EL TEMPS

Fa dos anys, el Pentàgon va decidir les mesures que podria prendre en el cas d'un ciberatac, seria

Tot esperant un Pearl Harbor cibernètic

Ara les guerres també es combaten en camps de batalla digitals. Per això, experts en dret internacional han establert unes normes per a les ciberguerres. S'hauria de permetre en el futur una resposta amb mitjans militars?

L'atac s'amagava en un correu electrònic ordinari. Fa dues setmanes, algunes empreses sud-coreanes, sens dubte escollides, van rebre missatges que contenien presumpta informació sobre targetes de crèdit.

Els destinataris que els van obrir tenien l'enemic a casa; dins dels correus s'ocultava un atac des d'Internet. En lloc de la informació de les targetes de crèdit que esperaven, els destinataris es van descarregar una bomba, que estava programada per a fer explosió dimecres a les 14:00 hora local.

Puntual, el caos es va sembrar en més de 30.000 ordinadors, en canals de televisió i bancs sud-coreans. En les pantalles va aparèixer un missatge que deia: "Instal·leu un sistema operatiu", els caixers automàtics es van quedar fora de servei. El programari maliciós, que els experts han batejat com Darkseoul, va eliminar dades dels discos durs, de tal manera que els ordinadors infectats ja no es podien reiniciar.

Encara que Darkseoul, enguany, ha estat un dels atacs digitals més greus del món, els centres de ciberdefensa de les capitals occidentals reben noves alertes gairebé setmanalment. L'atac més violent fins ara va venir des d'Amèrica: el 2010, *soldats d'alta tecnologia* van introduir el cuc informàtic Stuxnet a la central nuclear d'Iran per ordre del president dels EUA.

Però això no va quedar així. Caps militars dels EUA i els seus socis europeus de l'OTAN estan preparant nou batallons per a l'imminent guerra de dades. I arreu del món, experts en dret internacional discuteixen sobre l'índole de la nova amenaça: Es tracta d'una guerra, comptat i debatut? O es tracta d'un sabotatge i d'actes terroristes? I si fóra realment una nova classe de guerra, també caldria respondre amb mitjans militars?

Uns quants dies abans del desastre informàtic a Seül, va aparèixer un llibret, prim, blau, sota els auspicis de l'OTAN, que dóna respostes perilloses a totes aquestes preguntes. Probablement, el "manual de dret internacional aplicat a les ciberestratègies de guerra" no és més gros que el polze del president nord-americà. No és cap document oficial, però a les mans de Barack Obama pot canviar el món.

Les normes que han compilat en el manual els influents experts en dret internacional es presten a esborrar les fronteres entre guerra i pau i permeten que aviat s'agreugen ja seriosos atacs de dades i es convertisquen en una autèntica guerra amb bombes i míssils. Els caps militars també podrien interpretar-les com una invitació a un primer colp preventiu en una ciberguerra.

A la trobada d'un equip d'especialistes de l'OTAN a la capital estoniana

un míssil com a resposta.

de Tallinn i sota la presidència d'un advocat militar nord-americà proper al Pentàgon, els alts representants dels experts en dret internacional van discutir sobre les normes de la guerra del futur. La major part del dret internacional és dret consuetudinari. I els experts determinen allò que es pot considerar i es considera dret consuetudinari.

El document resultant, el "Manual de Tallinn", és el primer codi informal per a les guerres del futur. Però no té cap efecte tranquil·litzador, tot el contrari, ja que permet respondre a atacs cibernètics amb armes de les guerres reals.

Fa dos anys, el Pentàgon ja va aclarir la direcció que podria prendre: qui intentara, per exemple, tallar el corrent elèctric a la nació més poderosa del món amb un programari maliciós, hauria de comptar amb un míssil com a resposta.

Les últimes setmanes, els perills d'una ciberguerra es van invocar més clarament que mai a Washington. A mitjan març Obama es va reunir amb 13 alts representants de l'economia dels EUA a la Sala de Situacions, la més secreta de totes les sales secretes de conferències a la planta subterrània de la Casa Blanca. Entre ells hi havia els caps d'UPS, JPMorgan Chase i Exxon Mobil. Hi hauria un tema únic: com pot guanyar Amèrica la guerra en la xarxa?

Un dia abans, James Clapper, director d'Intel·ligència Nacional, havia qualificat la ciberamenaça com del "més gran perill a escala mundial".

La Casa Blanca no va voler desvelar el que van discutir Obama i els caps d'economia. "Es tractava, sobretot, de deixar clar a les empreses el grau d'amenaça que pateixen, perquè reforcen la seua disposició a cooperar", diu Christopher Bronk, expert en TIC a la Universitat de Rice.

El president necessita amb tota urgència la seua cooperació, ja que els EUA han deixat les infraestructures digitals en mans de les lleis del mercat. Tota la xarxa és gestionada per empreses privades. Si hi haguera una guerra en la xarxa, llavors els camps de batalla i les armes es trobarien en mans privades.

Per això, la Casa Blanca prepara possibles contraatacs amb molt d'esforç. "Hem d'infondre por als nostres enemics", diu l'ex-general James Cartwright, autor de les actuals ciberestratègies del Pentàgon.

El responsable d'aquesta estratègia és el cibercomandament del Pentàgon amb 900 empleats, la seu del qual és a Fort Meade, molt prop de l'Agència de Seguretat Nacional (NSA), el servei d'intel·ligència més gran dels EUA. Totes dues organitzacions tenen el mateix cap: el general Keith Alexander. S'espera que el cibercomandament tinga, al cap de pocs anys, al voltant de 4.900 empleats i que se separe en diferents "ciberforces de missió" (Cyber Mission Forces) d'atac i defensa.

No és cap coincidència que el Manual de Tallinn s'haja publicat justament ara. Creat sota la responsabilitat de Michael Schmitt, els representants de l'OTAN el descriuen com el "document legal més important de la ciberera".

L'advocat militar Schmitt va estudiar la legalitat de l'ús dels –absolutament confidencials– sistemes d'armes nuclears i els pros i els contres dels atacs nord-americans de *drones*. Els visitants de la seua oficina a l'Escola de Guerra Naval a l'estat de Rhode Island, l'acadèmia naval més antiga del món, han de passar diversos controls de seguretat.

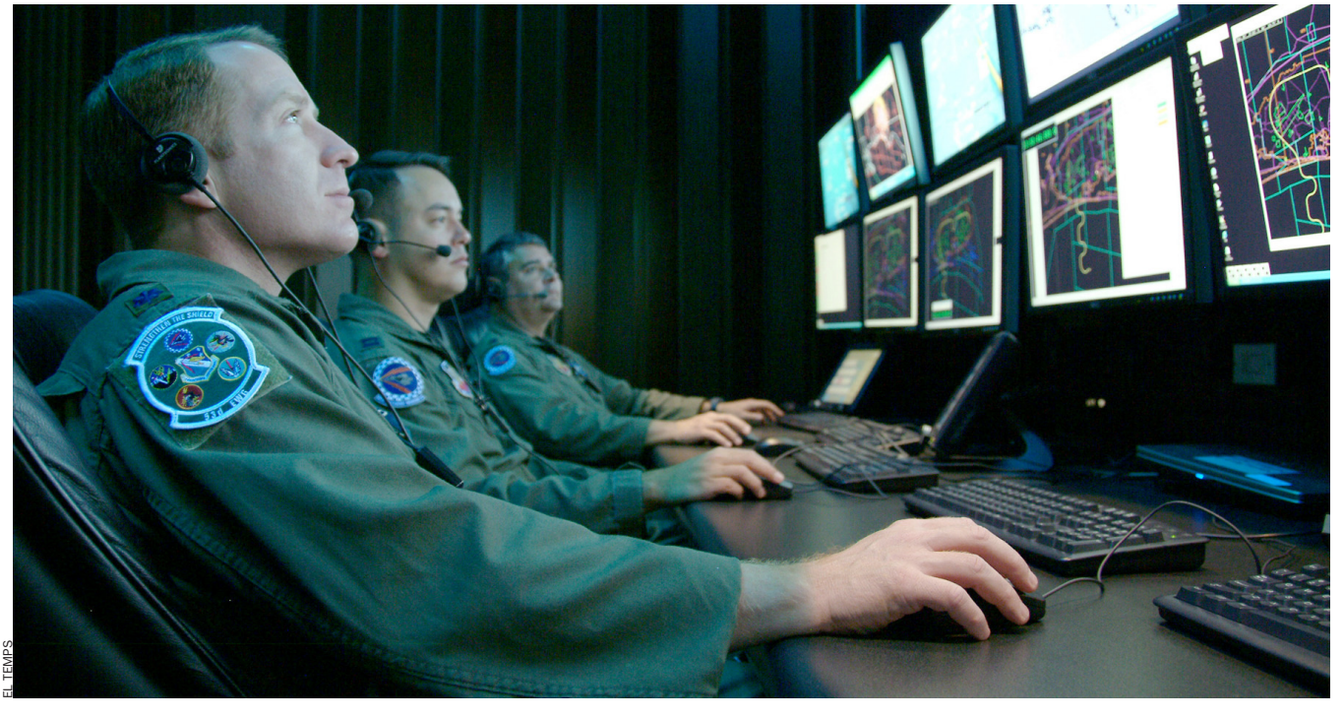
"Siguem honestos", diu Michael Schmitt, "tothom ha vist Internet com una mena de salvatge Oest, un espai sense lleis. Però el dret internacional s'ha d'aplicar tant a les ciberarmes com a les armes convencionals."

Això es diu aviat. Però quan es converteix un cuc informàtic en arma? I un *hacker*, en quin moment es converteix en soldat? I el simple entreteniment, o l'espionatge, adquireix categoria d'atac armat contemplat pel dret internacional? Les respostes a tan minucioses preguntes poden explicar amb claredat la diferència entre guerra i pau.

James Lewis, un dels experts caps de ciberguerra dels EUA del Center for Strategic and International Studies (CSIS), es mostra escèptic pel que fa al nou manual. Lewis el veu com un intent de reduir les barreres per als contraatacs militars. L'expert creu que respondre amb mitjans militars als atacs que provoquen la denegació del servei és una bogeria. Lewis diu que el suggeriment del manual no té un propòsit fix.

Claus Kreß, expert en dret internacional i director de l'Institut per la Pau i la Seguretat Internacionals de la Universitat de Colònia, veu en el manual una "línia d'actuació" amb "conseqüències per a tota la legislació sobre l'ús de la força". S'hi estan posant a disposició importants "barreres legals" que havien d'impedir l'escalada bèl·lica dels conflictes polítics o dels actes terroristes.

Segons Kreß, el punt més decisiu és el "reconeixement del dret nacional a la legítima defensa contra ciberatacs". Això correspon a l'estat de defensa, com defineix l'article 51 de la Carta de les Nacions Unides, que garanteix a tots els estats que siguen víctimes d'un atac armat el dret a defensar-se amb l'ús de la força. L'article va cobrar un nou sentit després de l'11 de setembre de 2001, quan els EUA van anunciar l'ocupació d'Afganistan com a legítima defensa contra al-Qaida i l'OTAN



EL TEMPS

Especialistes en ciberguerra de la força aèria dels Estats Units a la base de Florida.

va declarar el *casus foederis* per venir en socors de la potència mundial.

Preguntar-se quin grau de malícia ha de tenir un programari maliciós per a justificar el dret a un contraatac és decisiu per a la pau. Segons la nova doctrina, sols aquells atacs que provoquen danys físics o personals, però no virtuals, són rellevants en termes de dret internacional. El mal funcionament d'un ordinador o la pèrdua de dades solament no basten per a parlar d'un "atac armat".

Però què passa, com és freqüent, si les avaries dels ordinadors no porten a danys físics, sinó a danys econòmics considerables? Un ciberatac a Wall Street amb una interrupció de la borsa de diversos dies fou el *casus belli* entre els experts a Tallinn. Els representants dels EUA volien reconèixer-lo com un estat de defensa, mentre que els europeus no. Tanmateix, els advocats militars dels EUA insistien que els danys econòmics justifiquen el dret a contraatacar si són catastròfics.

Últimament, és a les mans de cada país de decidir quin grau de danys econòmics considera suficient per a aventurar-se en una guerra. Per això, l'expert en dret militar Kreß tem un "trencament del dic" per a la prohibició d'ús de la força sota el dret internacional.

Llavors, també va ser atac armat el que va tenir lloc a Corea del Sud? Els danys econòmics que va provocar la fallada dels ordinadors dels bancs no s'han calculat encara. Els polítics, i no els advocats, decidiran si són catastròfics.

Aquest mes es feia evident amb quina rapidesa Internet es pot convertir en un escenari de conflictes massius: de sobte, com sorgits del no-res, van aparèixer dos grans proveïdors entre atacs digitals constants.

L'objectiu principal d'atac va ser el lloc web *spamhaus.org*, un projecte que persegueix distribuïdors de correu brossa a la xarxa des de 1998. Aquest permet a altres proveïdors amb llistes negres de coneguts emissors de correu brossa de filtrar-lo. Donant aquest servei, l'organització es crea enemics i, per això, ha sigut la diana de molts atacs. Tanmateix, l'actual onada d'atacs li fa ombra. No sols va paralitzar *spamhaus*, sinó fins i tot també va afectar temporalment l'empresa nord-americana CloudFare, que va ajudar en la defensa dels atacs. Els analistes van calcular la força de l'atac en 300 gigabits per segon, que és diverses vegades més fort que el nivell al qual foren *tirotejades* les autoritats estonianes l'any 2007. L'atac va afectar fins i tot el trànsit de dades de tot Internet. El grup Stophaus es va declarar responsable i es va justificar manifestant una revenja contra *spamhaus* per haver-se entremès en els negocis de poderoses companyies russes i xineses d'Internet.

Les forces civils, motivades per interessos econòmics, juguen a la ciberguerra regirant tota la lògica de guerra que hi haja pogut haver fins ara.

Un assaig de camp als EUA ha demostrat la veracitat de l'amenaça. L'empresa de programaris i antivirus Trend Micro va construir una estació de bombament virtual en una petita ciutat americana, almenys, això és el que havia de semblar-los als visitants de la xarxa. En deien "pot de mel", dissenyat per a atreure potencials atacants en la xarxa.

Els paranyers van instal·lar servidors i sistemes de control industrials com els que utilitzen les companyies de serveis públics d'aquesta magnitud. Per donar més versemblança a la

El "Manual de Tallinn" és el primer codi informal per a les guerres del futur

disposició de l'experiment, fins i tot van penjar documents de l'administració municipal que semblaven autèntics aparentment.

Tot just al cap de 18 hores, els analistes ja havien registrat el primer intent d'atac. Durant les quatre setmanes següents hi hagué 39 atacs de 14 països diferents. La majoria procedien de la Xina (35%), seguida dels EUA (19%) i Laos (12%).

Molts atacants van intentar introduir eines d'espionatge a la suposada estació de bombament d'aigua per provar la feblesa de la pàgina. El dret internacional no prohibeix l'espionatge. Però alguns passaren de la ratlla: intentaren manipular i, fins i tot, destruir els sistemes de control.

"Alguns van intentar augmentar el nombre de revolucions de les bombes hidràuliques", diu Udo Schneider, treballador de Trend Micro, que qualifica aquests casos de "sabotatge clàssic".

"La pregunta no és si hi haurà ciberatacs catastròfics contra els EUA. La pregunta és quan", diu Terry Benzel, la dona que ha de protegir els EUA contra aquest tipus d'atacs fent més segures les xarxes cibernètiques. La qualificada especialista en informàtica és la directora de DeterLab a Califòrnia, un projecte fundat amb la col·laboració del Ministeri de Seguretat Nacional dels EUA, que ofereix una plataforma de simulació per a les reaccions davant els ciberatacs.

A Benzel no li tremola la veu quan parla d'un escenari de guerra que anomena "Cyber Pearl Harbor". Aquest podria ésser l'escenari: "Talls del subministrament elèctric durant períodes de temps prolongats, un col·lapse de la xarxa elèctrica, avaries irreparables en Internet". De sobte, el menjar no arribaria a temps a les tendes i els caixers automàtics ja no repartirien més bitllets. "Ara tot depèn dels ordinadors, fins i tot la venda d'entrepans d'aquí de la cantonada", diu Benzel.

També descriu altres escenaris de crisi: assenyala programes que obrin i tanquen les comportes dels dics dels EUA, que són considerablement vulnerables. Un *hacker* intel·ligent podria, segons tem Benzel, obrir les preses d'Amèrica quan li vinguera de gust.

Aquests i més casos són posats a prova actualment en "Cyber City", una ciutat model que han construït experts dels EUA en els seus ordinadors a Nova Jersey per poder simular les conseqüències dels ciberatacs de dades. Hi ha una torre d'aigua, una estació de trens i 15.000 habitants. Tot està connectat d'una manera molt versemblant, cosa que permet estudiar als experts la desolació que entre els habitants provocarien els ciberatacs.

EL TEMPS

El general Keith Alexander és el cibercomandant del Pentàgon i el responsable de l'Àgència de Seguretat Nacional (NSA), el servei d'intel·ligènica més gran dels Estats Units.

A Europa són sobretot els serveis d'intel·ligència els que proven els jocs digitals de guerra. Al Servei Federal d'Intel·ligència i Contraespionatge (BND: *Bundesnachrichtendienst*), una unitat treballa els detalls de les futures guerres. Cal destacar que no se simulen solament situacions defensives, sinó, cada vegada més, escenaris ofensius per a estar preparats, si més no, per a una mena de segon atac digital.

Ciberoperacions ofensives, les anomenades OCOs, formen part de l'estratègia per a les futures ciberguerres en diversos estats membres de l'OTAN. El Manual de Tallinn estableix també una base legal per a possibles atacs preventius. Aquest ha sigut un tema de debat des que el president George W. Bush va llançar el seu atac preventiu contra l'Iraq.

El punt més polèmic de les discussions a Tallinn va ser la qüestió següent: és admissible un atac ofensiu com a acte de preventiva legítima defensa contra ciberatacs? D'acord amb la doctrina actual, un atac hauria de ser "imminent" per a activar el dret a una legítima defensa de manera preventiva. Pel que fa al cas, el Manual de Tallinn és més generós: encara que una ciberarma mostre els seus efectes funestos més tard, el primer colp ja podria haver-se justificat.

La doble moral es manifesta en el tracte dels experts en dret internacional amb Stuxnet, el programari maliciós més devastador fins a la data, que va ser introduït per ordre del president Obama a les instal·lacions de la central nuclear iraniana. L'atac de dades va destruir centrifugadors amb què s'obté urani enriquit a la planta de reciclatge de Natanz.

EL TEMPS

El perill d'una ciberguerra obliga Barak Obama a reunir-se amb alts representants de l'economia d'Estats Units per preparar una cooperació.

Segons els criteris del Manual de Tallinn, això constituiria un acte de guerra.

Els EUA com a perpetrador d'un atac de guerra que viola el dret internacional? L'expert en dret internacional Claus Kreß creu que el que diu el Manual de Tallinn entre parèntesis sobre el cas Stuxnet és una instrucció per al Pentàgon, ja que allà l'atac digital d'Obama es veu com un acte de legítima defensa preventiva contra el programa nuclear dels aiatol·làs.

D'acord amb la interpretació de Tallinn, un sens fi d'incidents virtuals d'espionatge que afecten els països industrialitzats gairebé a diari podrien actuar com a acceleradors. Però, el pur ciberespionatge, també anomenat *atac* pels polítics, no és un acte de guerra segons les normes de Tallinn. No obstant això, els experts en dret internacional opinen que tals atacs d'espionatge es poden valorar com una preparació per a atacs destructius. Per això, podria ésser legítim llançar un atac preventiu contra l'espia per defensar-se.

Alguns mostren preocupació davant les propostes del manual, perquè podrien ampliar les normes de la "guerra contra el terrorisme". Els autors del manual han incorporat la petició de Joseph Nye, expert en geoestratègia dels EUA, de prendre precaucions contra un "ciber 11-S". Això significaria que la superpotència podria declarar la guerra, fins i tot, a grups de *hackers* organitzats. *Drones* de combat per a enfrontar-se als *hackers*? L'expert Kreß considera que l'ampliació del camp de batalla cap a ordinadors particulars "constituiria una amenaça per als drets humans".

Mentrestant, la Bundeswehr, l'exèrcit alemany, també manifesta la seua preocupació envers l'ampliació dels mètodes de combat. Karl Scheiner, general de brigada de la Führungsakademie der Bundeswehr a Hamburg, veu necessàries unes "normes ètiques" per al camp de batalla d'Internet i creu que és indispensable un cànon internacional per a l'ús de ciberarmes.

Els militars han de replantejar-se la pregunta més important pel que fa a la defensa al ciberespai: Qui és l'atacant? "En la majoria de casos", així d'optimista ho contempla el Manual de Tallinn, és possible identificar la font dels ciberatacs de dades. Tanmateix, això no coincideix amb les experiències de molts experts en seguretat de les TIC.

La típica boira de la ciberguerra es feia evident recentment en el cas de Corea del Sud. En un primer moment, es va dir que Darkseoul procedia del nord, després es van descobrir presumptes indicis que assenyalaven la Xina, Europa i els EUA. Entretant, alguns analistes sospiten de *hackers* nord-coreans motivats pel patriotisme a causa del relativament senzill programari maliciós. Llavors, contra qui ha de llançar Corea del Sud un contraatac?

El cas d'aquest país impulsa l'expert en dret internacional Kreß a concloure que els advocats tindran aviat a les mans un "nou problema sense resoldre": "la guerra sota sospita".

Thomas Darnstädt
Marcel Rosenbach
Gregor Peter Schmitz
© Der Spiegel
Traducció d'Amparo Bonet