Catedràtic de Seguretat Informàtica de la Universitat Rovira i Virgili

Josep Domingo

La seguretat i la defensa de Catalunya

Aquest és un document de reflexió sobre la conveniència que Catalunya es doti d'estructures d'estat en matèria de defensa. No pretén ser un document exhaustiu ni detallat, simplement es proposa centrar el tema. Al segon apartat es tracta la seguretat, la defensa del territori, la intel·ligència i la ciberseguretat. L'apartat tercer s'ocupa del nou paradigma dels conflictes armats actuals que tenen lloc al món. El quart repassa les funcions que exerceixen les forces armades en aquests conflictes i quin tipus de personal els cal per dur-les a terme. El cinquè se centra en les tecnologies de doble ús i les sinergies econòmiques entre l'R+D militar i civil. El darrer paràgraf de cada secció conté conclusions aplicades al futur estat propi català, conclusions que es recapitulen al sisè apartat.

Seguretat, defensa del territori, intel·ligència i ciberseguretat[1]

Quan una nació assoleix un estat propi, agafa les regnes del seu destí. Entre els afers dels quals s'ha d'ocupar ella mateixa, hi ha la seva seguretat i la seva defensa. Convencionalment, la seguretat se sol entendre com la prevenció i la persecució del delicte, el manteniment de l'ordre públic i, més recentment, la lluita anti-terrorista (allò que els americans anomenen *homeland security*). La defensa és més de cara enfora, i es pot definir com la protecció de la sobirania, del territori, de la població i de les infraestructures crítiques contra amenaces o agressions externes. Ara bé, la distinció entre seguretat i defensa es difumina quan parlem del ci-

berespai. En efecte, el món virtual és global i les fronteres estatals no hi regeixen gaire, per molt que alguns estats s'entestin a invertir quantitats enormes per dotar-se de tallafocs: la Xina té fa anys el *Great Firewall of China*, d'altres estats (sobretot musulmans) també restringeixen el trànsit de la xarxa i, en el cas extrem, Corea del Nord es manté pràcticament aïllada d'Internet.

Amb el desplegament progressiu dels Mossos d'Esquadra, Catalunya s'ha anat fent càrrec de la seva seguretat, si més no en el terreny convencional i amb algunes limitacions imposades per l'Estat espanyol. Pel que fa a la seguretat al ciberespai, el Govern de Catalunya va prendre la iniciativa el 2008, amb la creació del Centre de Seguretat de la Informació de Catalunya (CESICAT). En canvi, pel que fa a defensa, el nostre país no té competències ni de moment capacitats específiques, tot i que les estructures de seguretat esmentades són un bon punt de partida. En el que segueix, esbossaré algunes reflexions orientades a desenvolupar aquesta estructura d'estat essencial.

En el context europeu, les amenaces externes molt difícilment seran invasions d'exèrcits estrangers, per la qual cosa tindria poc sentit que un estat català creés unes forces armades convencionals gaire nombroses. Ara bé, tampoc no sembla prudent prescindir-ne totalment si Catalunya vol ser acceptada en el concert dels estats europeus, per la senzilla raó que tots els estats europeus disposen de forces armades convencionals. En efecte, quan en una classe o en un grup d'esplai s'hi incorpora un nen nou, la millor manera que té el nouvingut de fer-se acceptar és comportar-se com la resta de companys. Doncs igual passa amb els estats: serem acceptats més fàcilment si demostrem voluntat de col·laboració lleial amb les actuals aliances internacionals de caire defensiu i d'interposició. Un cop serem un estat consolidat i reconegut, tindrem més marge per plantejar-nos l'oportunitat de models alternatius (neutralitat militaritzada a la suïssa, neutralitat desmilitaritzada estil Costa Rica, etc.).

Els serveis d'intel·ligència i el ciberespai són, en canvi, uns àmbits no convencionals de defensa en els quals Catalunya *no pot fer altra cosa* que apostar-hi decididament ja des d'ara i amb voluntat de continuïtat. Sense capacitats significatives en aquests àmbits, no és només que costi sobreviure com a estat, sinó que costa molt d'esdevenir-ne un: la transició nacio-

nal requereix el control de la informació i de les infraestructures crítiques. La nostra inferioritat pel que fa a serveis d'intel·ligència s'ha fet palesa aquests darrers temps arran dels escàndols d'escoltes i de guerra bruta. Mal m'està autocitar-me, però cinc anys enrere ja vaig reivindicar la creació d'un servei d'intel·ligència català en un article aparegut al diari *Avui* (25-3-2008). No sembla pas que hàgim avançat gaire en aquest tema des de llavors. Per sort, com he apuntat més amunt, hem avançat més pel que fa a ciberseguretat i el país té prou capacitat tecnològica per avançar molt més.

A banda de ser essencial per a la creació i el desenvolupament dels serveis d'intel·ligència, la ciberseguretat és una tecnologia clau per defensar les nostres infraestructures crítiques, des de les centrals energètiques a les telecomunicacions, passant pels aeroports, centres de processament de dades (hisenda pròpia, sistema sanitari, sistema bancari i d'altres) i abastiment d'aigua, gas i electricitat. En efecte, actualment totes aquestes infraestructures crítiques estan controlades per sistemes informàtics, per la qual cosa la seva seguretat esdevé un problema informàtic. En el nostre segle, el ciberespai és l'escenari de moltíssimes batalles silencioses però altament destructives. Per exemple, l'exèrcit xinès ha format unitats especials de guerra cibernètica, en les quals treballen milers de hàckers; semblantment, l'Índia té com a màxima prioritat neutralitzar els ciberatacs rebuts dels seus veïns musulmans i comunistes, etc.

Catalunya, en tant que nació que vol esdevenir estat tot i l'oposició d'Espanya, ha d'estar preparada per detectar i per prevenir eventuals sabotatges derivats de ciberatacs. Cal, en definitiva, un pla integral de protecció de les nostres infraestructures crítiques, que garanteixi que les coses rutllaran l'endemà de la independència, fins i tot si a algun dels nostres veïns li ve l'acudit d'intentar que no rutllin.

Els conflictes armats actuals

En dissenyar estructures per a un estat nou, hi ha l'oportunitat i el deure de fer-ho amb els criteris més moderns possibles, per tal de maximitzar-ne la utilitat i evitar inèrcies caducades i ineficaces. Això inclou el disseny de les forces armades, la missió de les quals és garantir la defensa de l'estat (la seva supervivència en el context internacional) i la seguretat de la seva població (la vida tranquil·la dels ciutadans).

Les forces armades han de respondre al canvi de paradigma que han experimentat els conflictes actuals. Tal com postula el general britànic Sir Rupert Smith en el seu llibre *The Utility of Force* (2005), el paradigma ha passat de ser la «guerra industrial» a ser la «guerra enmig de la població». En una guerra industrial, exèrcits regulars de dos o més governs s'enfrontaven en camps de batalla ben definits fent servir tota la potència industrial i econòmica dels estats respectius, per tal de resoldre una crisi política mitjançant una prova de força definitiva que dugués de nou a una situació de pau. Els dos darrers grans exemples de guerra industrial van ser les guerres mundials. Tot i que aquest tipus de guerra continua essent arquetípic en l'imaginari de la societat, dels mitjans de comunicació i fins de bona part dels militars, té ben poc a veure amb els conflictes armats que s'esdevenen en els nostres dies. Conflictes com la invasió de l'Iraq, la guerra de Bòsnia, la lluita contra Al-Qaida i contra el gihadisme, els successius conflictes d'Afganistan, el conflicte enquistat entre israelians i palestins, els conflictes armats derivats de les primaveres àrabs, la lluita contra el crim organitzat a l'Amèrica Llatina i al Sahel, àdhuc els enfrontaments al ciberespai, etc., són exemples de guerres enmig de la població. Els trets definitoris d'aquesta mena de conflictes són: i) la finalitat de la lluita ja no és decidir la solució política a adoptar, sinó establir condicions en les quals aquesta solució es pugui decidir; ii) es lluita enmig de la població, no al camp de batalla; iii) el conflicte tendeix a ser intemporal, gairebé sense fi; iv) cada facció lluita intentant preservar la seva força, en comptes d'arriscar-ho tot per guanyar l'objectiu (com era el cas a les guerres industrials); v) es fan servir de maneres noves les institucions i les armes heretades de la guerra industrial; vi) la major part de les faccions no són estats, sinó que solen incloure alguna forma de coalició internacional contra una o més organitzacions no estatals (exèrcits irregulars, guerrilles, bandes terroristes, etc.).

La distinció entre seguretat i defensa es difumina quan parlem del ciberespai.

El general i teòric militar prussià Carl von Clausewitz, en el seu tractat *Vom Kriege* (*De la guerra*, 1832), va descriure la guerra com el producte d'un «xoc de voluntats» i d'una «prova de força». En les guerres industrials, des de Napoleó a les guerres mundials, s'aplicava tota la força de cada estat per mirar de guanyar la prova de força i així llevar a l'enemic la voluntat

de continuar lluitant, amb la qual cosa es vencia també el xoc de voluntats. Un exemple paradigmàtic fou el llançament de bombes atòmiques sobre Hiroshima i Nagasaki: llur força devastadora llevà als japonesos la voluntat de continuar la guerra. En les guerres enmig de la població, el que és crític és guanyar el xoc de voluntats, és a dir, a la llarga guanya la facció que aconsegueix atreure's la voluntat majoritària de la població enmig de la qual es desenvolupa el conflicte.

En aquest nou paradigma, com ha d'organitzar les seves forces armades un estat democràtic? El general Smith fa diverses recomanacions. Vivim en un món de confrontacions (antagonismes) i de conflictes continus més que no pas de guerra i de pau. Els estats o les coalicions no fan guerres industrials, sinó «operacions» o «intervencions», que han de ser tan breus com es pugui i que no poden pretendre resoldre per elles mateixes el conflicte polític subjacent amb una victòria militar definitiva. És fonamental que aquestes intervencions militars es coordinin amb intervencions de les altres palanques del poder (poder polític, econòmic, diplomàtic i mediàtic), mitjançant un organisme estratègic únic. Els militars han de donar la màxima importància a les relacions amb la societat enmig de la qual es desenvolupa el conflicte. Han de dotar-se de personal especialitzat d'enllaç que domini la llengua i la cultura d'aquesta societat, que en pugui polsar l'opinió en cada moment i que sàpiga distingir els guerrillers entre la massa dels ciutadans. Les tecnologies de la informació, com la mineria de dades, són de gran utilitat en aquesta tasca d'intel·ligència i d'enllaç. Finalment, per guanyar el xoc de voluntats, els estats s'han de dotar de la màxima legitimitat democràtica, i això se sol aconseguir operant en coalicions internacionals, per exemple, sota el paraigua de l'ONU, de la Unió Europea o de l'OTAN. En aquestes coalicions, tots els estats hi tenen feina a fer, també els estats de la mida de Catalunya. Sent com som ben a la vora de molts dels conflictes actuals, el món no entendria que defugíssim les nostres responsabilitats.

Al nostre segle, el ciberespai és l'escenari de moltíssimes batalles silencioses però altament destructives.

Funcions i tipus de personal de les forces armades modernes

El general Smith distingeix quatre funcions que els militars poden fer

en una confrontació o conflicte: millorar, contenir, dissuadir/obligar i, en darrer terme, destruir. Millorar no implica fer servir la força (llevat d'autodefensa), sinó proporcionar ajuda per restablir la vida civil (per exemple, construint campaments de refugiats, comunicacions, ponts, etc.) o bé entrenar soldats d'altres exèrcits. A banda de situacions de conflicte, els militars també solen fer tasques de millora després de catàstrofes naturals, perquè són un col·lectiu que es troba a punt, que sap sobreviure en condicions adverses i que té algunes de les habilitats que calen. La segona funció, contenir, ja implica un cert ús de la força, per impedir una activitat considerada il·lícita. Exemples de contenció serien impedir que es violin sancions comercials, lluitar contra el tràfic d'armes o imposar zones d'exclusió aèria. La funció de dissuadir/obligar requereix un ús de la força més ampli: per dissuadir, els militars es despleguen per fer creïble una amenaça; per obligar, executen l'amenaça. La guerra freda va ser l'exemple paradigmàtic de dissuasió mútua entre els dos blocs. El bombardeig de Sèrbia per part de l'OTAN el 1999 és un exemple recent d'obligació per la força: va obligar els serbis a retirar-se de Kosovo. Finalment, la funció de destruir implica un ús intens de la força: els militars ataquen l'enemic per tal d'impedir-li d'assolir el seu objectiu polític. La guerra de les Falklands (1982) entre la Gran Bretanya i l'Argentina, o l'operació Tempesta del Desert a l'Iraq (1990-91), són exemples relativament recents d'aquesta funció.

En dissenyar estructures per a un estat nou, hi ha l'oportunitat i el deure de fer-ho amb els criteris més moderns possibles.

Clarament, per realitzar les quatre funcions anteriors en els nous conflictes enmig de la població, no són gaire útils els grans exèrcits de lleva, ideats a partir de la Revolució Francesa per a la guerra industrial. Per això, en els darrers decennis, la majoria d'estats occidentals han anat suprimint el servei militar obligatori. Actualment, la tendència és constituir forces armades molt més reduïdes, amb professionals preparats tècnicament i aptes per a la cooperació internacional. És evident que la funció de millora esmentada anteriorment requereix personal sanitari, administradors i enginyers civils, entre d'altres. Al mateix temps, la complexitat dels equips utilitzats fa que per a totes les funcions calguin enginyers de tota mena. Les tasques d'intel·ligència necessiten des de criptògrafs i matemàtics a antropòlegs i especialistes en llengües, passant per informàtics. De

fet, en alguns països s'han posat en marxa programes de formació d'oficials adreçats a candidats que ja tinguin qualificacions professionals civils: és el cas, per exemple, de la Royal Military Academy Sandhurst al Regne Unit. En d'altres països, existeix una simbiosi entre la formació tecnològica i la militar que ha estat tan o més fructífera per a l'economia que per a les forces armades: és el cas d'Israel i dels Estats Units, que compten amb multitud d'empreses tecnològiques que van originar-se per respondre a necessitats militars i que actualment exporten tecnologia civil arreu del món.

Els estats democràtics de la mida de Catalunya estan entrant també en el nou paradigma, fins i tot els més exigents en termes d'ètica pública, com serien els països escandinaus. Dinamarca, amb menys habitants que Catalunya, té la capacitat de desplegar dos mil soldats en missió internacional, que poden ser fins a cinc mil durant un període curt. Amb una població semblant a la danesa, Noruega, que concedeix cada any el Premi Nobel de la Pau i que té un prestigi reconegut com a mitjancer en conflictes internacionals, té desplegats soldats a la zona àrtica i a l'Afganistan. Suècia, lleugerament més poblada que el nostre país, no només té forces armades, sinó que té una indústria capdavantera de defensa que exporta al món sencer. Per exemple, el grup Saab, que fins al 2010 fabricava els coneguts automòbils, actualment només es dedica a la indústria aeroespacial i de defensa.

Podem veure, doncs, que hi ha una sinergia creixent entre el sector militar, les universitats i el sector tecnològic en la majoria de països avançats, fins al punt que el primer actua sovint de tractor dels altres dos. D'altra banda, tal com es veurà a la secció següent, aquesta sinergia també ha contribuït a «democratitzar» la tecnologia militar, fent-la molt més assequible i encoratjant-ne les aplicacions civils. Un país amb la situació geoestratègica i la vocació industrial de Catalunya faria bé de seguir els passos dels estats més avançats i democràtics d'Europa en matèria militar.

Tecnologies de doble ús: sinergies entre l'R+D militar i civil

Als tres àmbits de defensa tradicionals, terra, mar i aire, en les darreres dècades se n'hi han afegit dos més, l'espai i el ciberespai. Paradoxalment,

la sofisticació progressiva de la tecnologia militar n'està augmentant el doble ús per a propòsits civils, i viceversa.

Per més que les guerres industrials ja formin més part del passat que del present, les inèrcies dels governs i els interessos del complex militar-industrial fan que es continuï desenvolupant i renovant equipament per a aquest tipus de conflictes, com ara vehicles blindats, vaixells, avions de guerra i satèl·lits militars. Igualment, els Estats Units, Rússia i la Xina continuen invertint grans quantitats de diners per renovar llur armament dissuasiu de la guerra freda, sobretot els caps nuclears. Tot i així, la doctrina predominant ha canviat radicalment: avui dia l'enfrontament és «sistema contra sistema». En altres paraules, per guanyar n'hi ha prou de destruir l'equipament de l'enemic, les seves infraestructures crítiques i la seva capacitat tecnològica, no cal pas delmar-ne els combatents. A tall d'exemple, mentre que la Primera Guerra Mundial no va acabar-se fins que la meitat dels combatents van ser morts o ferits, l'exèrcit de Saddam Hussein va caure derrotat a la segona guerra del Golf quan només tenia un 2,6% de baixes (però s'havia quedat sense ni blindats ni avions). És innegable que la precisió creixent de l'armament permet de minimitzar les baixes en els nous conflictes.

A la majoria de països avançats hi ha una sinergia creixent entre el sector militar, les universitats i el sector tecnològic.

Tot i que l'armament clàssic esmentat al paràgraf anterior no sembla gaire útil a la vida civil, moltes de les tecnologies subjacents sí que són clarament de doble ús. Els làsers tenen molts usos militars: se'n fan servir per guiar míssils i per incapacitar o destruir satèl·lits espia, i se n'està explorant l'ús en paraigües anti-míssils i per recarregar d'energia els satèl·lits militars. D'altra banda, són més que evidents les seves aplicacions civils en ciència, medicina, química i molts més camps; ben aviat, la funció de recàrrega d'energia de dispositius remots, iniciada en l'àmbit militar, pot esdevenir una nova aplicació civil. Els petits reactors nuclears que es van inventar per propulsar vaixells i submarins de guerra s'estan considerant ara per a generació d'electricitat amb finalitats civils. En efecte, són dissenys molt provats i tenen l'avantatge de la modularitat: es poden anar afegint petits reactors a una planta nuclear a mesura que augmenta la demanda d'energia i el cost resultant pot arribar a ser un terç d'un sol gran

reactor de capacitat equivalent. Els sistemes de navegació per satèl·lit o la mateixa Internet sorgiren en l'àmbit militar i ara són indestriables de la vida civil. El mateix podríem dir dels famosos *drones* o avions no tripulats, que han permès atacs molt selectius en les actuals guerres enmig de la població; aquests artefactes voladors tenen cada cop més aplicacions civils, com la vigilància de recintes o de parcs naturals, la fotografia aèria i potser aviat l'extinció d'incendis sense perill de la vida dels bombers. També hi ha transferència de tecnologia civil cap a usos militars, sobretot centrada en la informàtica i l'electrònica de consum: els jocs d'ordinador es fan servir per a entrenament militar, i els processadors gràfics de les videoconsoles s'usen per construir superordinadors tant d'ús militar (per exemple, el Roadrunner del Los Alamos National Laboratory nord-americà) com civil (el mateix Mare Nostrum, del Barcelona Supercomputing Center).

Més enllà de la terra, el mar, l'aire i l'espai, hi ha el ciberespai, en el qual la distinció entre tecnologia civil i militar s'esborra gairebé completament. Estats, empreses i particulars poden ser cibervíctimes i cibercriminals. Al ciberespai s'hi lliuren guerres enmig de la població, amb ciberguerrillers atacant ordinadors i infraestructures crítiques de governs i amb governs fent servir mineria de dades i altres tecnologies per rastrejar guerrillers i ciberguerrillers i distingir-los de la població entre la qual es confonen. Igualment, al ciberespai s'hi lliuren lluites econòmiques i polítiques, amb l'espionatge com a principal activitat. És evident que la ciberseguretat és un tema en el qual la cooperació entre els sectors civil i militar és fonamental.

Un país democràtic que aspiri a tenir un estat propi i a ser competitiu en tecnologia i en indústria s'ho hauria de pensar molt i molt abans de donar l'esquena al món de la defensa. Per exemple, si Catalunya realment vol constituir *clústers* potents en tecnologies de la informació i de les comunicacions o bé en aeronàutica, no només no ha d'ignorar que són tecnologies de doble ús, sinó que ho ha d'explotar a fons. La mateixa reflexió és aplicable per facilitar que la recerca d'excel·lència sobre làsers que es fa a Catalunya (per exemple, a l'ICFO) pugui transferir-se a empreses del país.

Conclusions

Llisto a continuació les conclusions que he anat posant al final de cadascuna de les seccions anteriors:

- Catalunya, en tant que nació que vol esdevenir estat malgrat l'oposició d'Espanya, ha d'estar preparada per detectar i per prevenir eventuals sabotatges derivats de ciberatacs. Cal, en definitiva, un pla integral de protecció de les nostres infraestructures crítiques, que garanteixi que les coses rutllaran l'endemà de la independència, fins i tot si a algun dels nostres veïns li ve l'acudit d'intentar que no rutllin.
- Els conflictes armats actuals que s'esdevenen al món solen tenir lloc enmig de la població, i per guanyar-los és fonamental guanyar-se la voluntat d'aquesta població. Això requereix que els països democràtics hi actuïn revestits de la màxima legitimitat, cosa que se sol aconseguir operant en coalicions internacionals, per exemple, sota el paraigua de l'ONU, de la Unió Europea o de l'OTAN. En aquestes coalicions, tots els estats hi tenen feina a fer, també els estats de la mida de Catalunya. Sent com som ben a la vora de molts dels conflictes actuals, el món no entendria que defugíssim les nostres responsabilitats.

La ciberseguretat és un àmbit en el qual la cooperació entre els sectors civil i militar és fonamental.

- Pràcticament cap estat democràtic de la mida de Catalunya no renuncia a tenir unes forces de defensa, ni tan sols els països més exigents en termes d'ètica pública, com serien els països escandinaus. Dinamarca, amb menys habitants que Catalunya, té la capacitat de desplegar dos mil soldats en missió internacional, que poden ser fins a cinc mil durant un període curt. Amb una població semblant a la danesa, Noruega, que concedeix cada any el Premi Nobel de la Pau i que té un prestigi reconegut com a mitjancer en conflictes internacionals, té desplegats soldats a la zona àrtica i a l'Afganistan. Suècia, lleugerament més poblada que el nostre país, no només té forces armades, sinó que té una indústria capdavantera de defensa que exporta al món sencer. Un país amb la situació geoestratègica i la vocació industrial de Catalunya faria bé de seguir els passos dels estats més avançats i democràtics d'Europa en matèria militar.
- Un país democràtic que aspiri a tenir un estat propi i a ser competitiu

en tecnologia i en indústria s'ho hauria de pensar molt i molt abans de donar l'esquena al món de la defensa. Per exemple, si Catalunya realment vol constituir *clústers* potents en tecnologies de la informació i de les comunicacions o bé en aeronàutica, no només no ha d'ignorar que són tecnologies de doble ús, sinó que ho ha d'explotar a fons. La mateixa reflexió és aplicable per facilitar que la recerca d'excel·lència sobre làsers que es fa a Catalunya pugui transferir-se a empreses del país.

1. Aquest apartat fou publicat per l'autor al diari *Ara* el 6 de maig del 2013 amb el títol «La seguretat i la defensa de Catalunya».