CILD Coalizione Italiana Libertà e Diritti civili

TROJAN & CO.

Tecnologie di sorveglianza e controllo delle esportazioni

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 ROME - cild.eu - info@cild.eu

Indice

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 ROME - cild.eu - info@cild.eu

I trojan o spyware sono strumenti potenti e invasivi, usati da anni nell'ombra da molti governi per esigenze investigative. Oltre a questi, che hackerano singoli dispositivi per controllarne le comunicazioni, la sorveglianza di massa di attività digitali viene invece effettuata tramite sistemi di monitoraggio del traffico internet. O attraverso apparecchi come gli Imsi-catcher, usati per localizzare telefoni mobili in una certa area. E se il rischio di abusi è palese in Stati non democratici, lo status e l'impiego di simili tecnologie resta ambiguo anche altrove. Ora l'Italia e l'Europa stanno provando a regolare alcuni di questi strumenti

Trovare il giusto equilibrio è particolarmente complicato, considerato che le regolamentazioni di software e sistemi di telecomunicazioni hanno anche potenziali conseguenze negative per individui e per la ricerca in corso sulla sicurezza dei sistemi informatici.
"Tracciare e controllare le esportazioni è cruciale per l'accountability e la riduzione dei pericoli che derivano dal commercio non controllato di sistemi avanzati di sorveglianza utilizzati da forze di polizia, per sicurezza e spionaggio. Tuttavia, controlli pesanti e non proporzionali su strumenti che accrescono privacy e sicurezza possono essere una minaccia alla stabilità globale e alla protezione dei diritti umani" hanno scritto nove Ong che lavorano nel campo dei diritti digitali lo scorso marzo 2017, in una lettera[1] indirizzata ai partecipanti dell'accordo di Wassenaar, un accordo multilaterale a carattere globale che vede 41 stati firmatari.

Lo scenario: strumenti a lungo invisibili

2001, Stati Uniti Emerge la notizia che l'Fbi starebbe sviluppando un programma informatico per rubare le password usate da sospetti criminali al fine di cifrare i loro messaggi. Il nome di questo strumento è Magic Lantern. Il programma viene inviato all'indagato sotto forma di messaggio email, si installa e inizia a catturare le password digitate dal proprietario del computer. Magic Lantern

[1] "Rights groups demand action on export controls", EDRi, 6 March 2017: https://edri.org/rights-groups-demand-action-export-controls/

sarebbe solo uno degli attrezzi usati dall'agenzia americana per le sue indagini informatiche e punterebbe a superare proprio l'ostacolo della crittografia usata all'epoca soprattutto per scambiarsi email cifrate. "Entrare in un computer è ben diverso dall'intercettare qualcuno", dichiara allora al New Scientist[2] l'ex ministro della Difesa britannico Brian Gladman . "Questo genere di strumenti deve essere fortemente regolato". Ma le regole tarderanno ad arrivare.

A livello tecnico strumenti come Magic Lantern sono definiti trojan horse, cavalli di Troia. Si tratta di un tipo di software che infetta di nascosto un computer per poi compiere una serie di azioni: catturare password o quanto digitato sulla tastiera (keylogger), intercettare conversazioni VoIP o chat, copiare file e persino attivare la videocamera e il microfono per effettuare intercettazioni ambientali.

A partire almeno dall'inizio degli anni Duemila, i trojan horse iniziano ad essere silenziosamente usati da vari Stati per condurre indagini. La motivazione del loro utilizzo è che siano necessari per poter catturare una serie di comunicazioni (all'inizio soprattutto Skype) che iniziano ad essere cifrate, per cui non basta più effettuare una intercettazione telefonica o telematica.

Non sono gli unici strumenti utilizzati dagli Stati per monitorare le comunicazioni digitali. Se i trojan effettuano una intercettazione in profondità, ma mirata su un obiettivo preciso, non mancano altri sistemi di controllo più di massa. Da diversi anni Paesi come gli Stati Uniti e il Canada utilizzano Imsi-catcher, apparecchi che fingendosi un ripetitore telefonico sono usati per registrare, monitorare e localizzare tutti i tipi di telefonini presenti in una certa area, in alcuni casi catturando anche messaggi e voce. Per non parlare dei sistemi di monitoraggio del traffico internet. Alcuni di questi, prodotti da aziende europee come Nokia Siemens Networks o Ultimaco, sono stati rinvenuti in Tunisia, Siria e Iran[3].

---

[2] "FBI's "Trojan horse" program to grab passwords", W. Knight, New Scientist, 21 novembre 2001: https://www.newscientist.com/article/dn1589-fbis-trojan-horse-program-to-grab-passwords/

[3] "Monitoring Centres: Force multipliers from the surveillance industry", E. Omanovic, M. Rice, Privacy International, 29 aprile 2014: https://www.privacyinternational.org/node/439

Il punto è che di questi strumenti – chi li produce, come funzionano, come e quanto vengono usati dalle forze dell'ordine e dalle agenzie di intelligence, e in quali casi – si sa poco e nulla per vari anni. Nel caso dei trojan, in Europa uno dei momenti chiave in cui si inizia a parlarne è l'ottobre 2011, quando il Chaos Computer Club, storica organizzazione di hacker tedeschi, svela l'esistenza di uno spyware impiegato dal governo nazionale per indagini criminali e ribattezzato Bundestrojaner. Il trojan era in grado di registrare conversazioni Skype, scattare screenshot, più varie funzioni aggiuntive che poteva scaricare in distinti moduli. All'incirca nello stesso periodo la Siria di Assad provava a rifornirsi di tecnologie di sorveglianza di massa per monitorare il traffico internet da varie aziende europee, come la tedesca AGT e l'italiana RCS Lab[4]. La francese Amesys, invece, è stata poi accusata – e la causa è ancora in corso – di aver venduto un sistema simile alla Libia di Gheddafi, che lo avrebbe usato contro gli oppositori[5].

La Primavera Araba ha portato alla luce le vendite di queste tecnologie in Paesi autoritari da parte di aziende occidentali. L'uso di questi trojan da parte di governi illiberali, invece, è stato segnalato da una serie di report del Citizen Lab[6], laboratorio dell'Università di Toronto che studia malware e sistemi di sorveglianza. I suoi ricercatori hanno individuato una serie di trojan-spyware, prodotti da aziende occidentali (in particolare dalla anglo-tedesca Gamma Group/FinFisher, dall'italiana Hacking Team, dall'israeliana NSO Group), che sono stati ritrovati sui pc o gli smartphone di attivisti, giornalisti, difensori dei diritti umani in Paesi come il Marocco, l'Etiopia, il Bahrein, gli Emirati Arabi Uniti, il Messico, il Kazakistan, il Sudan e molti altri[7]. Tra i primi casi ad emergere sulla stampa, quello del gruppo di giornalisti marocchini Mamfakinch, critici del governo, che nel 2012 sono stati

[4] "European companies reportedly sold spy tools to help build Syria's surveillance system", I. Ashok, International Business Times, 13 dicembre 2016: http://www.ibtimes.co.uk/european-companies-reportedly-sold-spy-tools-help-build-syrias-surveillance-system-1596221

[5] The Enemies of the Internet, Amesys, Reporters Without Borders (RSF): https://surveillance.rsf.org/en/amesys/

[6] Il sito di Citizen Lab, centro di ricerche dell'Università di Toronto: https://citizenlab.org/

[7] "Cyberwar for sale", M. Schwartz, The New York Times, 4 gennaio 2017: https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html

presi di mira da uno spyware. Secondo Citizen Lab, si sarebbe trattato del software prodotto da un'azienda italiana, Hacking Team.

Nel 2016 è stato reso noto che Ahmed Mansoor, noto attivista per i diritti umani residente negli Emirati Arabi, era stato intercettato per la terza volta da uno spyware installato su uno dei suoi device elettronici. Secondo una ricerca di Citizen Lab, il telefono di Mansoor era stato precedentemente colpito dallo spyware FinSpy (della compagnia Fin Fisher) nel 2011, e da uno di Hacking Team nel 2012. "Una volta infettato dal software, il telefono di Mansoor sarebbe diventato una spia digitale nella sua tasca, in grado di utilizzare anche la videocamera del suo iPhone" scrivono i ricercatori[8].
Il 20 marzo 2017 Mansoor viene arrestato negli Emirati Arabi. Amnesty International chiede il suo immediato rilascio: "Crediamo che Ahmed Mansoor sia attualmente in carcere per la pacifica espressione delle sue convinzioni"[9].
Secondo un altro rapporto di Citizen Lab risalente al 2014, diversi giornalisti etiopi sono stati ripetutamente attaccati da captatori informatici (trojan) di provenienza governantiva, alcuni dei quali sembrano essere stati prodotti da Hacking Team[10].
Secondo l'Ong Bahrain Watch[11], anche il governo del Bahrain è sospettato di aver infettato i computer di alcuni dei principali avvocati, attivisti e politici con lo spyware prodotto da FinFisher.

[8] The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender, B. Marczak, J. Scott-Railton, Citizen Lab, 24 August 2016: https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[9] UAE: Surprise overnight raid leads to arrest of prominent human rights defender, Amnesty International, 20 March 2017: https://www.amnesty.org/en/latest/news/2017/03/uae-surprise-overnight-raid-leads-to-arrest-of-prominent-human-rights-defender/

[10] Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware, B. Marczak, J. Scott-Railton, S. McKune, Citizen Lab, 9 March 2015: https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/

[11] "Bahrain Government Hacked Lawyers and Activists with UK Spyware", F. Desmukh, Bahrain Watch, 7 August 2014: https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

Italia, Paese di sorveglianza

In Italia ci sono diversi produttori di trojan, in particolare la già citata Hacking Team, che ha iniziato a lavorarci dall'inizio degli anni Duemila, vendendoli prima a varie forze di polizia, procure e intelligence italiane, e poi esportandoli e vendendoli ai governi in decine di Paesi. Usati in Italia almeno dal 2004, sarà solo nel 2011 che i maggiori media italiani inizieranno a parlare di questi strumenti in seguito a un'inchiesta giudiziaria[12] dove erano stati usati per indagare su una presunta associazione a delinquere nell'ambito della pubblica amministrazione (la cosiddetta P4).

Nelle carte giudiziarie appaiono però di rado e non sono mai indicati come trojan o spyware o malware. Quando sono usati per indagini criminali sono definiti captatori informatici, agenti intrusori, virus autoinstallanti. Ma il loro status giuridico in Italia resta incerto, e i pochi casi venuti alla luce mostrano che il loro utilizzo – a partire dal tipo di reati – è estremamente variabile e discrezionale.

I trojan emergono di nuovo sui maggiori media italiani nell'estate 2015, quando Hacking Team verrà hackerata[13] e i suoi documenti e mail diffusi online (e poi indicizzati da WikiLeaks). Da allora si è iniziato a discutere in alcuni ambienti della necessità di regolare il loro utilizzo. Organizzazioni come Privacy International hanno più volte affrontato la questione, rivolgendosi direttamente alle autorità italiane, e chiedendo regole più stringenti sulle esportazioni di queste tecnologie.[14]

---

[12] "Un virus per pc inchioda Bisignani lo Stato diventa hacker a fin di bene", A. Sgherza, Repubblica, 22 giugno 2011: http://www.repubblica.it/politica/2011/06/22/news/mail_spia_hacker-18041273/

[13] "Con Hacking Team va su WikiLeaks un pezzo di Stato italiano", C. Frediani, La Stampa, 10 luglio 2015: http://www.lastampa.it/2015/07/10/tecnologia/con-hacking-team-va-su-wikileaks-un-pezzo-di-stato-italiano-mY6laMRZb1g7zJlSx4kOll/pagina.html

[14] "Con Hacking Team va su WikiLeaks un pezzo di Stato italiano", ibid., http://www.lastampa.it/2015/07/10/tecnologia/con-hacking-team-va-su-wikileaks-un-pezzo-di-stato-italiano-mY6laMRZb1g7zJlSx4kOll/pagina.html

Sul tema sono intervenute, nell'aprile 2016, le Sezioni Unite della Corte di Cassazione, che hanno confermato[15] la possibilità di usare i captatori per effettuare intercettazioni ambientali (dette tra presenti) attraverso il microfono dei dispositivi, senza dover indicare preventivamente i luoghi (quindi anche all'interno di abitazioni private, anche se lì non si sta commettendo un crimine) per procedimenti su delitti di criminalità organizzata, inclusa l'associazione per delinquere. La Corte in realtà estendeva ai trojan una deroga al divieto di intercettare in casa (a meno che lì non si stia commettendo un reato), già prevista dal decreto antimafia del 1991. Di fatto però la sua decisione, anche se riguardava nello specifico solo su una delle tante funzioni del trojan, veniva vista da alcuni come un parziale via libera.

Il panorama europeo

L'Unione europea ha iniziato a prestare attenzione al tema dopo che una serie di report internazionali – dalle prime indagini[16] sul campo di Citizen Lab, che risalgono al 2012[17], ai paper di Fidh.org[18] – avevano messo sotto la lente alcuni produttori europei di tecnologia di intrusione e di monitoraggio delle comunicazioni che esportavano in Paesi autoritari e dopo il ritrovamento di malware *made in Europe* sui dispositivi di giornalisti, dissidenti e avvocati in Stati dove le violazioni dei diritti umani sono molto frequenti – come avvenuto in Bahrain, dove attivisti e giornalisti anti-governativi sono stati presi di mira attraverso questi strumenti[19].

---

[15] Corte di Cassazione, Sezioni Unite, Sentenza 1 luglio 2016, n.26889 Ricognizione, Nel Diritto: http://www.neldiritto.it/appgiurisprudenza.asp?id=13067

[16] "For Their Eyes Only: The Commercialization of Digital Spying", M. Marquis-Boire, B. Marczak, C. Guarnieri, J. Scott-Railton, Citizen Lab, 30 aprile 2013: https://citizenlab.org/2013/04/for-their-eyes-only-2/

[17] "From Bahrain with Love: FinFisher's Spy Kit Exposed?", M. Marquis-Boire, Citizen Lab, luglio 2012: https://citizenlab.org/wp-content/uploads/2012/08/09-2012-frombahrainwithlove.pdf

[18] "Surveillance technologies "made in Europe": regulation needed to prevent human rights abuses", C.Perarnaud, A. Klocke, G. Paul, International Federation for Human Rights, dicembre 2014: https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe.pdf

[19] "Bahrain Government Hacked Lawyers and Activists with UK Spyware", F. Desmukh, Bahrain Watch, 7 agosto 2014: https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

O come negli Emirati Arabi Uniti, dove ancora nell'estate 2015 l'attivista per i diritti umani Ahmed Mansoor veniva bersagliato[20] col suo terzo spyware (quest'ultimo apparentemente di origine israeliana).

A partire dal 2014 l'Unione europea ha quindi cercato di porre un freno alla vendita incontrollata di tecnologie di sorveglianza, anche sulla spinta delle pressioni[21] provenienti da CAUSE, la Coalizione Contro l'Export Illegale di Sorveglianza, composta da organizzazioni come Privacy International, Amnesty International, Human Rights Watch, Digitale Gesellschaft, Open Technology Institute e Reporters without Borders[22].

Fino ad allora alcuni di questi prodotti non erano considerati beni di uso duale, vale a dire che possono essere usati sia in ambito civile sia militare (e che, come tali richiedono controlli più stretti). Possono essere sostanze chimiche, tossine, equipaggiamenti o componenti per armi, e nel caso specifico anche alcune tecnologie informatiche. Nello specifico il Regolamento Ue N°428/2009[23] sull'uso duale (EU Regulation (EC) N°428/2009) lasciava agli Stati Membri l'implementazione a livello nazionale, con una conseguente frammentazione legale. Nell'articolo 8 del Regolamento, gli Stati Membri potevano ad esempio imporre la richiesta di un'autorizzazione per l'export anche per quei prodotti non inclusi nella lista a uso duale per ragioni di sicurezza pubblica e per considerazioni sui diritti umani. Queste clausole "catch-all" sono state però usate raramente dagli Stati Membri e la loro implementazione era considerata troppo discrezionale.

---

[20] "iPhone vulnerabile a spyware, le falle scoperte da attivista sotto attacco", C. Frediani, La Stampa, 26 agosto 2016: http://www.lastampa.it/2016/08/26/tecnologia/news/iphone-vulnerabile-a-spyware-le-falle-scoperte-da-attivista-sotto-attacco-5zVY7rhgLFDLUVnwSUtcxH/pagina.html

[21] "A critical opportunity: bringing surveillance technologies within the EU Dual-Use Regulation", Steering Committee of the Coalition Against Unlawful Surveillance Exports (CAUSE), giugno 2015: https://www.privacyinternational.org/sites/default/files/CAUSE_8.pdf

[22] "Surveillance technologies "made in Europe": regulation needed to prevent human rights abuses", ibid., https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe.pdf

[23] "REGOLAMENTO (CE) N. 428/2009 del Consiglio del 5 maggio 2009 che istituisce un regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso", 5 maggio 2009: http://www.sviluppoeconomico.gov.it/images/stories/commercio_internazionale/embarghi_dualuse/reg428_09.pdf

Il 22 ottobre 2014 la Commissione europea ha dunque annunciato un aggiornamento della lista di beni di uso duale, in linea anche con un altro accordo internazionale volontario di regolamentazione dell'export di armi e tecnologie di uso duale (il Wassenaar Arrangement[24]), e per riflettere le crescenti preoccupazioni sull'uso delle tecnologie di sorveglianza e di altri strumenti cyber per violare i diritti umani. La lista aggiornata introduce controlli per nuove categorie come i software di intrusione (spyware) e gli apparati di sorveglianza IP, che permettono di monitorare il traffico internet. Le nuove disposizioni sono entrate in vigore a fine 2014.

È importante specificare però che l'accordo di Wassenaar non tocca in modo specifico la componente tecnica del trojan ma l'infrastruttura di comando e controllo usata per generare, installare e "istruire" il trojan, vale a dire il software installato su un server governativo per inviare il trojan a uno specifico obiettivo.

Tuttavia, anche questo aggiornamento non sembra aver impedito l'esportazione di queste tecnologie in Stati non democratici e con gravi problemi di violazione dei diritti umani. Una inchiesta internazionale – Security for Sale[25] – condotta da una rete di giornalisti europei e pubblicata nel 2017 ha mostrato che negli ultimi tre anni gli Stati membri dell'Ue hanno permesso l'export di tecnologia di cyber-sorveglianza almeno 317 volte. E che le richieste che sono state respinte sono state solo 14. Quasi un terzo delle licenze erano dirette a Paesi definiti "non liberi" dall'organizzazione di monitoraggio dei diritti umani nel mondo Freedom House[26]. Mentre il 52 per cento era diretto a Paesi classificati dalla stessa organizzazione come "parzialmente liberi", quali la Turchia. Tuttavia i numeri conteggiati

[24] The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies: http://www.wassenaar.org/

[25] "Security for Sale The price we pay to protect Europeans", The Correspondent, 7 marzo 2017: https://thecorrespondent.com/10221/security-for-sale-the-price-we-pay-to-protect-europeans/497732037-a3c8cc9e

[26] "Populists and Autocrats: The Dual Threat to Global Democracy", Freedom House, 2017: https://freedomhouse.org/report/freedom-world/freedom-world-2017

dall'inchiesta sono parziali. Dei 28 Stati membri, 11 si sono rifiutati di dare informazioni sulle esportazioni. Tra questi Francia e Italia, "sede entrambi di alcuni dei maggiori business globali di tecnologie di sorveglianza", come riferisce Security for Sale.

La Commissione europea si è resa conto della necessità di rendere le regole più chiare, cogenti e uniformi e, come vedremo, ha elaborato una nuova proposta in questa direzione, che aumenta le tecnologie da porre sotto controllo e aumenta l'enfasi sulla necessità di considerare i diritti umani nel rilascio delle licenze.

Focus: le esportazioni italiane

All'interno dell'industria globale della sorveglianza, l'Italia si è conquistata negli ultimi anni un posto di primo piano, dopo Stati Uniti, Gran Bretagna, Francia, Germania, Israele. Sono infatti circa 18 le aziende italiane del settore, secondo una stima di Privacy International[27], secondo la quale l'Italia, accanto a una consistente industria della difesa, avrebbe sviluppato negli anni anche quella della sorveglianza – in parte trainata dall'uso interno di questi strumenti, in funzione di lotta al crimine, da parte delle forze dell'ordine.

Negli anni le due aziende tricolori che più sono finite sotto la lente internazionale, anche in virtù delle loro esportazioni, sono state Hacking Team e Area. Hacking Team, il maggior produttore italiano di spyware, ha esportato per anni indisturbata, inclusi Paesi come la Russia[28] e il Sudan[29]. All'inizio del 2015, quando anche i trojan (software di intrusione) sono entrati nella lista europea di prodotti di uso duale,

---

[27] "iPhone vulnerabile a spyware, le falle scoperte da attivista sotto attacco", ibid.: http://www.lastampa.it/2016/08/26/tecnologia/news/iphone-vulnerabile-a-spyware-le-falle-scoperte-da-attivista-sotto-attacco-5zVY7rhgLFDLUVnwSUtcxH/pagina.html

[28] "Intelligence o panini? La doppia vita di Hacking Team", C. Frediani, La Stampa, 14 luglio 2015: http://www.lastampa.it/2015/07/14/tecnologia/intelligence-o-panini-la-doppia-vita-di-hacking-team-AuCZyCJquh8XyS68bhaYaP/pagina.html

[29] "Così il Sudan ha messo in crisi Hacking Team", C. Frediani, La Stampa, 9 luglio 2015: http://www.lastampa.it/2015/07/09/tecnologia/cos-il-sudan-ha-messo-in-crisi-hacking-team-6oxJBVvCJUvCshTr1uSqWK/pagina.html

richiedendo quindi una autorizzazione per l'esportazione, Hacking Team, aveva ottenuto dal Ministero dello Sviluppo Economico (MISE) un'autorizzazione globale[30] all'esportazione, che di fatto era un via libera generalizzato. Tale licenza è stata però revocata[31] nell'aprile 2016, forse una reazione tardiva ai precedenti report di Citizen Lab o più probabilmente all'attenzione mediatica seguita all'omicidio del ricercatore italiano Giulio Regeni in Egitto. Da allora l'azienda dovrà ottenere autorizzazioni specifiche individuali per i Paesi extraeuropei.

L'incertezza regolatoria delle autorità nazionali è testimoniata anche da un'altra vicenda. Nel giugno 2016 il Ministero dello Sviluppo Economico (Mise) concede all'azienda italiana Area spa, di Vizzola Ticino, una autorizzazione specifica per l'esportazione di una tecnologia di sorveglianza del traffico internet in Egitto. Il cliente finale è il Technical Research Department (TRD), del Consiglio nazionale di difesa, già emerso in precedenti report di Privacy International, un'unità priva di controlli dell'intelligence egiziana, che per anni ha acquistato molteplici tecnologie di sorveglianze da aziende europee.Tuttavia nel gennaio 2017, dopo la pubblicazione di una lettera al Mise scritta da Cild insieme a Privacy International e Hermes Center for Transparency and Digital Human Rights, in cui si chiedeva conto dell'autorizzazione concessa ad Area, il ministero risponde con una nota[32] specificando che già da luglio era stato avviato il provvedimento di riesame in autotutela dell'autorizzazione concessa ad Area e che si sarebbe proceduto alla revoca definitiva alla successiva riunione dell'apposito Comitato consultivo. Inoltre la stessa Area, nel dicembre 2016, era stata sottoposta[33] a una perquisizione e a un provvedimento

[30] "Dual use - Prodotti tecnologici a duplice uso", Ministero dello Sviluppo Economico (ultima consultazione: 18 marzo 2017): http://www.sviluppoeconomico.gov.it/index.php/it/component/content/article?id=2022475

[31] "Hacking Team, revocata l'autorizzazione globale all'export del software spia: stop anche per l'Egitto dopo il caso Regeni", A. Pitoni, Il Fatto Quotidiano, 6 aprile 2016: http://www.ilfattoquotidiano.it/2016/04/06/hacking-team-revocata-lautorizzazione-globale-allexport-del-software-spia-stop-anche-per-legitto-dopo-il-caso-regeni/2610721/

[32] "Il MISE risponde alla nostra lettera: la licenza di Area spa sarà revocata", CILD, 24 gennaio 2017: http://www.cilditalia.org/blog/il-mise-risponde-alla-nostra-lettera-la-licenza-di-area-spa-sara-revocata

[33] "Esportava un sistema di monitoraggio internet ai servizi siriani": come è nata l'ipotesi di reato che ha travolto Area", C. Frediani, La Stampa, 5 dicembre 2016: http://www.lastampa.it/2016/12/05/italia/cronache/esportava-un-sistema-di-monitoraggio-internet-ai-servizi-siriani-come-nata-lipotesi-di-reato-che-ha-travolto-area-qVSJ1zMIDGoODZfH4jSRMK/pagina.html

di sequestro preventivo del valore di 7,7 milioni di euro nell'ambito di un'indagine che riguardava la presunta violazione delle leggi sulle esportazioni per le tecnologie di uso duale in Siria, fra 2010 e 2011. L'autorizzazione è sospesa in attesa di una decisione finale che dovrebbe arrivare a seguito di un incontro previsto per il 27 giugno 2017[34].

Nell'aprile 2017 Al-Jazeera ha trasmesso e pubblicato online "Spy Merchants"[35], un documentario che mostra, tramite indagine sotto copertura, diverse aziende italiane e internazionali disponibili a esportare strumenti di sorveglianza senza particolari preoccupazioni per eventuali violazioni dei diritti umani. CILD, Privacy International e Hermes Center for Transparency and Digital Human Rights hanno scritto nuovamente al Ministero dello Sviluppo Economico chiedendo di pubblicare informazioni relative alle licenze e sostenendo l'importanza di una maggiore trasparenza e responsabilità per il settore industriale in questione[36].
Ad oggi tra i Paesi verso i quali l'Europa ha adottato[37] restrizioni sulle esportazioni di tecnologie a duplice uso ci sono, oltre alla Siria, l'Iran, la Corea del Nord, la Russia, l'Ucraina e la Crimea.

Verso un nuovo quadro regolatorio europeo?

Come già accennato sopra, a fine 2016 la Commissione europea ha proposto[38] di rafforzare i controlli sulle esportazioni di beni di uso duale.

---

[34] Risposta scritta pubblicata Mercoledì 12 aprile 2017 nell'allegato al bollettino in Commissione X (Attività produttive) 5-11055, 12 April 2017: http://aic.camera.it/aic/scheda.html?numero=5/11055&ramo=CAMERA&leg=17

[35] "Spy Merchants", Al Jazeera, 10 April 2017: http://www.aljazeera.com/indepth/features/2017/04/spy-merchants-electronic-surveillance-170409100231959.html

[36] Esportazioni di cybersorveglianza, l'Italia torna nel mirino, C. Frediani, La Stampa, 11 April 2017: http://www.lastampa.it/2017/04/11/esteri/esportazioni-di-cybersorveglianza-italia-torna-nel-mirino-OVCGrUFyFqxyAtE5pQxDaJ/pagina.html

[37] "Dual use - Prodotti tecnologici a duplice uso", Ministero dello Sviluppo Economico (ultima consultazione: 18 marzo 2017): http://www.sviluppoeconomico.gov.it/index.php/it/component/content/article?id=2022475

[38] "Commission proposes to modernise and strengthen controls on exports of dual-use items", Commissione Europea, 28 settembre 2016: http://europa.eu/rapid/press-release_IP-16-3190_en.htm

In particolare si fa riferimento alla dimensione della "sicurezza umana" nel valutare le autorizzazioni per evitare violazioni dei diritti attraverso tecnologie di cybersorveglianza. La proposta include anche una armonizzazione delle regole e delle procedure adottate nei vari Stati membri.

La lista delle tecnologie che dovrebbero essere coperte dal nuovo regolamento include:

- sistemi di intercettazioni delle telecomunicazioni mobili;
- software di intrusione (trojan); centri di monitoraggio;
- sistemi di data-retention e intercettazione legale (lawful interception);
- tecnologie di informatica forense

Le prime tre tecnologie erano già state aggiunte alla lista di controllo delle tecnologie a uso duale dell'intesa di Wassenaar e nel dicembre 2014 erano stati aggiunti alla lista Ue. L'attuale proposta[39] è oggetto di valutazione[40] proprio in questi mesi: il Parlamento europeo ha iniziato a discuterla il 28 febbraio 2017.

Nel marzo 2017 alcune organizzazioni internazionali che si occupano di diritti umani hanno scritto una lettera[41] a tutti i firmatari dell'accordo di Wassenaar chiedendo loro di aggiornare le disposizioni nell'ottica di una maggiore protezione dei diritti umani, mostrando preoccupazione circa la genericità dell'attuale regolamentazione, anche per il suo potenziale impatto sulla possibilità di fare ricerca sulla sicurezza informatica.

---

[39] "Review of dual-use export controls - briefing", Parlamento Europeo, 30 gennaio 2017: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf

[40] "Review Of Dual-Use Export Controls [EU Legislation In Progress]", B. Immnkamp, European Parliamentary Research Service Blog, 11 gennaio 2017: https://epthinktank.eu/2017/01/11/review-of-dual-use-export-controls-eu-legislation-in-progress/

[41] "Rights Organisations Urge Export Control Body to Change Control List", Privacy International, 6 March 2017: https://medium.com/privacy-international/rights-organisations-urge-export-control-body-to-change-control-list-997c209c6aa4

TROJAN & CO

Tecnologie di sorveglianza
in Europa e in Italia

REALIZZATO DA

CILD

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 ROME - cild.eu - info@cild.eu