Estructures d'Estat: els serveis d'intel·ligència

Introducció

En aquest breu document farem una descripció general del què és i com funciona un servei d'intel·ligència. En general, la major part de la societat catalana en té una visió esbiaixada i reduccionista, doncs es limita a pensar-hi des de tòpics cinematogràfics i literaris, així com a identificar-los com a eines exclusives dels estats.

Anem per parts doncs: per a què serveix un servei d'intel·ligència? Sent molt planers podem dir que per anticipar riscos i amenaces, tot obtenint informació contrastada i verificada, que ajudi als decisors a actuar encertadament en funció dels interessos.

Si hi pensem una mica, veurem que un servei d'intel·ligència no necessàriament ha de ser exclusiu d'un estat. Qualsevol empresa mitjana o gran, amb un mínim d'organització seriosa, disposa de persones i equips destinats a aquesta funció. Imaginem que una empresa catalana pretén expandir-se al país X sense preveure l'estabilitat política d'aquest, les preferències de consum dels habitants o el grau de corrupció de l'administració. Oi que ho trobaríem temerari? És lògic doncs que disposi dels corresponents informes d'intel·ligència abans de fer cap moviment. No obstant, del que tractarem aquí és de la intel·ligència d'un estat, peça fonamental si realment volem que Catalunya assoleixi aquest nivell. Tampoc parlarem de la intel·ligència militar, doncs aquesta està centrada en aquells aspectes que afecten a les forces armades.

El cicle d'intel·ligència

El primer que hem de comprendre és el que s'anomena cicle (o procés) d'intel·ligència. Està generalment acceptat que consta de les següents etapes:

1. Planificació i direcció
2. Recol·lecció
3. Processament
4. Anàlisi i producció
5. Disseminació

Passem a l'exposició de cadascuna d'elles. Un cop els decisors institucionals (caps d'estat i de govern, ministres, etc...) sol·liciten informació sobre l'afer o persona X, la direcció d'intel·ligència posa en marxa el procés. El temps i els recursos mai són il·limitats i en conseqüència cal una **planificació** acurada per tal d'optimitzar tots els recursos disponibles i en quin ordre els emprem. És impossible enumerar tots els recursos, però proposem agrupar-los en dues grans categories: propis i externs. En els primers hi englobarem no només l'Agència Estatal d'Intel·ligència, sinó totes aquelles institucions (policia, forces armades, ministeris, ambaixades, etc.) que poden generar-nos *inputs* d'informació i formen part d'una mateixa estructura: l'Estat. En els recursos externs hi trobem una enorme quantitat de fonts, de fiabilitat variable, però de la qual no podem pas prescindir. No es tracta només d'altres estats o la comunitat d'intel·ligència internacional. Un recurs extern pot ser una empresa que, per la seva activitat pot aportar-nos informació sobre l'objectiu X. Per descomptat, sempre hi ha la figura dels informadors o confidents, que actuen per motivacions diverses (generalment diners) i dels que se n'ha de fer un us molt caut, buscant sempre la verificació d'allò que ens

aportin per altres vies. Com dèiem més amunt, la comunitat d'intel·ligència internacional serà un marc de treball habitual dins la categoria de recursos externs. Ara bé, i això és important, participar-hi implica **reciprocitat**. Si nosaltres sol·licitem informació sobre l'objectiu X, quan algun altre estat ens en demani sobre l'objectiu Z, li haurem de proporcionar. Pot agradar o no, però aquest és el joc, i Catalunya aspira a "jugar" com un estat. Compresos doncs tots els recursos disponibles i establert un *tempo*, conclourem la planificació i passarem a la següent fase.

La **recol·lecció** d'informació és potser la fase amb que la societat identifica més els serveis d'intel·ligència. No obstant, queda bastant allunyada de la percepció cinematogràfica habitual. Existeix una classificació internacional sobre les àrees de treball o disciplines d'obtenció d'informació. N'enumerem aquí algunes de les més destacades:

- **HUMINT** (*Human Intelligence*): comprèn totes aquelles fonts humanes sobre el terreny que poden aportar-nos informació: agents, confidents, unitats militars de reconeixement clandestí...
- **IMINT** (*Imagery Intelligence*): tota aquella informació provinent d'imatgeria, ja sigui aèria (avions de reconeixement, *drones*...) o espacial (satèl·lits).
- **OSINT** (*Open-source Intelligence*): totes aquelles informacions disponibles en documents no classificats, en contraposició a les que s'obtenen de forma encoberta. En l'actual societat de la informació, cal disposar d'equips que en facin un seguiment constant.
- **SIGINT** (*Signals Intelligence*): comprèn tota la informació provinent de la intercepció de senyals, ja siguin comunicacions de veu o dades.

És una llista breu que podríem ampliar i perfeccionar molt però depassaria les dimensions i nivell d'aquest document. En qualsevol cas, queda clar que la recol·lecció d'informació és una fase que requereix de vàries disciplines, amb moltes especialitats que requereixen professionals qualificats.

El **processament** és la següent etapa. Quan es considera que es disposa d'una quantitat d'informació prou important, cal procedir al tractament i encreuament de dades per tal que aquestes siguin quelcom més que un munt de peces inconnexes. Afortunadament, dècades de progrés en el camp de la informàtica ens permeten realitzar aquest treball amb molta més velocitat. No obstant, el factor humà hi segueix sent present.

Encara que ens segueixin arribant *inputs* des dels mitjans de recol·lecció, com hem dit, quan tenim un volum d'informació acceptable, hem de procedir a la fase d'**anàlisi i producció**. En aquesta fase cal presentar un conjunt intel·ligible, amb les corresponents conclusions, de tota la informació recollida. Els analistes d'intel·ligència, professionals que poden tenir procedències diverses, han de ser capaços de saber encaixar les "peces" procedents de les etapes anteriors. Resumidament, han de ser persones molt "sinàptiques". Cal ser molt conscient que per més que s'hagin reunit quantitats notables d'informació, l'anàlisi i les conclusions van dirigides a decisors institucionals que han d'actuar amb rapidesa i sempre sota pressió. En conseqüència, l'equip d'analistes d'intel·ligència ha de ser molt conscient que no n'hi ha prou amb ser bons en la seva feina, sinó també han de saber transmetre-la de forma entenedora.

La fase de **disseminació** és aquella en que, un cop validada la producció de l'anàlisi d'intel·ligència es fa arribar als decisors institucionals, en primer lloc i, segons convingui, a la comunitat d'intel·ligència. Vol dir això que el cicle s'hagi acabat? No, doncs el més probable és

que fruit de la feina feta s'encarreguin noves anàlisis, així com sol·licituds o propostes de col·laboració d'altres serveis d'intel·ligència. També hem de comptar que les forces armades i la policia, proveïdors d'intel·ligència, en són també receptors. Correspon a l'Agència d'Intel·ligència decidir a qui destina cada informació en funció de les jurisdiccions i capacitats de cadascú. Per exemple, si el servei d'intel·ligència, després del corresponent procés detecta una xarxa de finançament del gihadisme a Barcelona, passarà la informació a Departament d'Interior, perquè la Policia de Catalunya procedeixi a la seva detenció. Si, alhora, detecten que grups gihadistes pretenent atemptar o segrestar a ciutadans catalans a l'exterior, la informació serà passada al Departament de Defensa perquè procedeixi a enviar les Forces Especials, evacuar els nostres i neutralitzar els elements hostils abans no puguin actuar.

La institució

Exposat com funciona el cicle d'intel·ligència, passem a una breu i genèrica proposta d'estructura.

Avui en dia, i malgrat els grans canvis que ha generat la globalització, els estats segueixen essent la cèl·lula bàsica de les relacions internacionals. Cap d'ells, grans o petits, ha renunciat a disposar d'una font pròpia per al proveïment d'intel·ligència. Recordem també que això no està oposat a la col·laboració en el camp que ens ocupa. Actualment la majoria de serveis d'intel·ligència (sobretot els occidentals) disposen d'una agència d'intel·ligència de l'estat, civil, que alhora es subdivideix en altres departaments o agències especialitzades.

Fins la difusió a gran escala d'Internet, les agències d'intel·ligència es dividien en un servei interior i un d'exterior. Podem citar-ne alguns de llegendaris, com els britànics (MI5 – MI6) o els israelians (*Shin Bet – Mossad*). Ambdues divisions comparteixen objectius: protecció de ciutadans i interessos nacionals, avaluació i anticipació a riscos i amenaces, etc.

Amb procediments i àmbits d'actuació diferents (territori propi o estranger) els objectius eren i són comuns. Ara bé, què passa quan el ciber-crim i la ciber-guerra esdevenen un perill clar i present? A quina jurisdicció correspon respondre-hi? Serveis d'intel·ligència, policia, forces armades? La resposta no és clara encara avui, i en la majoria d'estats hi ha hagut una part d'improvisació. Podem trobar departaments dedicats al ciberespai en la majoria d'institucions de seguretat i defensa de tots els estats occidentals. Certament, ni policies ni forces armades poden restar al marge ja del ciberespai però es corre el risc de caure en duplicitats o llacunes per un excés de corporativisme. La futura Agència d'Intel·ligència de Catalunya, a part de les divisions interior i exterior, ha de disposar d'una encarregada del ciberespai. Aquesta divisió no ens hauria de representar un problema excessiu, donada la quantitat de professionals i acadèmics que Catalunya ha generat en el camp de la informàtica i les TIC.

Contra-intel·ligència

Efectivament, quan siguem independents hi haurà serveis d'intel·ligència (estatals o no-estatals) que voldran obtenir informació de nosaltres pels seus propis interessos. És un deure doncs de l'Agència d'Intel·ligència protegir tota aquella informació sensible que pugui ser emprada en perjudici nostre. Ara bé, aquesta informació pot venir de qualsevol de les institucions públiques o infraestructures crítiques (públiques o privades) d'interès vital o estratègic. Posem pel cas que algú aconsegueix obtenir els codis per accedir al software de gestió de la xarxa elèctrica. Tenim un problema oi? És només un exemple.

La majoria de lectors ja deuen haver deduït el que cal fer: tallar, distorsionar o confondre el cicle d'intel·ligència de l'adversari, per tal que n'obtingui unes conclusions errònies o insuficients. I, efectivament, la prevenció és la millor de les formules per evitar que els adversaris assoleixin els seus objectius.

Disposant de la llista d'infraestructures crítiques, així com d'organismes de l'estat que generen informació sensible, caldrà elaborar plans de protecció de la informació. Poden variar en cada cas, però pivotaran sobre dos eixos: jerarquització i compartimentació. La millor manera d'evitar que una cosa no se sàpiga és no dir-la. No obstant, fins la persona més recta i conscient té moments de feblesa o descuit. És per això que ens serveixen els eixos esmentats. Agafem una central nuclear com a exemple. El criteri de jerarquia d'accés a la informació anirà d'il·limitat en el cas de la direcció fins a nul en el cas del personal de neteja. No obstant, això no és suficient, cal aplicar la compartimentació de la informació per tal de que les "fuites" d'aquesta tendeixin a 0. Posem pel cas, els tècnics no tenen perquè comentar als vigilants que en un temps X hi haurà una recàrrega del combustible. Òbviament, aquests plans de protecció de la informació han de contenir mesures de sanció perquè siguin realment efectius, així com programes de formació adaptats a cada nivell.

Des del cap d'estat fins a l'administratiu municipal hi ha d'haver una consciència col·lectiva per la protecció de la informació. L'Agència d'Intel·ligència no pot, per ella mateixa arribar a prevenir totes les fuites d'informació, però si que pot assessorar, avaluar i formar el personal de les institucions i infraestructures crítiques.

Segurament els lectors esperaran que exposem ara com infiltrar-se en les peces que composen el cicle d'intel·ligència de l'adversari, però això també depassa les dimensions i nivell d'aquest document. En definitiva, la contra-intel·ligència és quelcom essencial pel conjunt del país i cal no descuidar-la. En el cas de l'Agència d'Intel·ligència, serà una tasca transversal de tots els seus departaments, tot i que hi hagi responsables específics per la coordinació

Conclusions

Ser un Estat comporta diversos deures, entre d'altres, disposar d'un servei d'intel·ligència eficaç. Sense aquest, no hi ha anticipació ni capacitat per adaptar la Seguretat i la Defensa a escenaris realistes. Sense ser un element actiu en la intel·ligència, generador d'aquesta i no només receptor, Catalunya no tindrà el reconeixement de la comunitat internacional, fet que ens deixarà al marge de determinats àmbits de decisió. I com a catalans, sabem molt bé quin és el preu de no decidir.

ANC - Defensa