Xarxa Echelon

Contingut

ECHELON, el sistema ens vigila

Sovint hem sentit a parlar d'espies. Espiar una conversa, espiar a un veí, espiar la correspondència de correus, espiar fent fotografies mig amagats, espiar amb binocles o amb un teleobjectiu, etc. Posar un detectiu a algú, punxar la línia telefònica, posar càmeres de vídeo al carrer, etc. També organismes nacionals legalment constituïts, com el Cesid Espanyol, la CIA dels Estats Units, etc..
Però amb les noves tecnologies, s'obre un gran camp per a espiar i ser espiats. El món dels ordinadors, del correu electrònic, dels telèfons mòbils, dels documents encriptats, etc. Microsoft també insereix codis identificadors als arxius de Word i Excel (clau NSA en el registre). Estats Units liberalitza les seves lleis d'exportació per a programari d'encriptació, però els telèfons mòbils GSM segueixen incorporant un xifrat débil, etc, etc.

Què és Echelon?

El sistema d'intercepció denominat ECHELON es distingeix dels altres sistemes d'intel·ligència en dues propietats que li confereixen característiques molt peculiars:

- En primer lloc, se li atribueix la capacitat d'exercir una vigilància simultània de la totalitat de les comunicacions. Segons s'afirma, tot missatge enviat per telèfon, telefax, Internet o correu electrònic, sigui quin sigui el seu remitent, pot captar-se mitjançant estacions de intercepció de comunicacions per satèl·lit i satèl·lits espia, la qual cosa permet conèixer el seu contingut.
- Com a segona característica d'ECHELON s'esmenta que aquest sistema funciona a escala mundial gràcies a la cooperació de diferents Estats (el Regne Unit, els Estats Units, Canadà, Austràlia i Nova Zelanda), la qual cosa significa un valor afegit en comparació amb els sistemes nacionals: els Estats que participen en el sistema ECHELON (els Estats ECHELON) poden posar-se mútuament a disposició les instal·lacions d'escolta i intercepció, sufragar conjuntament les despeses resultants i utilitzar de manera conjunta la informació obtinguda. Aquesta cooperació internacional és imprescindible, justament, per a una vigilància a escala mundial de les comunicacions per satèl·lit, ja que només d'aquesta manera pot garantir-se que en les comunicacions internacionals puguin captar-se els missatges dels dos interlocutors en un intercanvi. És evident que les estacions d'intercepció de comunicacions per satèl·lit, per les seves dimensions, no poden construir-se al territori d'un Estat sense el consentiment d'aquest. En aquest terreny és imprescindible l'acord mutu i la cooperació de diversos Estats situats en distints continents.

Els possibles perills que un sistema com ECHELON té per a l'esfera privada i l'economia no sols es deriven del fet que es tracti d'un sistema d'intercepció especialment poderós; més aviat es deriva que aquest sistema funciona en un àmbit faltat, gairebé per complet, de regulació jurídica. Generalment, un sistema d'intercepció de comunicacions internacionals no apunta la població del propi país. Així, la persona objecte d'observació, per ser estrangera per al país observador, no disposa de cap mena de protecció jurídica intraestatal. Per això, cada persona està en situació de completa indefensió enfront d'aquest sistema. El control parlamentari resulta, en aquest àmbit, igualment insuficient, ja que els electors, que parteixen de la base que el problema no els afecta a ells sinó «només» a persones que viuen en l'estranger, no mostren especial interès que es controli tal activitat, i els seus representants electes cuiden, en primer lloc, els interessos dels seus electors. Així, no és d'estranyar que a les audiències celebrades al Congrés dels Estats Units sobre l'activitat de la NSA (Agència de Seguretat Nacional dels USA) només s'examini la qüestió de si aquestes activitats afecten ciutadans dels Estats Units, sense que l'activitat de tal sistema, en si, susciti majors inconvenients. Per això és més

important encara examinar aquest afer en l'àmbit europeu, tot i que en aquest àmbit, ja està creada també la pròpia xarxa, l'ENFOPOL.

Mitjans de Comunicació

Quan les persones es desitgen comunicar entre si a una distància determinada, necessiten un mitjà de comunicació. Aquest mitjà pot ser:

- l'aire (ones sonores)
- la llum (centelletjos Morse, cable de fibra òptica)
- el corrent elèctric (telègraf, telèfon)
- ona electromagnètica (el senyal de ràdio en les seves distintes formes).

Quan un tercer aconsegueix accedir al mitjà de comunicació, pot interceptar els missatges que es transmeten per ell. L'accés pot ser fàcil o difícil, des de qualsevol lloc o des de determinades ubicacions. En els apartats següents s'examinen dos casos extrems: les possibilitats tècniques d'un espia al lloc de la comunicació, d'una banda, i les possibilitats d'un sistema d'intercepció que actuï a escala mundial, per una altra.

Qualsevol comunicació pot ser interceptada sobre el terreny quan l'espia està disposat a cometre un delicte i l'espiat no es protegeix enfront d'aquest risc.

- Les **converses** en immobles poden interceptar-se amb micròfons introduïts en ells (micròfons ocults) o captant les vibracions dels vidres de les finestres amb làser.
- Les **pantalles de tubs de raigs catòdics** emeten radiacions que poden captar-se a una distància de fins a 30 metres; d'aquesta manera es fa visible el contingut de la pantalla.
- El **telèfon**, el **telefax** i el **correu electrònic** poden interceptar-se quan l'espia accedeix físicament als cables que surten d'edifici.
- Un **telèfon portàtil** pot interceptar-se a una distància de fins a ... quilòmetres.
- Les **comunicacions radiofòniques internes d'empresa** poden interceptar-se dins l'àmbit de difusió de les ones ultracurtes.

Les condicions per a l'ocupació de mitjans tècnics per a l'espionatge resulten ideals quan aquesta activitat s'efectua sobre el terreny, ja que les mesures d'intercepció poden limitar-se a una persona o un objecte i pràcticament poden captar-se totes les seves comunicacions. L'únic inconvenient és, en el cas de la instal·lació d'un micròfon ocult o de la intercepció física d'un cable, un cert risc que es descobreixi la maniobra.

L'accés als mitjans de comunicació

Comunicació per cable

Es transmeten per cable tots els tipus de comunicació (veu, fax, correu electrònic, dades). La comunicació per cable només pot interceptar-se quan és possible accedir físicament al cable. Això és possible, en qualsevol cas, en els extrems d'una connexió per cable, quan el punt de connexió està dins el territori de l'Estat que ordena o permet la intercepció. En el pla interestatal també és possible, **tècnicament parlant**, interceptar els missatges que circulen per tots els cables, quan les lleis el permeten. No obstant això, els serveis d'intel·ligència estrangers no solen disposar d'accés legal als cables dins el territori de sobirania d'altres Estats. Malgrat aquest suposat impediment, poden aconseguir un accés puntual al cable, de manera il·legal i amb un elevat risc de ser

descoberts.
Les connexions intercontinentals per cable es van crear en l'època del telègraf i mitjançant cables submarins. Sempre resulta possible accedir a aquests cables en els punts en què surten de l'aigua. Quan diversos Estats col·laboren en l'activitat d'intercepció es dóna la possibilitat d'accés a tots els extrems de les connexions per cable que entren en els dits Estats. Aquesta circumstància va ser històricament important, ja que tant el cable submarí telegràfic com els primers cables submarins coaxials telefònics entre Europa i Amèrica en Terranova (en territori de sobirania del Canadà) sortien de l'aigua i les comunicacions amb Àsia passaven per Austràlia, ja que es necessitaven amplificadors intermedis. Avui en dia els cables de fibra òptica s'estenen directament i sense estacions intermèdies a Austràlia ni en Nova Zelanda, sense que el relleu escarpat del fons submarí suposi una dificultat i sense que siguin necessàries les instal·lacions intermèdies d'amplificació. Els cables elèctrics també poden interceptar-se entre els extrems d'una connexió mitjançant inducció (és a dir, per electromagnetisme, aplicant una bobina al cable), sense crear una connexió elèctrica directa. Aquesta tècnica l'empren, amb important desplegament tècnic, els submarins que detecten comunicacions transmeses per cables elèctrics submarins. Aquesta tècnica la van utilitzar els Estats Units per a «punxar» un determinat cable submarí de la Unió Soviètica pel qual es transmetien ordres no xifrades destinades a la flota de submarins nuclears russa. L'ús generalitzat d'aquesta tècnica resulta impossible per allò que s'ha elevat dels seus costos.
En el cas dels cables de fibra òptica de la generació anterior utilitzats encara avui només és possible una intercepció inductiva en els amplificadors intermedis. En ells, el senyal òptic es converteix en senyal elèctric; aquesta s'amplifica i, al seu torn, es converteix en senyal òptic. No obstant això, se insubordinació aquí la qüestió de com transportar les enormes quantitats de dades que es transmeten per un cable d'aquestes característiques des del lloc de la intercepció fins al lloc de la interpretació sense utilitzar al seu torn un cable propi de fibra òptica. L'ocupació d'un submarí amb instal·lacions d'interpretació a bord només es dóna en casos molt aïllats, per motius de costos, com, per exemple, en situacions de guerra i per capturar comunicacions militars estratègiques de l'enemic. Per a la vigilància habitual del tràfic telefònic internacional no té sentit, a judici del ponent, emprar un submarí. Els cables de fibra òptica d'última generació utilitzen un làser d'erbi com a amplificador intermedi; això fa impossible el recurs a tècniques electromagnètiques per interceptar els missatges. Així doncs, aquests cables de fibra òptica només poden ser interceptats en els extrems de les connexions.
Aplicat a la pràctica, tot això significa que per al grup de països que participen en l'estructura ECHELON, els **Estats ECHELON**, només poden interceptar a un cost acceptable les comunicacions transmeses per cable submarí en els extrems del dit cable situats al seu territori de sobirania. Així doncs, fonamentalment només poden captar comunicacions per cable que entren en els seus respectius països o que surten d'ells. És a dir, el seu accés a les comunicacions per cable que entren o surten dels seus països es limita, **a Europa**, al **territori del Regne Unit**.
Fins ara, la major part de les comunicacions internes es transporta per la xarxa nacional de cable; amb la privatització de les telecomunicacions pot haver-hi excepcions, però aquestes són parcials i no predicibles.
Això és així, almenys, pel que es refereix al telèfon i al telefax; per a les comunicacions per Internet a través de cable, les condicions són altres. En síntesi, les limitacions són aquestes:

- En Internet, la comunicació s'efectua mitjançant paquets de dades; els paquets dirigits a un destinatari poden transitar per distints camins dins la xarxa.
- En els començaments d'era d'Internet, les zones de menor tràfic dins la xarxa científica s'aprofitaven per transmetre missatges electrònics. Per això, el camí que seguiria un missatge era completament impredicible; els paquets aïllats recorrien camins caòtics impossibles de preveure. En aquella època, la connexió internacional més important era la «xarxa troncal científica» entre Europa i Amèrica.

- Amb la comercialització d'Internet i l'establiment de proveïdors d'accés es va produir una comercialització de la xarxa. Els proveïdors d'accés a Internet gestionaven o llogaven xarxes pròpies. Per això, intentaven cada vegada amb major freqüència mantenir la comunicació dins la seva pròpia xarxa per evitar pagar drets d'ús a altres membres de la xarxa. Per aquesta raó, avui en dia el camí que recorre un paquet de dades dins la xarxa no sols està determinat per la distribució del tràfic, sinó que també depèn de consideracions de costos.
- Un missatge electrònic que el client d'un proveïdor envia el client d'un altre proveïdor es manté, per regla general, a la xarxa de l'empresa, encara que això signifiqui que el missatge no recorre el camí més curt. Els ordinadors que decideixen sobre el mode de transport dels paquets de dades en els nusos de la xarxa (els denominats «encaminadores») organitzen la transició a altres xarxes en determinats punts de pas (els denominats «punts de commutació»)
- En l'època de les xarxes troncals científiques, els punts de commutació de la comunicació mundial per Internet estaven situats en els Estats Units. Per això, en aquella època els serveis d'intel·ligència podien accedir a una part essencial de la comunicació europea per Internet. Avui en dia, la comunicació intraeuropea per Internet només pansa en una proporció molt reduïda a través dels Estats Units.
- La comunicació intraeuropea pansa en una proporció molt petita per un punt de commutació situat a Londres a què té accés el servei britànic d'intel·ligència (GCHQ). La major part de les comunicacions no abandona el continent. Així, per exemple, més del 95% de la comunicació alemanya per Internet passa per un punt de commutació situat a Frankfurt.

Al terreny pràctic, això significa que els Estats ECHELON només tenen accés a una **part molt reduïda** de la comunicació per Internet a través de cable.

Comunicació per ones

La possibilitat d'interceptar comunicacions transmeses per ones depèn de l'abast de les ones electromagnètiques empleades. Si les ones emeses es mouen per la superfície terrestre (les denominades **ones terrestres**), el seu abast és limitat i depèn de l'estructura del terreny, la presència d'edificis i la vegetació. Si les ones es projecten cap a l'espai (les denominades **ones indirectes o d'espai**), poden superar distàncies considerables després de reflectir-se en capes de la ionosfera. La reflexió múltiple augmenta considerablement l'abast de l'ona.

L'abast de la transmissió depèn de la longitud d'ona:

- Les ones llargues i molt llargues (3kHz-300kHz) només s'expandeixen per l'ona terrestre, ja que l'ona indirecta no es reflecteix. Tenen un abast escàs.
- Les ones mitges (300kHz-3MHz) s'estenen per l'ona terrestre i, de nit, també per l'ona indirecta. Tenen un aconseguiment mitjà.
- Les ones curtes (3MHz-30MHz) s'expandeixen principalment per l'ona indirecta i, per reflexió múltiple, permeten una recepció **d'àmbit mundial**.
- Les ones ultracurtes (30MHz-300MHz) només s'expandeixen per l'ona terrestre, ja que l'ona indirecta no es reflecteix. S'estenen de forma relativament rectilínia, com la llum, per la qual cosa el seu abast depèn, per efecte de la curvatura terrestre, de les altures de les antenes d'emissors i receptors. Segons la seva potència, tenen aconsegueixis de 100 km aproximadament; en el cas dels telèfons portàtils, el seu abast és d'uns 30 km.
- Les ones decimètriques i centimètriques (30MHz-30GHz) s'estenen, encara més que les ones ultracurtes, de forma cuasióptica. Es deixen unir en feixos amb facilitat

i, així, permeten transmissions dirigides amb precisió i amb escassa potència (trams terrestres d'ones direccionals). Només poden captar-se amb una antena pròxima, situada en paral·lel a la línia de transmissió o dins ella o de la seva prolongació.

Les ones llargues i mitges només s'utilitzen per a emissores radiofòniques, radiobalises, etc. La comunicació militar i civil per ràdio s'efectua per ona curta i, sobretot, per ona ultracurta, decimétrica i centimétrica.
De tot l'anterior es desprèn que un sistema d'intercepció que funcioni a escala mundial només pot captar comunicacions transmeses per ona curta. En totes les altres modalitats de la transmissió radiofònica, l'estació d'intercepció ha d'estar, com a màxim, a 100 km de distància (per exemple, en un navili o en una ambaixada).
En la pràctica, això significa que els Estats ECHELON només tenen accés a una part molt reduïda de la comunicació per ones.

Comunicacions per satèl·lits geoestacionaris de telecomunicacions

Com s'ha esmentat, les ones decimètriques i centimètriques poden agrupar-se en feixos amb facilitat i en una direcció precisa. Si es llança una ona direccional cap a un satèl·lit de comunicacions situat a gran altura en òrbita geoestacionària que rep el senyal, l'elabora i torna a enviar-la a la Terra, poden salvar-se distàncies molt grans sense emprar cables. L'abast aquestes transmissions està limitat només, de fet, pel fet que el satèl·lit no pugui rebre senyals de qualsevol punt de la Terra ni enviar-les a qualsevol punt. Per això, per garantir la cobertura global s'empren diversos satèl·lits. En principi, si els Estats ECHELON mantenen estacions d'intercepció a les zones de la Terra que resulten necessàries, poden interceptar tot el tràfic telefònic, de fax i de dades canalitzades per aquests satèl·lits.

Les possibilitats d'intercepció des d'avions i vaixells

Se sap des de fa temps que s'empren avions especials del tipus AWACS per localitzar a altres avions a gran distància. El radar d'aquests aparells es recolza en un sistema de registre per a la identificació d'objectius detectats que pot localitzar i classificar emissions i establir una correlació amb els contactes de radar. No disposen de capacitat independent de SIGINT. En canvi, l'avió espia EP-3, de vol lent, de la Marina dels Estats Units posseeix capacitats d'intercepció de microones i d'ones ultracurtes i curtes. Els senyals s'interpreten directament a bord; l'aeronau serveix per a objectius purament militars.
A més a més, també s'empren vaixells i, prop de les costes, submarins per a l'escolta del tràfic de missatges de ràdio militars.

Les possibilitats d'intercepció des de satèl·lits espia

Les ones de ràdio es difonen, si no s'uneixen en feixos amb les antenes corresponents, en totes direccions; és a dir, també en l'espai. Els satèl·lits d'intel·ligència de senyals que orbiten a baixa altura poden captar els senyals de les emissores objecte d'observació durant uns pocs minuts cada vegada. En zones densament poblades i molt industrialitzades, l'escolta resulta dificultada per l'elevada densitat d'emissores de la mateixa freqüència, de forma tal, que a penes és possible seleccionar mitjançant filtrat els senyals individuals. Per a la vigilància continuada de la comunicació civil per ones radiofòniques, aquests satèl·lits no resulten apropiats.
Paral·lelament, hi ha satèl·lits SIGINT dels Estats Units situats a 42 000 km d'altura, en òrbita semiestacionaria. A diferència dels satèl·lits de comunicacions geoestacionaris,

aquests satèl·lits tenen una inclinació de 3 a 10 graus, un apogeu de 39 000 a 42 000 km i un perigeu de 30.000 a 33.000 km. Per això, els satèl·lits no estan fixos en òrbita, sinó que es mouen en una òrbita el·líptica complexa. Per això, durant un dia cobreixen una extensió major i permeten la localització de fonts d'ones. Tot això, al costat de les característiques dels satèl·lits, que d'altra banda són d'accés públic, indiquen una utilització purament militar.
Els senyals captats es transmeten a l'estació receptora a través d'un enllaç descendent en feix de 24 GHz fortament concentrat en un punt.

Interpretació automàtica de comunicacions interceptades

Per a l'escolta de comunicacions de l'estranger no es pren com a objectiu una connexió telefònica concreta. Més aviat s'enregistra la totalitat o una part de les comunicacions transmeses pels satèl·lits observats o pel cable observat i es filtra mitjançant ordinadors aplicant paraules clau, ja que la interpretació de totes les comunicacions captades resulta absolutament impossible.
El filtrat de les comunicacions que passen per determinades connexions és senzill. Mitjançant paraules clau poden aïllar-se també missatges de telefax i de correu electrònic. És possible, fins i tot, aïllar una veu determinada si s'ensinistra al sistema per reconèixer-la. En canvi, el reconeixement automàtic de paraules pronunciades per una veu qualsevol resulta avui en dia, a jutjar, almenys, per les dades que disposa el ponent, impossible. A més a més, les possibilitats de filtrat estan limitades també per altres factors: per la capacitat limitada dels ordinadors, pel problema de les **llengües** i, primer que res, per la limitació del nombre de persones encarregades de llegir i avaluar els missatges filtrats.
Per avaluar les possibilitats dels sistemes de filtre ha de tenir-se així mateix en compte que les possibilitats tècniques plenes d'un sistema d'escolta que, com aquest, es regeix per el «principi de l'aspirador» es distribueixen en distints temes. Una part de les paraules clau està relacionada amb la seguretat militar; una altra part, amb el tràfic d'estupefaents i altres formes de delinqüència internacional; una altra procedeix del món del comerç amb articles de doble ús; i una altra part està relacionada amb el respecte de l'embargament. Una part de les paraules clau també està relacionada amb l'economia. Això significa que les capacitats del sistema es divideixen en diversos àmbits. Limitar les paraules clau als àmbits econòmicament interessants no sols estaria en contraposició amb les exigències imposades als serveis tècnics per les autoritats polítiques, sinó que ni tan sols s'ha practicat després del final de la Guerra Freda.

Els objectius de l'espionatge

Les dades estratègiques, que són importants per a l'espionatge destinat al sector econòmic, es poden classificar per sectors o sectors empresarials.

Sectors

És evident que tenen gran interès les informacions dels següents sectors: biotecnologia, enginyeria genètica, tècnica medicinal, tècnica ambiental, ordinadors d'alt rendiment, aplicacions informàtiques, optoelectrónica, tecnologia de senyals i sensors òptics, memòries electròniques, ceràmica tècnica, aliatges d'alt rendiment i nanotecnologia. La llista no és completa i, a més a més, canvia constantment d'acord amb el desenvolupament tecnològic. En aquests àmbits, l'espionatge consisteix, sobretot, a robar els resultats de la investigació o tècniques especials de producció.

Sectors empresarials

Els objectius dels atacs d'espionatge es troben, lògicament, en els sectors d'investigació i desenvolupament, adquisicions, personal, producció, distribució, vendes, comercialització, línies de productes i finances. Amb freqüència s'infravalora la importància i el valor d'aquestes dades.

Espionatge competitiu

La posició estratègica d'una empresa al mercat depèn del seu estat en els àmbits de la investigació i desenvolupament, mètodes de producció, línies de producció, finançament, comercialització, venda, distribució, adquisicions i mà d'obra. Les informacions respecte d'això són molt interessants per a tot competidor al mercat, ja que desvelen els plans i debilitats, així que és possible elaborar mesures estratègiques de contraatac.
Una part de tals informacions és d'accés públic. Hi ha empreses consultores molt especialitzades, que dins un marc plenament legal elaboren una anàlisi de competència, com, per exemple, empreses de tan gran renom com Roland & Berger a Alemanya. "Competitive Intelligence" és en els Estats Units, mentrestant, una eina estàndard de gestió. D'una pluralitat de petites informacions és possible elaborar una clara imatge de la situació mitjançant un tractament professional.
La transició de legalitat a espionatge industrial il·legítim es basa en l'elecció dels mitjans amb els que s'obté la informació. Tan sols quan els mitjans empleats són il·legals en el marc jurídic corresponent, comença a ser delictiva l'activitat -la realització d'anàlisi no és en si delictiva-. Les informacions particularment interessants per als competidors, naturalment, són confidencials i únicament poden obtenir-se violant la llei. Les tècniques empleades respecte d'això no es diferencien en res dels mètodes generals d'espionatge.
No es compta amb informacions precises sobre les dimensions de l'espionatge competitiu. Les xifres submergides, igual que en l'espionatge clàssic, són molt altes. Ambdues parts interessades (agressor i víctima) no estan interessades en la publicitat. Per a les empreses afectades això sempre suposa una pèrdua d'imatge i els agressors, naturalment, no tenen cap interès a publicar les seves activitats. Per consegüent, únicament es presenten pocs casos davant dels tribunals.
No obstant això, amb freqüència s'informa en la premsa sobre l'espionatge competitiu. El ponent ha parlat a aquest respecte amb alguns caps de seguretat de grans empreses alemanyes i amb executius d'empreses americanes i europees. En resum, pot constatar-se que l'espionatge competitiu sempre es descobreix, però que no determina l'activitat quotidiana.

Qui espia?

Els principals clients de l'espionatge contra empreses es descriuen en un estudi de l'empresa d'auditoria econòmica Ernest Young LLP, portat a terme amb 39 competidors, 19 clients, 9 subministradors i 7 serveis secrets. Realitzen tasques d'espionatge els propis empleats, les empreses privades d'espionatge, els pirates informàtics a sou i els professionals dels serveis secrets.

Propis empleats (delictes interns)

L'avaluació de la literatura especialitzada, les informacions a aquest respecte dels experts en comissió i les converses mantingudes pel ponent amb caps de seguretat i autoritats d'espionatges coincideixen a demostrar el següent: el major perill d'espionatge part d'uns empleats desil·lusionats i insatisfets. En quant empleats de l'empresa tenen accés directe a les informacions, s'embenin per diners i esbrinen per als seus clients els secrets de l'empresa.

També comporta grans riscos el canvi d'ocupació. Avui en dia no cal copiar muntanyes de papers per emportar-se informacions d'una empresa. Aquestes es poden arxivar discretament en disquets o CD's i emportar-se a la nova empresa quan es canviï d'ocupació.

Empreses privades d'espionatge

El nombre d'empreses que s'ha especialitzat en la recerca de dades creix contínuament. En part, treballen en tals empreses antics empleats dels serveis d'intel·ligència. Aquestes empreses treballen freqüentment tant com a empreses assessores en matèria de seguretat com a agències de detectius que obtenen informacions per encàrrec. Com a norma general s'utilitzen mètodes legals, però també hi ha empreses que empren mètodes il·legals.

Pirates informàtics

Els pirates informàtics són especialistes en ordinador que amb els seus coneixements obtenen des de l'exterior accés a les xarxes d'ordinadors. En els anys inicials, els pirates informàtics eren sonats de la informàtica a què els divertia superar les barreres de seguretat dels sistemes d'ordinadors. En l'actualitat, hi ha pirates informàtics que treballen per encàrrec, tant per als serveis d'intel·ligència com per al mercat.

Serveis d'informació

Després de finalitzada la guerra freda, les tasques dels serveis d'intel·ligència s'han desplaçat. La delinqüència internacional organitzada i la situació econòmica són els seus nous àmbits d'activitat.

Com s'espia?

D'acord amb les informacions de les autoritats de contraespionatge i els caps de seguretat de les grans empreses, en l'espionatge econòmic s'empren tots els mètodes i instruments acreditats en els serveis d'intel·ligència. Les empreses tenen unes estructures més obertes que els organismes militars i els serveis d'intel·ligència o els òrgans governamentals. L'espionatge econòmic suposa, per consegüent, riscos addicionals:

- el reclutament d'empleats és senzill, perquè les possibilitats en la seguretat de les empreses no és comparable a la de les autoritats de contraespionatge;
- la mobilitat laboral fa que importants informacions es portin a l'ordinador portàtil. El robatori d'ordinadors portàtils o la còpia secreta del disc dur després de l'accés il·legal a l'habitació de l'hotel formen part del sistema estàndard de l'espionatge industrial;
- l'accés a les xarxes informàtiques és més senzill que en les institucions estatals amb major sentit de la seguretat, perquè precisament en les petites i mitjanes empreses estan menys desenvolupats els mecanismes i consciència de la seguretat;
- les escoltes sobre el terreny són més senzilles pels mateixos motius.

L'avaluació de les informacions recopilades permet deduir que l'espionatge econòmic es realitza fonamentalment sobre el terreny o en un lloc de treball mòbil, perquè amb poques excepcions la informació desitjada no s'aconsegueix mitjançant la intercepció de les xarxes internacionals de telecomunicacions.

Sí, però, i Echelon?

El desenvolupament d'Internet en els últims anys ha inclòs les dades i missatges que circulen pel ciberespai entre els objectius d'Echelon. La NSA empra programes informàtics robotitzats per recollir informació i fitxers en funció de paràmetres preseleccionats al llarg de les pàgines, servidors, portals i bases de dades d'internet.
L'Agència de Seguretat nord-americana també utilitza programes automatitzats per succionar el correu electrònic i els missatges a través de nou punts neuràlgics d'Internet en EUA.
Dos d'aquests nòduls estan directament controlats per l'Administració nord-americana: College Park, en Maryland, i *Mountain* View, a Califòrnia. Els principals centres d'intercepción i rastreig de comunicacions d'Echelon es troben situats en Menwith Hill (Gran Bretanya), Bad Aibling (base militar a Alemanya) Sugar Grove (Virgina, EUA), Sabana Seca (Puerto Rico), Leitrim (Canadà), Shoal Bay (Austràlia) i Waihopai (Nova Zelanda). La capacitat de captació d'aquestes estacions de radiocomunicaciones s'incrementa constantment. La base de Sugar Grove, situada en una remota àrea de les muntanyes Shenandoah, a unes 250 milles al sud-oest de Washington, disposava el 1990 de només quatre antenes de satèl·lit. Al novembre de 1998, el nombre d'antenes havia crescut fins a nou, de les quals sis estan orientades a les comunicacions europees i atlàntiques.
Echelon compta amb uns supercomputadors especials, denominats «Diccionari», que són capaços d'emmagatzemar una ampli banc de dades sobre objectius específics partint d'un nom, una direcció, un nombre telefònic o altres criteris seleccionats. Quan un satèl·lit detecta una comunicació que pot ser interessant, el missatge se seleciona i s'envia a determinada carpeta als centres especialitzats de la NSA i del GCHQ. Allí, un agent el llegeix i li dóna el curs que correspongui, sempre amb còpia a la NSA. Els serveis britànics reben les comunicacions en Westminster, en el cor de Londres, on disposen d'un d'aquests superordinadors Diccionari.
El filtrat de les converses telefòniques resulta més problemàtic, perquè encara no pot utilitzar-se un programa per detectar automàticament paraules verbals. El sistema que s'utilitza és la preselecció dels nombres de telèfon i de les identitats fòniques (l'empremta vocal individual). De totes maneres, segons les revelacions d'alguns ex-agents britànics, Echelon utilitza moderníssims sistemes de detecció de veu capaç de «entendre» paraules clau. Al «escoltar» una d'aquestes paraules, enregistren automàticament les comunicacions detallant fins i tot la posició d'emissor i receptor.
Les úniques comunicacions que resulten relativament segures són les que circulen per cable de fibra òptica a l'interior de la Unió Europea, a causa de la seva alta capacitat de transport i l'extrema dificultat de seleccionar els missatges. Al contrari, la protecció dels programes criptogràfics d'origen nord-americà és molt dèbil.
Programes amb trampa
Els sistemes de codificació dels programes de Microsoft, Netscape i Lotus exportats fora d'EUA estan especialment adaptats per facilitar la descodificació per part de la NSA nord-americana. El Govern suec va sofrir el 1997 la desagradable experiència de comprovar que la NSA nord-americana disposava d'una part de la clau de codificació del programa de comunicació utilitzat per la seva Administració i que havia estat subministrat per Lotus. El programa era utilitzat per a les comunicacions electròniques confidencials dels ministres, els alts càrrecs governamentals, l'agència tributària i la cúpula de l'administració sueca. La companyia informàtica va explicar que la legislació nord-americana obligava a dipositar en la NSA una part de la clau de codificació (24 dels 64 bits) que s'utilitzarà al criptografiar cada missatge en tots els programes que s'exporten fora d'EUA.
De totes maneres, el descobriment dels treballets d'Echelon ha posat sobre el tapet un problema fonamental: l'espionatge comercial. La xarxa saxona (denominada també Ukusa pel fet que aquestes són les sigles, en anglès, dels Estats Units i del Regne Unit [UK-USA]) utilitza 120 satèl·lits per interceptar les comunicacions. La informació sus-

ceptible de tenir rellevància econòmica o comercial és transmesa per la NSA a les companyies nord-americanes per ajudar-les en les seves operacions i contractes internacionals. La NSA, l'Agència Central d'Intel·ligència (CIA) i el Departament de Comerç van firmar el 5 de maig de 1977 un acord per crear una oficina d'enllaç secreta que canalitzés tota aquesta informació, denominada Oficina de Suport Executiu.
Echelon va ser dissenyat perquè es comporti com una entitat intel·ligent. No es limita a interceptar missatges i retransmetre'ls, ja que l'enorme volum de comunicacions existent el faria inviable. Per això, s'ha apel·lat a procediments informatitzats de reconeixement de veu i de context, i de recerca de paraules. Els missatges intervinguts són confrontats en un «diccionari» a la recerca de concordances. Si es troba alguna combinació de paraules clau-estratègiques, el missatge és enviat a on correspongui. És com una xarxa de deriva intel·ligent, que només captura els peixos que li interessa. Clar que els peixos, ignorants de l'existència de la xarxa, segueixen el seu camí creient-se fora de perill, fins a ser pescats.

Juliol-2001

e-mail: melcior@bermol.com

http://www.bermol.com

juliol-2001