenti che si trovano all'estero, cioè sul territorio di un altro Stato. I principi inerenti alla sovranità territoriale si oppongono però al fatto che uno Stato compia attività sul territorio di un altro Stato senza il consenso di quest'ultimo. Nel diritto svizzero, questa protezione è conferita dal Codice penale, e in particolare dall'articolo 271 CP che vieta di compiere sul territorio svizzero, senza esservi autorizzato, atti per conto di uno Stato estero. Sono considerati atti di questo genere quelli che, secondo la loro natura o il loro scopo, possono essere caratterizzati quali attività ufficiale[44].

La questione centrale è se l'ascolto tecnico all'estero costituisce un'intrusione – e dunque una violazione del principio di territorialità – o se occorre partire dal presupposto che essendo svolto a partire della Svizzera non è connesso a una violazione fisica sul territorio dell'altro Stato. Una terza soluzione potrebbe consistere nel dire che l'intercettazione ha luogo nello spazio extraatmosferico in cui sono situati i satelliti di comunicazione. In questo caso non vi sarebbe violazione del principio di territorialità dato che lo spazio extraatmosferico è di dominio pubblico internazionale[45] e non è soggetto pertanto alle regole della territorialità.

Indipendentemente dalla risposta data al problema della territorialità, bisogna ammettere che gli ascolti pregiudicano il diritto alla tutela della vita privata. Costituiscono in effetti ingerenze unilaterali di uno Stato nella vita privata delle persone che si trovano sul territorio di un altro Stato, che accorda loro la sua protezione. Nel diritto svizzero, questa protezione è garantita dalla Costituzione federale (art. 13 Cost.), dal Codice penale (in particolare gli art. 179bis–179^{septies} CP) nonché dalla legislazione in materia di protezione dei dati. Sul piano del diritto internazionale pubblico, il diritto alla tutela della vita privata e familiare è fissato in numerose convenzioni come la Dichiarazione universale dei diritti dell'uomo (art. 12), il Patto ONU II (art. 17) o la CEDU (art. 8). Ci si potrebbe dunque immaginare – almeno teoricamente e senza tenere conto del fatto che sarebbe difficile produrre le prove – che uno Stato o un privato adisse le giurisdizioni internazionali (Corte europea dei diritti dell'uomo, Comitato dei diritti dell'uomo dell'ONU, Corte internazionale di giustizia) per violazione della tutela della vita privata da parte delle autorità svizzere[46].

Per la Delegazione, le intercettazioni realizzate dal sistema Onyx delle comunicazioni all'estero presentano problemi giuridici delicati dal punto di vista del diritto internazionale. In realtà, questi problemi sono insiti nell'attività di ogni servizio di

44 DTF **114** IV 130.

45 Trattato del 27 gennaio 1967 sulle norme per l'esplorazione e l'utilizzazione, da parte degli Stati, dello spazio extraatmosferico, compresi la luna e gli altri corpi celesti, RS **0.790**.

46 Cfr. Dimitri Yernault, «De la fiction à la réalité: le programme d'espionnage électronique global «Echelon» et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'homme», in: *Revue belge de droit international*, vol. XXXIII, 2001/1, Editions Bruylant, Bruxelles, pag. 137 segg.

informazione e nel suo carattere segreto. Non sono specifici alla Svizzera; tutti i Paesi che dispongono di servizi di informazione sono nella stessa situazione.

Alcuni autori ritengono che lo spionaggio in tempo di pace sia contrario al diritto internazionale perché implica per definizione una violazione della sovranità territoriale. Altri pensano che, non essendo vietate nel diritto internazionale, le attività di informazione all'estero rappresentano al massimo atti poco amichevoli fra Stati e non sono pertanto da considerare atti giuridici[47].

Questa situazione può sembrare paradossale. Mentre tutti i Paesi proibiscono in generale lo spionaggio nella loro legislazione interna (è il caso in Svizzera degli art. 271–274 e 301 CP), la questione della legalità dello spionaggio in tempo di pace non è regolata nel diritto internazionale, né a livello contrattuale né a livello consuetudinario. La constatazione vale anche per le intercettazioni di comunicazioni: nella maggior parte degli Stati, le legislazioni impongono limiti rigorosi alle intercettazioni delle comunicazioni sul loro territorio; nessun regime internazionale sembra invece vietare le intercettazioni extraterritoriali.

In altre parole, il rispetto da parte dello Stato della vita privata dell'individuo finisce spesso alle frontiere nazionali che sono anche i limiti estremi a partire dai quali gli imperativi della sicurezza prevalgono sui diritti fondamentali. La situazione è comprensibile in una logica di sovranità territoriale; è però difficile da applicare nel settore della sorveglianza di telecomunicazioni poiché lo Stato incaricato della sorveglianza, la persona sorvegliata e il procedimento di esplorazione non si trovano sullo stesso territorio ed è pertanto difficile a queste condizioni determinare la legislazione applicabile.

Per la Delegazione, la questione della compatibilità delle intercettazioni realizzate dalla Svizzera all'estero da una parte e il principio della sovranità nazionale e del diritto internazionale dall'altra non possono essere risolti con misure normative o convenzionali; altrimenti si dovrebbe rinunciare ad un servizio di informazione estero. Il problema richiede un approccio politico, che regola le questioni in funzione delle situazioni che si presentano di volta in volta.

5.2 Sistemi di controllo

Per la Delegazione, l'esistenza di una base legale che disciplina le intercettazioni è una condizione necessaria, ma non ancora sufficiente, per garantire un funzionamento di Onyx conforme ai diritti fondamentali. In effetti, l'esperienza mostra che le attività segrete, più di ogni altra attività, rischiano di portare ad abusi perché sfuggono in larga misura ai controlli tradizionali della giustizia o dei media. Per questo motivo, sin dall'inizio del progetto, la Delegazione ha chiesto al Consiglio federale di realizzare un sistema di controllo destinato a proteggere da eventuali abusi.

La Delegazione è intervenuta presso il capo del DDPS e della Delegazione del Consiglio federale per la sicurezza nella primavera 2001 per chiedere loro di elaborare un concetto di controllo[48]. Nell'autunno 2001, il capo del DDPS ha presentato alla Delegazione un primo concetto di controllo elaborato dal servizio del coordina-

47 Cfr. Fabien Lafouasse, «L'espionnage en droit international», in: *Annuaire français de droit international*, XLVII, 2001, CNRS Editions, Parigi, pag. 64 segg. e i diversi altri riferimenti.

48 Cfr. in particolare il comunicato stampa della DCG del 27 marzo 2001.

tore dei servizi d'informazione. Il concetto è stato quindi migliorato sulla base delle esperienze fatte. Dovrà essere ulteriormente perfezionato di pari passo con la messa in esercizio del sistema.

Il sistema di controllo attuale fissa tutta una serie di processi, di documenti e di metodi che consentono la sorveglianza dell'esercizio di Onyx, dall'allestimento dei mandati di esplorazione fino all'analisi dei risultati. È basato su modelli esteri sperimentati[49].

Il sistema di controllo è composto di tre livelli istituzionali distinti:

- il primo livello comprende i mandanti, nel presente caso il SIS e il SAP, e i gestori del sistema Onyx. I mandanti sono responsabili di definire i mandati di esplorazione e di assicurarne la legalità e la proporzionalità. Per il flusso delle informazioni fra la CGE, il SIS e il SAP sono state fissate procedure dettagliate, che regolano, ad esempio, il comportamento in caso di intercettazioni fortuite di informazioni su utenti svizzeri. Queste informazioni devono essere censurate o il loro contenuto deve essere modificato prima dell'inoltro al SIS. La CGE, il SIS e il SAP svolgono regolarmente sedute per discutere sui risultati e sui problemi incontrati durante l'esecuzione dei mandati di esplorazione.
- Il secondo livello di controllo è costituito dall'istanza di controllo indipendente (ICI). L'istanza di controllo ha natura interdipartimentale. È stata creata dal Consiglio federale il 15 ottobre 2003 su proposta del DDPS. I suoi membri sono nominati dalla Giunta del Consiglio federale per la sicurezza su proposta del capo del DDPS (art. 18 cpv. 3 OCGE). Il DDPS non è rappresentato con la maggioranza dei membri nella Giunta e non ne assume la presidenza (art. 18 cpv. 1 OCGE). L'ICI verifica la legalità e la proporzionalità dei mandati di esplorazione radio tenendo conto delle priorità stabilite sulla base delle necessità di informazioni delle istanze politiche (art. 15 cpv. 1 OCGE). L'ICI può trasmettere raccomandazioni scritte al mandante e alla CGE (art. 15 OCGE). Può anche chiedere al dipartimento del mandante la sospensione di mandati di esplorazione radio che non soddisfano o non soddisfano più i principi della legalità e della proporzionalità (art. 15 cpv. 3 lett. b OCGE). L'ICI deve sottoporre annualmente al capo del DDPS un rapporto all'attenzione della Giunta del Consiglio federale in materia di sicurezza (art. 15 cpv. 4 OCGE).

  L'ICI è stata istituita dal Consiglio federale per permettere un controllo dei mandati d'esplorazione indipendente dai mandanti. L'istanza di controllo non è ancora operativa; dovrebbe entrare in funzione all'inizio del 2004.
- Il terzo livello è composto dagli organi dirigenti del DDPS e del Consiglio federale. Comprende il capo dello Stato maggiore generale quale superiore gerarchico della CGE e della direzione del progetto Onyx nonché il capo del DDPS quale responsabile politico del Dipartimento. Il capo del DDPS esercita una sorveglianza generale su Onyx grazie a un sistema di rapporti trimestrali istituito durante il 2002. I rapporti destinati al capo del DDPS, al capo

49 Cfr., per esempio, le direttive americane: «United States Signals Intelligence Directive 18 (USSID 18) – Limitations and Procedures in Signals Intelligence Operations of the United States Sigint System», National Security Agency, del 27 luglio 1993. Per maggiori informazioni, cfr. James Bamford, «Body of secrets. Anatomy of the ultra-secret National Security Agency», Doubleday, New York, 2001, pagg. 442–449.

dello Stato maggiore generale e al sottocapo di stato maggiore dell'aiuto alla condotta presentano lo stato d'avanzamento del progetto Onyx nonché i problemi che richiedono una decisione. Il capo del DDPS può anche incaricare il suo relatore per compiti speciali o l'Ispettorato del DDPS di realizzare controlli puntuali. Infine, il capo del DDPS stabilisce i mandanti autorizzati (art. 2 cpv. 3 OCGE) ed è informato delle richieste e delle decisioni di sospensione di mandati d'esplorazione (art. 16 cpv. 3 OCGE). In questo modo può anche esercitare la sua sorveglianza sull'esercizio del sistema.

– La Giunta del Consiglio federale per la sicurezza è informata ogni anno dal capo del DDPS sulle attività dell'ICI (art. 15 cpv. 4 OCGE). Nomina anche i membri dell'ICI per un periodo di quattro anni (art. 18 cpv. 3 OCGE). Le due competenze le assicurano un diritto di ispezione indiretto sull'esercizio di Onyx.

La Delegazione ritiene che questo sistema di controllo costituisca un quadro adatto alle attività di Onyx e limiti i rischi di abuso. A livello strategico, le competenze e le responsabilità fra le autorità politiche e gli organi esecutivi sono chiaramente definite. A livello operativo, vi è una separazione netta dei ruoli fra i servizi che ordinano le intercettazioni (SIS, SAP), quelli che le eseguono (CGE) e quelli che le controllano (ICI). Questa ripartizione dei ruoli offre, secondo la Delegazione, una garanzia supplementare contro qualsiasi ingerenza nella vita privata dei cittadini.

Il sistema di controllo applicato costituisce anche un quadro adeguato sul quale la DCG potrà basarsi per esercitare il suo mandato di alta vigilanza. Il controllo della Delegazione si svolge comunque a tutti i livelli e a ogni tappa del processo di esplorazione dalla formulazione delle convenzioni quadro fino al livello dei prodotti attraverso le convenzioni sulle prestazioni e i criteri per il filtraggio dei messaggi (elementi d'indirizzo, parole chiave).

È ancora troppo presto per poter valutare il lavoro svolto dall'ICI. Per la Delegazione, questo organo rappresenta un elemento chiave del dispositivo di controllo. In effetti, spetterà a tale autorità valutare la proporzionalità dei mandati di esplorazione e trovare il giusto equilibrio di interessi fra gli imperativi di sicurezza che giustificano la missione dei servizi di informazione e la protezione della vita privata delle persone all'estero di cui si intercettano le comunicazioni. Per la Delegazione, è indispensabile che l'ICI possa disporre non solo di un'autonomia di diritto, ma anche di un'autorità di fatto per acquisire credibilità nella prassi. In questo contesto, sarà determinante la scelta delle persone.

La Delegazione seguirà da vicino la costituzione e il lavoro dell'ICI. Inoltre farà in modo di estendere il concetto di controllo – basato oggi principalmente su questioni di legalità – a controlli dell'efficienza e della qualità.

5.3 Utilità e limiti del sistema Onyx

Onyx costituisce un investimento particolarmente importante dal punto di vista finanziario. Per questo motivo la Delegazione ha cercato di farsi un'idea del contributo fornito dal sistema per rapporto ad altre forme di raccolta di informazioni.

Valutare il valore delle informazioni fornite attraverso Onyx è un'operazione complessa. È risaputo che un'informazione di qualità si ottiene raramente sulla base di una sola fonte, ma che è il risultato di un insieme di informazioni. Un'informazione

intercettata attraverso Onyx non ha di per sé nessun valore particolare. Essa deve poter essere collocata in un contesto già esistente, che viene modificato o rafforzato, ma non necessariamente capovolto da questa informazione. Il lavoro di analisi che conferisce valore aggiunto all'informazione è il risultato dell'interpretazione e del confronto di diverse informazioni provenienti da fonti differenti.

La valutazione dell'efficienza del sistema è complicata anche dal fatto che il sistema non è ancora pienamente operativo e che il periodo considerato è relativamente corto. Le seguenti osservazioni devono dunque essere considerate come una panoramica della situazione attuale.

Dopo la sua entrata in funzione nell'aprile 2000, Onyx ha fornito migliaia di informazioni, in particolare nel settore della lotta contro la proliferazione delle armi di distruzione di massa. Questi dati sono stati analizzati dal SIS e determinati risultati sono stati messi a disposizione dei servizi del Segretariato di Stato dell'economia incaricati del controllo delle esportazioni. Attualmente, Onyx rappresenta una fonte importante di informazioni del SIS nel settore della proliferazione.

Secondo i servizi di informazione e le persone che operano nel settore della lotta contro la proliferazione, le informazioni fornite da Onyx sono utili. Esse consentono ai servizi responsabili di disporre di informazioni di prima mano e di essere meno dipendenti dai servizi di informazione esteri. Grazie a Onyx, i servizi possono anche, in certi casi, verificare l'affidabilità delle informazioni provenienti da altre fonti, completarle, precisarle, o addirittura correggerle.

Le informazioni raccolte mediante Onyx costituiscono anche un «mezzo di scambio» utile nelle relazioni con servizi omologhi all'estero. Questi scambi si svolgono in base al principio del «do ut des». I servizi svizzeri possono sperare di ricevere dai loro partner informazioni interessanti solo fornendo in contropartita informazioni altrettanto interessanti. Le informazioni raccolte attraverso Onyx costituiscono dunque anche uno strumento che consente di aprire le porte verso altri servizi di informazione e di assicurare credibilità ai servizi di informazione svizzeri all'estero.

La Delegazione ha ricevuto un rapporto dettagliato con diverse decine di esempi reali di informazioni captate grazie a Onyx. La Delegazione ha così potuto farsi un'idea precisa del tipo di informazioni intercettate e dell'utilizzazione che ne è stata fatta dai servizi informazioni.

La Delegazione è stata anche informata in dettaglio su diversi casi in cui Onyx ha fornito al SIS informazioni non ancora note su differenti eventi accaduti nel Vicino e nel Medio Oriente, nella Transcaucasia e nel sub-continente indiano. I casi esposti hanno interessato per la maggior parte questioni relative al trasferimento illecito di tecnologie o di beni a doppio uso, al terrorismo internazionale o al commercio di armi internazionale.

Grazie a Onyx, il SAP ha potuto identificare anche un certo numero di imprese attive nel settore dei beni a doppio uso. Queste imprese non erano conosciute prima dalle autorità di controllo e disponevano di indirizzi fittizi in Svizzera.

Secondo lo stato attuale delle conoscenze, le informazioni fornite attraverso Onyx rappresentano un importante valore aggiunto e il sistema ha permesso di aumentare le capacità dei servizi di informazioni.

Questa constatazione non deve tuttavia far perdere di vista che Onyx ha anche dei limiti e che è sottoposto a diverse restrizioni.

Uno dei limiti più importanti è il fatto che la grande maggioranza delle comunicazioni fra Paesi industrializzati non transita via satellite, ma utilizza infrastrutture via cavo terrestri o sottomarine che non possono essere intercettate. A causa dello sviluppo di cavi in fibra ottica con una grande capacità di trasmissione il traffico delle comunicazioni si concentra su questi a scapito dei satelliti. Secondo alcuni ingegneri, solo l'1 per cento del traffico telefonico internazionale transiterebbe via satellite, principalmente per assicurare la connessione con Paesi che non dispongono di buone infrastrutture via cavo terrestri[50]. Nelle regioni con una forte densità di comunicazioni, solo una piccola parte delle comunicazioni si svolge via satellite. Nonostante queste vaste possibilità, Onyx può essere utilizzato con successo solo per l'intercettazione di una piccola parte delle comunicazioni internazionali. Per contro, Onyx può rivelarsi utile per seguire gli sviluppi in Paesi momentaneamente in crisi e senza infrastrutture terrestri di comunicazione.

Il secondo limite è costituito dalla crescita esponenziale del volume delle comunicazioni, che rende impossibile l'intercettazione di tutti i messaggi, e *a fortiori* il loro immagazzinamento e la loro analisi. Dato che non è possibile aumentare le capacità di analisi al ritmo dell'aumentare del volume delle comunicazioni, la parte delle comunicazioni che potrà essere intercettata e analizzata diminuirà. Questo problema si accentuerà con l'inizio della piena operatività del sistema.

Il terzo limite è dato dall'impiego sempre più frequente da parte degli utenti di comunicazioni criptate, ciò che complica e rallenta l'intercettazione e l'analisi. In materia di informazioni, è tuttavia essenziale che le informazioni giungano rapidamente alle autorità incaricate della presa di decisione. Un'informazione buona che giunge troppo tardi al suo destinatario non presenta in effetti nessuna utilità.

Il quarto limite è costituito dai mezzi finanziari: per l'intercettazione di comunicazioni occorrono tecnologie estremamente costose rispetto ad altri metodi di raccolta di informazioni, le quali richiedono investimenti notevoli e regolari, già solo per adattare i sistemi all'evoluzione tecnica. La DCG constata che le spese per lo sviluppo di Onyx si sono triplicate fra il 1997 e il 2003. La crescita massima dei costi si è registrata nella fase iniziale del progetto, fra il 1997 e il 2000.

Tutti questi elementi rappresentano altrettante sfide per i servizi interessati.

Per evitare che il sistema si trasformi, per imprevidenza, in uno smacco tecnologico, la Delegazione invita il DDPS a stilare un elenco completo dei rischi tecnologici e finanziari che possono compromettere la realizzazione del progetto e delle eventuali misure da adottare.

Raccomandazione n. 4

La Delegazione delle Commissioni della gestione invita il DDPS a stilare un elenco completo dei rischi tecnologici e finanziari che possono compromettere la realizzazione del progetto e delle eventuali misure da adottare.

50 Cfr. il rapporto complementare della commissione permanente di controllo dei servizi di informazione sul modo in cui i servizi di informazione belgi reagiscono all'eventualità di una rete «Echelon» di sorveglianza delle comunicazioni, in: «Rapport complémentaire d'activités 1999», Bruxelles, 2000, pag. 30.

In maniera più generale, la Delegazione ritiene che i servizi di informazione debbano badare a non basarsi solo sulla raccolta elettronica delle informazioni a scapito delle altre fonti. In effetti, l'efficienza di un servizio di informazione dipende essenzialmente dalla complementarità delle sue fonti di informazioni.

Per questo motivo, a livello di sforzi e di investimenti, è necessario assicurare un'evoluzione coerente e equilibrata delle differenti forme di raccolta di informazioni (COMINT, OSINT, HUMINT, collaborazione con servizi partner) e delle capacità di esplorazione.

Raccomandazione n. 5

La Delegazione delle Commissioni della gestione invita il Consiglio federale a elaborare, per i servizi di informazione, una strategia quinquennale che presenta gli sforzi e gli investimenti in termini finanziari e umani che il DDPS e il DFGP intendono fare nell'ambito delle fonti di informazione (OSINT, HUMINT, COMINT, collaborazione con servizi partner) e della loro analisi.

5.4 Informazione del Parlamento e dell'opinione pubblica

Per evidenti ragioni di confidenzialità, il DDPS si è sempre mostrato reticente nei confronti del Parlamento e del pubblico sul progetto Onyx.

Il Consiglio federale ha preso la decisione di realizzare Onyx nell'agosto 1997; le prime informazioni su Onyx sono state comunicate alla DCG solo il 12 gennaio 1999 in una lettera spedita dal sottocapo di stato maggiore del Gruppo del servizio informazioni al presidente della Delegazione. La DCG ha poi ricevuto ulteriori informazioni in occasione di una seduta organizzata il 28 gennaio 1999 in seguito a diversi articoli pubblicati nella stampa.

Dopo aver informato la DCG, il DDPS ha diffuso, il 1° febbraio 1999, un comunicato stampa ufficiale nel quale presentava brevemente il progetto. Il progetto è stato anche illustrato in circolari che sono state distribuite nei Comuni direttamente interessati dal progetto.

In Parlamento, il progetto Onyx è stato trattato per la prima volta in occasione dell'esame del messaggio sugli immobili militari 2000 durante la sessione invernale 1999. Con questo messaggio venivano proposti alle Camere differenti lavori di trasformazione di edifici nell'ambito del progetto Onyx[51]. Durante i dibattiti dedicati al messaggio sugli immobili militari e durante l'esame del preventivo 2000 svolto alcuni giorni dopo, sono state poste diverse domande sugli obiettivi e sui principi dell'esercizio del sistema[52].

Onyx è stato discusso in Parlamento anche un anno dopo, in relazione con la vendita a Verestar delle stazioni satellitari di Swisscom nell'ottobre 2000. L'argomento è stato pure trattato nell'ambito di diversi interventi parlamentari.

51 Cfr. n. 212 del messaggio del Consiglio federale del 18 agosto 1999 sugli immobili militari (FF **1999** 7431).
52 Boll. Uff. **1999** S 1015, Boll. Uff. **1999** N 2460 e Boll. Uff. **1999** N 2508.

A parte queste discussioni, l'opportunità e il finanziamento del progetto Onyx non sono mai stati oggetto di una discussione politica in Parlamento. Gli investimenti, scaglionati su diversi anni, sono stati imputati a diverse rubriche budgetarie senza che il Parlamento abbia mai avuto una visione d'insieme dei costi totali del progetto. Anche se parlamentari[53] e media hanno menzionato alcune cifre, queste non sono mai state confermate dal DDPS. La mancanza di trasparenza finanziaria è stata anche criticata dal Controllo federale delle finanze (CDF) in un rapporto di revisione[54] del 15 agosto 2003, di cui la DCG ha ricevuto un esemplare. Sulla base di questo rapporto, la Delegazione delle finanze ha chiesto al DDPS informazioni complementari dopo aver constatato che i costi del progetto si sarebbero con ogni probabilità triplicati.

La DCG giudica anche problematico il fatto di essere stata informata del progetto Onyx solo 16 mesi dopo che il Consiglio federale aveva deciso di realizzarlo. La Delegazione ritiene che questo progetto avrebbe dovuto esserle comunicato immediatamente.

La Delegazione trova infine che il Parlamento e il pubblico non sono sufficientemente informati su Onyx. Nonostante un concetto dettagliato[55], l'informazione ha luogo solo se lo richiedono le circostanze e per reagire a eventi particolari o alla pubblicazione di informazioni da parte dei media. La Delegazione ritiene che il Parlamento e l'opinione pubblica abbiano il diritto di essere informati meglio sugli obiettivi del progetto Onyx, al quale sono stati assegnati notevoli crediti.

Per questo motivo, la Delegazione invita il DDPS a sviluppare una politica di informazione attiva sul progetto Onyx. È necessario dimostrare alle autorità politiche responsabili il valore aggiunto creato da Onyx e mostrare chiaramente la sua legittimità democratica. Il presente rapporto è un primo passo in tale direzione.

Raccomandazione n. 6

La Delegazione delle Commissioni della gestione invita il DDPS ad informare in modo aperto e regolare sulle attività svolte nell'ambito del sistema Onyx.

5.5 La vendita delle antenne di Swisscom all'operatore Verestar

In occasione della sua visita del 15 settembre 2000 a Zimmerwald, la Delegazione è stata informata dal capo dello Stato maggiore generale che l'azienda Swisscom aveva l'intenzione di vendere a un operatore estero determinati impianti e edifici che avevano a che fare con la difesa generale della Confederazione e in particolare con il settore della radiodiffusione (settore «broadcasting») di Swisscom nonché con le stazioni terrestri di comunicazione via satellite di Leuk che si trovano nelle vicinan-

53 Boll. Uff. **1999** N 2530.
54 Bericht an den Rüstungs- und Generalstabschef über die Prüfung des Projektes elektronische Aufklärungssystem für Satellitenverbindungen (SATOS/ONYX), dell'11 agosto 2003, pag. 1 (solo in tedesco, non pubblicato).
55 Concetto d'informazione del capo dello stato maggiore generale «EA von Satellitenverbindungen», del 22 gennaio 1999 (solo in tedesco, non pubblicato).

ze degli impianti Onyx della CGE. Il capo dello Stato maggiore generale aveva detto alla Delegazione di essere venuto a conoscenza della decisione di Swisscom per caso e che il DDPS non era implicato nel progetto di vendita.

Lo stesso giorno, la Delegazione è intervenuta presso il Consiglio federale, gli ha espresso le proprie preoccupazioni e lo ha invitato ad adottare immediatamente tutte le misure necessarie per difendere gli interessi legittimi della Confederazione nei confronti del Consiglio d'amministrazione e della direzione generale di Swisscom.

Alcuni giorni dopo, la questione è stata discussa anche in seno alla Commissione della gestione del Consiglio degli Stati e nelle Commissioni della politica di sicurezza del Consiglio nazionale e del Consiglio degli Stati. È stata inoltre oggetto di differenti interventi parlamentari[56] e di discussioni in seno alle Camere[57].

Per la Delegazione, costituisce un problema solo la vendita delle stazioni terrestri di Leuk poiché le antenne del sistema Onyx sono situate su un terreno di proprietà di Swisscom. Inoltre, in data 20 marzo 2000, il DDPS aveva concluso un contratto di dieci anni con Swisscom che prevedeva che l'azienda assicurasse l'alimentazione di acqua e corrente degli impianti Onyx nonché differenti lavori di manutenzione per lo Stato maggiore generale.

Con la vendita degli impianti di Swisscom all'operatore americano Verestar, si è dovuto rinegoziare il contratto e separare gli impianti utilizzati a scopo commerciale da quelli esercitati dal DDPS.

Fra il DDPS e Swisscom è stata trovata una soluzione, che ha richiesto una nuova suddivisione del terreno di Leuk e la cessione di diverse parcelle alla Confederazione. L'atto di vendita è stato stipulato a Leuk il 15 novembre 2000 e l'iscrizione nel registro fondiario ha avuto luogo il 3 gennaio 2001 – con effetto dal 1° gennaio 2001 – al momento della conclusione della transazione e della consegna degli impianti a Verestar.

Attualmente tutti le componenti registrate del sistema Onyx sono integrate negli impianti del DDPS e non vi sono interfacce fra questi impianti e quelli esercitati da Verestar. L'unico legame che ancora esiste fra i due siti concerne l'alimentazione di acqua e corrente. Un'alimentazione di acqua e corrente indipendente degli impianti Onyx è allo studio.

La vendita da parte di Swisscom degli impianti a Verestar ha differito di 9 mesi la realizzazione del progetto Onyx. Per il resto, il sistema non è stato toccato dalla vendita dell'impianto di trasmissione.

La Delegazione constata con soddisfazione che, nonostante i problemi registrati all'inizio dell'operazione, il DDPS è riuscito a tutelare gli interessi e la sicurezza del sistema Onyx.

56 00.5180 Ora delle domande. Domanda. Swisscom. Vendita di impianti di trasmissione, del 2 ottobre 2000 (Boll. Uff. **2000** N 1055); 00.5181 Ora delle domande. Domanda. Swisscom/DDPS. Vendita di immobili, del 2 ottobre 2000 (Boll. Uff. **2000** N 1056); 00.5184 Ora delle domande. Domanda. Swisscom. Vendita di attività di radiodiffusione, del 2 ottobre 2000 (Boll. Uff. **2000** N 1056); 00.3518 Interpellanza. Swisscom. Vendita del servizio Broadcasting, del 4 ottobre 2000 (Boll. Uff. **2000** S 799); 00.5202 Ora delle domande. Domanda. Servizi Broadcasting di Swisscom e SSR, del 4 dicembre 2000 (Boll. Uff. **2000** N 1348).

57 Cfr. in particolare le discussioni nel Consiglio degli Stati, del 30 novembre 2000 (Boll. Uff. **2000** S 799).

5.6 Presunta partecipazione del sistema Onyx a una rete di esplorazione internazionale

Negli ultimi anni,in diversi rapporti ufficiali e in alcuni media si è potuto leggere che il sistema Onyx fa parte di una rete di esplorazione multinazionale.

La tesi è sostenuta, ad esempio, nel rapporto dell'Assemblea nazionale francese dell'ottobre 2000, in cui si afferma che la rete Echelon include nel suo sistema la Svizzera, la quale prevede di installare sul suo territorio stazioni di ricezione[58]. Il rapporto precisa anche che, secondo un deputato, il sistema Echelon ha tessuto una «ragnatela» mondiale con sedi in Svizzera[59].

Per quanto concerne il Parlamento europeo, il suo rapporto dell'11 luglio 2001 cita le affermazioni di Duncan Campbell, uno dei giornalisti più conosciuti in materia di esplorazione delle comunicazioni. Secondo lui, le «capacità di esplorazione di diversi Paesi europei (sarebbero) nettamente aumentate nel corso degli ultimi anni – in particolare in Svizzera, in Danimarca e in Francia. Inoltre si osserva un rafforzamento della cooperazione bilaterale e multilaterale nel settore dei servizi d'informazione»[60].

Il rapporto del Parlamento belga, del 25 febbraio 2002, precisa che, secondo certe fonti, la Svizzera collabora con gli Stati Uniti e il Regno Unito alla realizzazione del suo sistema di esplorazione[61]. Il rapporto riferisce anche che la Germania e la Francia non partecipano all'operazione.

Da un'analisi risulta che la maggior parte delle informazioni fornite dai rapporti del Parlamento francese, europeo e belga hanno la loro origine in affermazioni di Duncan Campbell, che sono però state travisate. In effetti, Duncan Campbell non ha mai affermato che esiste una collaborazione fra la Svizzera e Echelon, né dichiarato di poterlo provare. Duncan Campbell sottolinea solo che la collaborazione fra Stati è usuale in materia di esplorazione elettronica[62] e che la Svizzera non fa sicuramente eccezione a questa regola. In un articolo pubblicato nella stampa britannica rileva inoltre che le capacità unite della Danimarca e della Svizzera sarebbero in grado di fornire a Echelon più informazioni di quelle fornite dalle capacità riunite del Canada, dell'Australia e della Nuova Zelanda[63], senza affermare tuttavia che una simile collaborazione esiste o è esistita.

Le supposizioni relative a una possibile partecipazione di Onyx alla rete Echelon sono ridiventate attuali nell'autunno 2000, quando Swisscom ha venduto le sue stazioni terrestri di comunicazione via satellite all'operatore americano Verestar (cfr. n. 5.5). La società Verestar è una filiale di uno dei principali gestori e progettisti di

58 Rapporto francese, pag. 25.
59 Rapporto francese, pag. 66.
60 Rapporto europeo, pag. 74.
61 Rapporto belga, pag. 37.
62 A parte Echelon, questa affermazione di Duncan Campbell è smentita da altre fonti. In: «Renseignement européen: les nouveaux défis – réponse au rapport annuel du Conseil», Assemblea dell'Unione dell'Europa occidentale, 48ª sessione, documento A/1775, Parigi, 4 giugno 2002, pag. 19 si constata che non esiste per ora una vera cooperazione tecnica nel settore dell'esplorazione elettronica, dato che ogni Stato ritiene che la padronanza della situazione elettromagnetica in una determinata zona rientri nell'ambito delle proprie competenze.
63 Duncan Campbell, «Fight over Euro-intelligence plans», in: *The Guardian*, 6 agosto 2001.

servizi di radiodiffusione nell'America del Nord. Verestar dispone di una vasta clientela tra cui il Dipartimento di Stato americano e il Dipartimento americano della difesa. Per alcuni, l'acquisto delle antenne di Swisscom da parte di Verestar e la loro vicinanza alle antenne del sistema Onyx erano ulteriori indizi in base ai quali ci si poteva immaginare una collaborazione fra gli Stati Uniti e la Svizzera, anzi addirittura una partecipazione di Onyx alla rete Echelon. Alcuni parlamentari si sono mostrati preoccupati per questa situazione e per le conseguenze che una simile collaborazione avrebbe potuto avere per la neutralità svizzera[64].

La Delegazione non può confermare nessuna delle supposizioni relative ad una integrazione di Onyx in una rete internazionale di ascolto come Echelon. In effetti, nel corso dei suoi lavori, la Delegazione non ha trovato nessun elemento a conferma di una possibile integrazione del sistema Onyx in una qualsiasi rete di esplorazione internazionale. Inoltre, proprio per quanto riguarda Echelon, è difficile immaginare quali vantaggi questa rete potrebbe avere da una collaborazione con la Svizzera. Echelon dispone già di una copertura di antenne sufficiente in Europa. Per la Svizzera, una simile collaborazione non sarebbe inoltre compatibile con la politica di neutralità.

In base allo stato attuale delle conoscenze, la Delegazione può affermare che il sistema Onyx è uno strumento di carattere strettamente nazionale basato unicamente su infrastrutture situate sul territorio svizzero. Onyx funziona in maniera autonoma e non dispone di interfacce tecniche con un altro sistema estero. Per quanto ne sappia la DGC, non esiste nessun accordo di collaborazione con un altro Stato in materia di esplorazione delle comunicazioni via satellite, né sono scambiati automaticamente dati grezzi con l'estero.

Affermare che Onyx è indipendente da ogni sistema estero sul piano tecnico non significa dire che esso non approfitta, per lo sviluppo e l'esercizio, di informazioni provenienti dell'estero. Come già detto, i servizi di informazione e la CGE hanno contatti bilaterali regolari con i loro omologhi all'estero. Gli scambi di informazioni si effettuano di caso in caso e possono riguardare dati tecnici (bande di frequenza, canali di trasmissione, analisi del traffico ecc.) o elementi di indirizzo come numeri di chiamata. Mediante le informazioni spesso è possibile definire meglio gli obiettivi dell'esplorazione e facilitare la raccolta di informazioni.

I contatti e i Paesi con i quali essi hanno luogo sono sottoposti all'approvazione del Consiglio federale[65]. Anche la Delegazione ne ha conoscenza ed effettua regolarmente controlli puntuali.

La Delegazione conosce anche i Paesi da cui provengono i differenti sistemi che costituiscono Onyx.

64 000.3629 Interpellanza. Stazione terrestre per satelliti a Leuk, del 28.11.2000 (Boll. Uff. **2001** N 365); 01.3189 Postulato. Satos 3. Vendita di terreno a Leuk da parte di Swisscom, del 23.3.2001 (tolto di ruolo dopo due anni senza essere trattato); 03.1046 Interrogazione ordinaria. Spionaggio economico su territorio svizzero a vantaggio degli Stati Uniti, dell'8.5.2003 (Boll. Uff. **2003** N 1758).

65 Cfr. art. 6 cpv 2 OSINF e art. 26 cpv. 2 LMSI.

6 Conclusioni

La Delegazione delle Commissioni della gestione constata che:

1. diversi Stati hanno sviluppato negli ultimi anni sistemi di esplorazione delle comunicazioni.
2. Il sistema Onyx permette di captare le comunicazioni internazionali civili e militari che transitano via satellite. È esercitato dalla Divisione della condotta della guerra elettronica (CGE), che è una divisione dello Stato maggiore generale.
3. Il sistema è entrato in funzione nell'aprile 2000 e attualmente è nella fase sperimentale. Passerà alla fase operativa nel corso del 2004 e alla piena operatività alla fine del 2005/all'inizio del 2006.
4. Il sistema raccoglie informazioni che concernono unicamente la politica di sicurezza della Svizzera e non svolge sorveglianza economica, tecnologica o scientifica.
5. Il sistema procede a intercettazioni di comunicazioni unicamente al di fuori delle frontiere.
6. Il sistema rispetta i diritti fondamentali e le libertà delle persone in Svizzera poiché le intercettazioni di comunicazioni fra utenti in Svizzera sono vietate.
7. Il sistema è utilizzato unicamente nell'ambito dei servizi d'informazione. Allo stato attuale del diritto, le informazioni raccolte non possono essere utilizzate come mezzi di prova in una procedura penale.
8. Le intercettazioni ordinate dal Servizio informazioni strategico (SIS) nel settore della sicurezza esterna della Svizzera poggiano su una base legale formale ritenuta sufficiente.
9. Le intercettazioni ordinate dal Servizio di analisi e prevenzione (SAP) nel settore della sicurezza interna della Svizzera poggiano su una base legale formale che non è sufficiente.
10. I trasferimenti di informazioni fra la CGE, il SIS e il SAP poggiano su basi legali e convenzioni chiaramente definite.
11. Le intercettazioni di comunicazioni all'estero effettuate mediante Onyx sollevano problemi delicati dal punto di vista del diritto internazionale, sia sotto l'aspetto del principio di territorialità che sotto quello della tutela della vita privata e del segreto delle comunicazioni.
12. Esiste un sistema di controllo adeguato che permette a tutti i livelli responsabili, operativi e politici, di controllare le attività di esplorazione e di limitare i rischi di abuso.
13. Esiste una volontà politica manifesta del capo del DDPS e della Delegazione del Consiglio federale per la sicurezza di dare un quadro giuridico e politico preciso alle attività di esplorazione.
14. I mandati di esplorazione sono controllati per quanto riguarda l'aspetto della legalità e della proporzionalità da un'autorità interdipartimentale: l'istanza di controllo indipendente (ICI).

15. Esiste una chiara separazione dei ruoli fra i servizi che ordinano le intercettazioni (SIS, SAP), quelli che le eseguono (CGE) e quelli che le controllano (ICI).
16. Le informazioni intercettate attraverso Onyx rappresentano, per i servizi interessati, un valore aggiunto importante. Esse permettono di aumentare le capacità dei servizi di informazioni e di assicurare la loro credibilità all'estero.
17. Il sistema è soggetto a limiti tecnici e finanziari che rischiano di ridurne le potenzialità.
18. La politica di informazione del DDPS verso il Parlamento e il pubblico sulle attività svolte attraverso Onyx è giudicata estremamente riservata.
19. Il sistema Onyx è uno strumento di carattere strettamente nazionale basato unicamente su infrastrutture situate sul territorio svizzero. Non vi sono elementi che confermano una possibile integrazione del sistema Onyx in una qualsiasi rete di esplorazione internazionale.

Tenuto conto di quello che precede, la Delegazione delle Commissioni della gestione

1. raccomanda al Consiglio federale di esaminare l'opportunità di introdurre nella LM un riferimento esplicito alle intercettazioni di comunicazioni all'estero. Il riferimento dovrebbe indicare esplicitamente che le intercettazioni possono riguardare solo comunicazioni all'estero nonché rinviare alle disposizioni del Codice penale secondo cui l'intercettazione di comunicazioni di utenti in Svizzera è punibile;
2. raccomanda al Consiglio federale di esaminare la conformità alla CEDU della legislazione relativa alle attività di intercettazione delle comunicazioni all'estero e, in caso di bisogno, di apportarvi gli adeguamenti necessari;
3. raccomanda al Consiglio federale di presentare, nel suo secondo progetto di revisione della LMSI, una disposizione legale che disciplini i mandati di esplorazione che il SAP effettua o incarica di effettuare in materia di sicurezza interna. Il progetto dovrà essere presentato al Parlamento prima della fase di piena operatività di Onyx;
4. invita il DDPS a stilare un elenco completo dei rischi tecnologici e finanziari che possono compromettere la realizzazione del progetto e delle eventuali misure da adottare il DDPS;
5. invita il Consiglio federale a elaborare, per i servizi di informazione, una strategia quinquennale che presenta gli sforzi e gli investimenti in termini finanziari e umani che il DDPS e il DFGP intendono fare nell'ambito delle fonti di informazione (OSINT, HUMINT, COMINT, collaborazione con servizi partner) e della loro analisi;
6. invita il DDPS ad informare in modo aperto e regolare sulle attività svolte nell'ambito del sistema Onyx.

7 Seguito della procedura

La Delegazione delle Commissioni della gestione invita il Consiglio federale a comunicare il suo parere sul presente rapporto e sulle raccomandazioni entro la fine di marzo 2004.

10 novembre 2003

In nome della Delegazione
delle Commissioni della gestione

Il presidente:
Alexander Tschäppät, consigliere nazionale

Il segretario:
Philippe Schwab

Le Commissioni della gestione hanno preso atto del presente rapporto il 21 novembre 2003 e ne hanno approvato la pubblicazione.

21 novembre 2003

In nome delle Commissioni della gestione

Il presidente della Commissione della gestione
del Consiglio degli Stati:
Michel Béguelin, consigliere agli Stati

La presidente della Commissione della gestione
del Consiglio nazionale:
Brigitta M. Gadient, consigliera nazionale

Abbreviazioni

BND	Bundesnachrichtendienst (servizio di informazione federale tedesco)
CDF	Controllo federale delle finanze
CdG	Commissioni della gestione delle Camere federali
CEDU	Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (Convenzione europea dei diritti dell'uomo), del 4 novembre 1950)(ratificata dalla Svizzera con effetto dal 28 novembre 1974)
CGE	Divisione della condotta della guerra elettronica
CIA	Central Intelligence Agency (servizio di informazione degli Stati Uniti)
COMINT	Communications Intelligence (esplorazione radio)
COMSAT	Comunicazioni via satellite
Cost.	Costituzione federale della Confederazione Svizzera del 18 aprile 1999
CP	Codice penale svizzero del 21 dicembre 1937
CPS-N	Commissione della politica di sicurezza del Consiglio nazionale
DCG	Delegazione delle Commissioni della gestione delle Camere federali
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DFE	Dipartimento federale dell'economia
DFGP	Dipartimento federale di giustizia e polizia
DGSE	Direction générale de la sécurité extérieure (direzione generale della sicurezza esterna)
DSD	Defense Signals Directorate (agenzia australiana di intercettazione delle comunicazioni)
DTF	Decisione del Tribunale federale
ELINT	Electronic intelligence (esplorazione elettronica)
FBI	Federal Bureau of Investigations (ufficio federale investigativo)
GCHQ	Government Comunications Headquarters (agenzia britannica di intercettazione delle comunicazioni)
HUMINT	Human intelligence (raccolta di informazioni tramite fonti umane)
ICI	Istanza di controllo indipendente
LM	Legge federale del 3 febbraio 1995 sull'esercito e sull'amministrazione militare
LMSI	Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna
LRC	Legge federale del 23 marzo 1962 concernente la procedura dell'Assemblea federale e la forma, la pubblicazione,l'entrata in vigore dei suoi atti (legge sui rapporti fra i Consigli)
LSCPT	Legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni

LTC	Legge federale del 30 aprile 1997 sulle telecomunicazioni
NSA	National Security Agency (agenzia americana di intercettazione delle comunicazioni)
OCGE	Ordinanza del 15 ottobre 2003 concernente la condotta della guerra elettronica
OMSI	Ordinanza del 27 giugno 2001 sulle misure per la salvaguardia della sicurezza interna
Onyx	Sistema svizzero di esplorazione delle comunicazioni via satellite
OSINF	Ordinanza del 4 dicembre 2000 sul servizio informazioni del Dipartimento federale della difesa, della protezione della popolazione e dello sport (Ordinanza sul servizio informazioni)
OSINT	Open source intelligence
Patto ONU II	Patto internazionale relativo ai diritti civili e politici, del 16 dicembre 1966 (ratificato dalla Svizzera con effetto dal 18 settembre 1992)
SAP	Servizio di analisi e prevenzione
SATOS-3	Precedente denominazione del progetto Onyx
SIGINT	Signals intelligence (esplorazione dei segnali)
SIS	Servizio informazioni strategico
STOA	Science and Technology Options Assessment Panel (Ufficio per la valutazione delle scelte scientifiche e tecnologiche, servizio della Direzione generale degli studi del Parlamento europeo)
UE	Unione europea
WMD	Armi di distruzione di massa

Intercettazioni delle telecomunicazioni da parte delle autorità svizzere

	Basi legali	Finalità delle intercettazioni e restrizioni	Autorità abilitate a dare ordini di esplorazione	Autorità di sorveglianza	Vie di ricorso
Intercettazioni di comunicazioni in Svizzera					
In materia penale (procedura penale federale o cantonale oppure in caso di assistenza internazionale in materia penale)	LSCPT, OSCPT	Art. 3 LSCPT Esistenza di forti sospetti Gravità del reato giustifica la sorveglianza Le altre operazioni d'inchiesta non hanno dato esito positivo oppure le indagini risulterebbero vane Lista esaustiva degli atti punibili che permettono di ordinare una sorveglianza	Art. 6 LSCPT Procuratore generale della Confederazione Giudici istruttori federali o militari, Autorità competenti giusta il diritto cantonale Direttore dell'UFG (nei casi d'estradizione) Autorità federali o cantonali che eseguono le domande di assistenza giudiziaria	Art. 7 LSCPT Presidente della Camera d'accusa del Tribunale federale, se l'ordine di esplorazione emana d'una autorità civile della Confederazione Presidente del Tribunale militare di cassazione, se l'ordine emana da un giudice istruttore militare Autorità giudiziaria designata dal Cantone, se l'ordine emana da un'autorità cantonale	Art. 10 LSCPT In generale, al termine della sorveglianza, comunicazione dell'intercettazione alle persone sorvegliate e possibilità di ricorrere contro il provvedimento
In materia di informazione	Vietate (art. 179^{octies} CP), eccetto le misure che potrebbero essere adottate dal Consiglio federale in virtù della «clausola generale di polizia (art. 36 cpv. 1 e art. 185 cpv. 3 Cost.)				

Intercettazioni delle comunicazioni all'estero					
In materia penale	Vietate (sovranità territoriale per atti di carattere ufficiale e per le misure coercitive)				
In materia di informazione	Art. 99 LM e OCGE	– Unicamente per ottenere informazioni rilevanti in materia di politica di sicurezza (art. 2 cpv. 2 OCGE) – L'esplorazione non può comprendere utenti svizzeri (art. 5 cpv. 1 OCGE)	I servizi espressamente autorizzati dal capo del DDPS (art. 2 cpv. 3 OCGE)	– Istanza indipendente di controllo (ICI, art. 15 OCGE) – Capo del DDPS (art. 2 cpv. 3, art. 15 cpv. 4, art. 15 cpv. 3 lett b, art. 16 cpv. 3 OCGE) – Altri capi di dipartimenti (art. 15 cpv. 3 lett. b) – Giunta del Consiglio federale in materia di sicurezza (art. 15 cpv. 4, art. 18 cpv. 3 OCGE) – Consiglio federale – Delegazione delle Commissioni della gestione	Non previste nel diritto interno (eventualmente nel diritto convenzionale conformemente all'articolo 8 CEDU o all'articolo 17 del Patto ONU II)

Liste delle persone sentite

(funzione svolta al momento delle audizioni)

Borchert, Heiko	Esperto dell'ispettorato del DDPS, DDPS
Bühler, Jürg S.	Sostituto del capo del Servizio di analisi e prevenzione, Ufficio federale di polizia, DFGP
Ebert, Edwin	Divisionario, sottocapo di stato maggiore dell'aiuto alla condotta, Stato maggiore generale, DDPS
Graf, Urs	Direttore supplente del Servizio informazioni strategico, DDPS
Hofmeister, Albert	Capo dell'ispettorato del DDPS, DDPS
Keckeis, Christophe	Comandante di corpo, capo dello Stato maggiore generale, DDPS
Keller, Martin (+)	Capo dell'ispettorato e progetti del DFGP, DFGP
Kreiliger, Ivo	Sostituto del coordinatore dei servizi d'informazione, Ufficio per l'analisi della situazione e la detenzione tempestiva
Leuthold, Christian	Divisione della condotta della guerra elettronica, Gruppo dell'aiuto alla condotta, Stato maggiore generale, DDPS
Nydegger, Kurt	Capo della Divisione della condotta della guerra elettronica, Gruppo dell'aiuto alla condotta, Stato maggiore generale, DDPS
Ogi, Adolf	Consigliere federale, Capo del DDPS
Regli, Peter	Divisionario, sottocapo di stato maggiore del Servizio informazioni, Stato maggiore generale, DDPS
Rüdin, Jacques	Relatore del capo del DDPS per compiti speciali, DDPS
Scherrer, Hans-Ulrich	Comandante di corpo, capo dello Stato maggiore generale, DDPS
Schmid, Samuel	Consigliere federale, capo del DDPS
Stuber, Peter	Relatore del capo del DDPS per compiti speciali, DDPS
Von Daeniken, Urs	Capo del Servizio di analisi e prevenzione, Ufficio federale di polizia, DFGP
Von Orelli, Martin	Divisionario, sottocapo di stato maggiore del Gruppo servizio informazioni, Stato maggiore generale, DDPS
Wegmüller, Hans	Direttore del Servizio informazioni strategico, DDPS
Werz, Bernard	Sostituto del capo dell'ispettorato e compiti speciali, DFGP
Wyss, Othmar	Sostituto del capo del settore «Commercio mondiale», Segretariato di Stato dell'economia, DFE

La DCG ha anche sentito tre collaboratori del SIS di cui ha deciso di non comunicare le identità.