PAPER
APRILE 2017

IL CASO 'HACKING TEAM': QUIS CUSTODIET IPSOS CUSTODES?

PROBLEMATICHE E SFIDE PER UNA PIÙ EFFICIENTE PARTNERSHIP TRA SETTORE PRIVATO E AGENZIE D'INTELLIGENCE NELLA CYBERSECURITY

FILIPPO PIEROZZI

UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

IL CASO 'HACKING TEAM': QUIS CUSTODIET IPSOS CUSTODES?

PROBLEMATICHE E SFIDE PER UNA PIÙ EFFICIENTE PARTNERSHIP TRA SETTORE PRIVATO E AGENZIE D'INTELLIGENCE NELLA CYBERSECURITY

Filippo Pierozzi

UNIVERSITÀ DEGLI STUDI FIRENZE

Paper

Aprile 2017

IL CASO 'HACKING TEAM': QUIS CUSTODIET IPSOS CUSTODES?

-

Problematiche e sfide per una più efficiente partnership tra settore privato e agenzie d'intelligence nella cybersecurity

1. Hacking the hackers

Come ha potuto l'attacco informatico operato ai danni di un'impresa milanese (HT Srl) produttrice del malware Remote Control System (RCS) Galileo, trasformarsi in un caso critico tanto a livello nazionale, nella misura in cui l'ex direttore del DIS, Giampiero Massolo, ha avuto modo di riferire il caso al COPASIR[1] evidenziando i rischi sistemici per l'intelligence italiana, quanto a livello europeo[2] e internazionale[3]?

Per capire come un singolo attacco contro un operatore privato abbia potuto causare così vaste ricadute per la sicurezza nazionale è opportuno procedere ad un'analisi dei nuovi scenari apertisi con la collaborazione dei servizi di intelligence con aziende private di *cyber security*. Implicazioni che concernono tanto il profilo della responsabilità giuridica dei diversi soggetti quanto quello della loro vulnerabilità ed esposizione alle minacce informatiche[4].

[1] Comitato Parlamentare per la Sicurezza della Repubblica, Relazione annuale dell'attività svolta, (dal 1 Ottobre 2014 al 31 dicembre 2015), Trasmessa alle Presidenze delle Camere il 17 febbraio 2016. XVII Legislatura – Disegni di Legge e Relazioni - Documenti – Doc. XXXIV, N. 3

[2] La parlamentare del gruppo ALDE Marietje Schaake ha presentato un'interrogazione nella quale si sollecita un'indagine da parte dell'Italia su presunte violazioni delle sanzioni compiute da Hacking Team vendendo il malware al governo sudanese nel 2012 e alla Kvant, controllata dal Governo russo nel marzo 2015. http://www.marietjeschaake.eu/2015/07/written-questions-on-theitalian-company-hacking-teams-potential-violations-of-eu-sanctions

[3] UN Security Council (2016), Letter dated 22 September 2016 from the Chair of the Security Council Committee established pursuant to resolution 1591 (2005) concerning the Sudan addressed to the President of the Security Council

[4] Per una panoramica generale si rimanda a: Carr, M. (2016). Public–private partnerships in national cyber!" security strategies. *International Affairs*, 92(1), 43-62.

L'assenza di una cornice legale ben definita in merito alla stipula di contratti tra operatori privati che forniscono strumenti operativi e supporto informatico ed il Governo[5] fa sì che possa ingenerarsi incertezza sulle obbligazioni dei *contractors* e sulla loro responsabilità, che dovrà essere commisurata in modo ragionevole all'utilizzo che il sistema di intelligence nazionale ne fa[6].

Nella notte del 5 luglio 2015 un hacker, noto come Phineas Fisher che già si era reso responsabile della diffusione di oltre 40GB di materiale riservato dell'azienda anglo-tedesca Gamma Group (produttrice dello spyware FinFisher), entra in possesso dell'account Twitter di Hacking Team e rende nota la pubblicazione di circa 400GB di dati sensibili sottratti dai server di Hacking Team[7]. L'operazione evidenzia le intrinseche vulnerabilità che i malware utilizzati dalle agenzie di intelligence presentano[8].

Il RCS Galileo è un pacchetto offensivo di alto profilo in grado di infettare computer e dispositivi portatili quali tablet e smartphone: l'operazione avviene attraverso un malware che viene attivato mediante l'apertura di una mail o lo scaricamento di un file; a quel punto interviene lo spyware che invia screenshot, mail, chat o conversazioni al server che lo sta controllando da remoto[9]. Un sistema sofisticato, ma con vulnerabilità tali da permettere al gruppo di hacker Phineas Fisher di accedere – mediante un *hack* di durata relativamente breve - ai dati di Hacking Team mediante la combinazione di un exploit (un codice che permette di sfruttare una data vulnerabilità) e di una backdoor per proteggere il meccanismo di penetrazione[10].

---

[5] Ricordiamo come la legge n. 127 del 3 agosto 2007 all'art. 1 recita "Al Presidente del Consiglio dei ministri sono attribuiti, in via esclusiva: a) l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento."

[6] Nichols R. et al. (2014), "Cybersecurity for Government Contractors", *Briefing papers*, Westlaw, no. 14-15, apr. 2014, p. 14

[7] "Since we have nothing to hide, we're publishing all our e-mails, files, and source code", Twitter, riportato da Bicchierai L., "Spytech Company Hacking Team Gets Hacked", *Motherboard*, 5 luglio 2015.

[8] Si veda e.g. Marquis-Boire, M., Marschalek, M., & Guarnieri, C. (2015). Big Game Hunting: The Peculiarities in Nation State Malware Research. *Proc. of Black Hat USA*.

[9] Frediani C. et al., (2015) *Attacco ai pirati. Tutti i segreti del datagate italiano*, La Stampa, Torino p. 11.

[10] Come spiegato il 15 aprile 2016 con un tweet dal profilo 'Hack!Back!' dagli stessi autori https://twitter.com/GammaGroupPR/status/721085460932636673

Hacking Team era stata in passato oggetto di critiche dopo che il laboratorio antisorveglianza *Citizen Lab* dell'Università di Toronto aveva pubblicato un rapporto che collegava gli spyware italiani ad una serie di violazioni dei diritti umani perpetrate da parte di regimi autoritari[11].

Un elemento fortemente innovativo introdotto dal CEO di HT David Vincenzetti, che conferiva un vantaggio concorrenziale all'azienda milanese, è stato l'affiancamento a programmi altamente sofisticati di attacco con una procedura semplificata che poteva essere utilizzata, grazie a due settimane di corso, anche da personale non esperto di informatica[12].

Il meccanismo era tale che Hacking Team vendeva la piattaforma, rilasciava aggiornamenti periodici dei database degli exploit e insegnava ad utilizzarli[13]: tale escamotage faceva sì che l'azienda potesse dirsi estranea a qualunque tipo di violazione commessa per mezzo del RCS Galileo.

Marquis-Boire, membro del Citizen Lab, identifica 21 Paesi non democratici ai quali lo spyware sarebbe stato venduto e sottolinea come "la dirigenza [di HT] fosse incurante dei diritti umani e del diritto alla privacy i quali venivano visti da Vincenzetti come ostacoli ai loro interessi commerciali"[14]. Se l'acquisto dei prodotti di HT da parte di regimi autoritari[15] quali Bahrein, Egitto, Kazakistan, Nigeria, Uzbekistan, Marocco e le presunte violazioni delle sanzioni disposte dalle Nazioni Unite nei confronti del Sudan[16] ci aiuta a realizzare la vastità delle implicazioni internazionali del caso[17], ancora non

[11] Citizen Lab, (2014) "Mapping Hacking Team's "Untraceable" Spyware", *Munk School of Global Affairs*, Toronto; si veda anche Benedek, W. & Ketteman, M.C. (2014) Freedom of expression and the Internet, *Council of Europe*

[12] Frediani C. et al., (2015) "Attacco ai pirati. Tutti i segreti del datagate italiano".

[13] Hacking Team, http://www.hackingteam.it/policy.html

[14] Kushner D., "Fear This Man", *Foreign Policy*, 26 aprile 2016.

[15] "Dai documenti segreti resi pubblici a seguito dell'attacco, emerge che la società milanese abbia fornito e continui a fornire software "spia" per la sorveglianza informatica a diversi Paesi tra i quali figurano anche i cosiddetti Stati "canaglia", regimi autoritari alcuni dei quali sottoposti a misure di embargo sui prodotti e le tecnologie dual use". Senato della Repubblica (2015), XVII Legislatura, Fascicolo Iter DDL 2 1556, Seduta n. 497 del 04/08/2015, p. 246.

[16] Cfr. Nota 3.

[17] Alle denunce di *Reporters Without Borders* che aveva inserito Hacking Team tra i 'nemici della rete' (http://surveillance.rsf.org/en/hacking-team/) si aggiungono le recenti pubblicazioni in merito alla capillare diffusione del sistema Galileo in America Centrale e in America Latina, come dettagliatamente riportato da *Derechos Digitales* nel volume "Hacking Team: malware para la vigilancia en América Latina" di Perez de Acha G., marzo 2016.

abbiamo analizzato le ricadute che esso potrebbe avere sul sistema di intelligence italiano.

Tuttavia, vale la pena sottolineare come il piano internazionale e quello della regolamentazione a livello nazionale siano fortemente correlati, come emerge dalla mutata posizione del Governo in merito alla concessione di un'autorizzazione "globale individuale" ad HT per l'esportazione dei propri prodotti *dual use technology*[18] dapprima rilasciata dal Ministero dello sviluppo il 3 marzo 2015 (previo parere del Comitato consultivo ex art. 11 d. lgs. 96/2003), poi ritirata il 31 marzo 2016 – con ogni probabilità - anche a seguito delle forti pressioni tanto politiche e dell'opinione pubblica[19] che collegavano la vendita del RCS Galileo ai servizi segreti egiziani all'omicidio del ricercatore italiano Giulio Regeni[20].

Sotto il profilo del diritto interno, l'ipotesi di reato contestata è quella di accesso abusivo a sistema informatico, sancita dall'art. 615-ter del Codice Penale: la Procura di Milano ha aperto un'inchiesta coordinata dal pool competente per i reati informatici coordinato da Maurizio Romanelli[21]. Le implicazioni per la sicurezza nazionale, tuttavia, vanno ben oltre il mero profilo penalistico della responsabilità degli attaccanti.

Dal 2004, infatti, Hacking Team è uno dei maggiori fornitori di sistemi di cyber-intelligence a clienti istituzionali italiani ed in breve tempo l'azienda ha avuto modo di affermarsi come "monopolista per le forze dell'ordine del nostro Paese."[22]

La stretta correlazione tra enti istituzionali italiani e l'agenzia milanese non si esauriva in una collaborazione di carattere

[18] Sulle specificità di tali beni, regolati dal Regolamento UE No. 428/2009 si dirà in seguito.
[19] Visibilità ai rapporti di Hacking Team con i servizi egiziani è stata data dalla campagna di Amnesty International "Verità per Giulio" e da alcuni articoli comparsi su La Stampa, in primis "L'ombra di Hacking Team sull'omicidio Regeni" del 7 aprile 2016.
[20] La deputata di Scelta civica (Sc) Adriana Galgano ha presentato un'interrogazione parlamentare in data 20 aprile 2016 concernente le "*Questioni relative ad eventuali rapporti commerciali della società Hacking Team con il servizio di intelligence egiziano" rispondendo alla quale il sottosegretario del MISE Ivan Scalfarotto ha avuto modo di sottolineare come "il Ministero recentemente in relazione alle mutate condizioni politiche, ha comunicato all'impresa Hacking Team che al posto della autorizzazione globale individuale – che è stata, pertanto, revocata – dovrà ora, nel qual caso intendesse esportare i propri prodotti duali in Paesi terzi alla UE*."
Documenti Camera, Commissione X, 20 aprile 2016, Allegato No. 2, p. 234.
[21] Cfr. Nota 1, Comitato Parlamentare per la Sicurezza della Repubblica (2016), p. 24.
[22] Frediani C. et al., (2015) "Attacco ai pirati. Tutti i segreti del datagate italiano".

meramente tecnico[23]: dai documenti pubblicati su Wikileaks, infatti, emerge come Hacking Team abbia operato forti pressioni sul MISE così da eludere l'applicazione della 'catch all clause', che avrebbe costretto la società milanese a una sorta di autorizzazione preventiva per esportare i suoi prodotti. Dai documenti divulgati emerge come lo stesso CEO Vincenzetti ebbe modo di scrivere "stiamo facendo la massima pressione possibile e si stanno interessando alla cosa AISI, ROS, Polizia e AISE", per poi felicitarsi della concessione ottenuta (una deroga temporanea dall'applicazione della 'clausola onnicomprensiva' che avrebbe *ad interim* concesso una più libera attività di esportazioni) affermando che "[ormai] abbiamo coinvolto e sensibilizzato talmente tante parti che non sappiamo con esattezza da dove sono arrivate le maggiori pressioni al MISE"[24].
Il principale rischio sistemico dovuto alla penetrazione del sistema Galileo – largamente utilizzato dalle varie componenti delle forze dell'ordine e dell'intelligence italiano – è quello legato al proliferare di software-spia '*black*' ovvero creati a partire dalla base del codice sorgente di Galileo[25]: con la liberazione del codice si dà l'opportunità a chiunque di replicare, migliorare ed installare una delle più sofisticate armi digitali in circolazione[26].

2. Implicazioni per la Partnership-Pubblico Privato

La moltiplicazione delle minacce nel dominio cibernetico, che interessano in misura sempre maggiore gli Stati[27], fa sì che la compartecipazione del settore pubblico e privato divenga condizione irrinunciabile all'articolazione di qualunque approccio di cyber security.

---

[23] I documenti ufficiali sono pubblicati nell'articolo "Hacking Team: tra i clienti dei tecno-spioni di Milano anche servizi segreti" a firma di Massimo Sideri pubblicato sul *Corriere della Sera* il 15 luglio 2015.
[24] Wikileaks, mail da d.vincenzetti@hackingteam.com 1-5 novembre 2014, disponibile a https://wikileaks.org/hackingteam/emails/emailid/178399
[25] Come spiegato ad ANSA dall'hacker Raoul Chiesa "Hacking Team: utenti a rischio, 5 consigli per difendersi".
[26] È lo stesso sito istituzionale di Hacking Team a dichiarare, all'indomani dell'accaduto di aver perso il controllo sul malware da loro creato: disponibile a http://www.hackingteam.com/index.php/about-us
[27] Sistema di Informazione per la sicurezza della Repubblica, (2016) Allegato alla Relazione sulla politica dell'informazione per la sicurezza 2015, 22-24: in Italia nel 2015 il 69% dei target di attacchi era costituito da soggetti pubblici.

L'Unione Europea sin dal 2009 ha lanciato la *European Public-Private Partnership for Resilience*[28] mirata a promuovere la cooperazione tra privato e pubblico, allineandosi con quanto previsto dalle strategie di sicurezza cibernetica statunitensi, recentemente integrate dall'*Executive order 13636* che - alla sezione 4 "*cybersecurity information sharing*"- pone come centrale l'esigenza di scambiare in maniera efficace e rapida le informazioni sulle minacce cibernetiche emergenti con il settore privato[29].

Un'efficiente cooperazione tra pubblico e privato dovrebbe, tuttavia, conformarsi ad alcuni requisiti minimi quali il mantenimento di una bassa complessità strutturale che possa creare relazioni di fiducia tra i soggetti coinvolti e la creazione di meccanismi di controllo e rendicontabilità attraverso i quali l'implementazione possa essere costantemente controllata[30].

Se negli Stati Uniti il meccanismo delle cd. *revolving doors* ha creato un sistema privato di cybersecurity distinto e parallelo a quello ufficiale[31] - a differenza di quest'ultimo immune di qualunque forma di controllo - in Italia la maggiore problematicità concerne il "grave ritardo culturale e politico" nell'affrontare le nuove sfide alla responsabilità politica dello stato moderno in termini di strutture amministrative, processi decisionali, diritti civili, sicurezza e servizi al cittadino, inoltre, non favorisce la causa della partnership pubblico-privato la "molteplicità delle autorità politiche deputate [che] è in palese contrasto con la natura stessa della rivoluzione digitale[32]. Questa, infatti, per essere efficace, richiede di rompere i compartimenti stagni, le isole di potere e impone una visione trasversale e unitaria che consenta di agire con velocità, con una catena di comando chiara e [...] coerente con una visione a lungo termine dell'intero sistema Paese"[33].

La fuga di notizie ha fatto, inoltre, emergere un'estesa rete di stretti rapporti personali – al limite della collusione – tra alti esponenti

[28] Disponibile a European Union Agency for Network and Information Security (ENISA) http://www.enisa.europa.eu/activities/Resilience-andCIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

[29] Cit in. Mele S., (2014) "La cooperazione tra pubblico e privato nella cyber-security", p. 11.

[30] Ibid. e Clusit, (2016), *Rapporto 2015 sulla sicurezza ICT in Italia*

[31] Shorrock T., "How Private Contractors Have Created a Shadow NSA", *The Nation*, 27 maggio 2015.

[32] Cyber Security National Lab (2015), *Il Futuro della Cyber Security in Italia*, ottobre 2015, pp. 14-15.

[33] Ibid.

ministeriali e la dirigenza di Hacking Team: intesa testimoniata dall'intercessione di un alto esponente della direzione generale del MISE per facilitare l'ottenimento delle licenze per l'esportazione per l'azienda di Vincenzetti[34].

Un ulteriore elemento di difficoltà è costituito dalla natura ibrida di Hacking Team: può l'azienda essere considerata come un tassello del sistema nazionale o deve configurarsi solo e soltanto come un'impresa privata?

Nell'ultima direzione sembra andare la descrizione che l'impresa stessa fornisce, presentandosi come "*an active player in the IT security market and it offers security tools and intelligence instruments for governmental institutions*."[35] e verso la caratterizzazione del team di hacker di via Moscova come un'impresa 'business only' sembra andare la spregiudicata politica di vendite verso disparati interlocutori istituzionali internazionali.

Ciononostante dalla corrispondenza emerge una forte connotazione nazionalistica di Hacking Team: Vincenzetti ammonisce il generale Antonello Vitale dell'AISE che "sara' estremamente difficile, una volta che l'azienda non esisterà più, ricreare un gruppo R&D in grado di aiutare i nostri clienti — VOI in primis — a contrastare le minacce crescenti provenienti dalla Russia o dall'ISIS o da altro."[36]

L'apparente bipolarismo identitario di Hacking Team non esaurisce gli spunti di interesse nell'aneddotica di carattere giornalistico[37], ma comporta implicazioni legali e politiche sostanziali, tanto da essere citato in apertura della proposta di legge sull' "Istituzione del sistema nazionale di sicurezza cibernetica" presentata alla Camera il 19 gennaio 2016 dove si ricorda che la penetrazione del software RCS Galileo comporta un grave rischio in quanto ad essere stato violato è stato "uno dei principali strumenti di intelligence a disposizione delle Forze di polizia e dei servizi segreti italiani"[38].

---

[34] 10 Ottobre 2014: https://wikileaks.org/hackingteam/emails/

[35] www.hackingteam.it, dove, in apparente contraddizione con quanto emerso, HT precisa nella Customer Policy "we do not sell products to individuals or private businesses. We do not sell products to governments or to countries blacklisted by the U.S., E.U., U.N., NATO or ASEAN."

[36] Wikileaks, 11 novembre 2014 disponibile a https://wikileaks.org/hackingteam/emails/emailid/166703

[37] Il tema è lungamente discusso in Frediani C. et al., (2015) "Attacco ai pirati. Tutti i segreti del datagate italiano".

[38] Camera dei deputati, Proposta di legge no. 3544, *Istituzione del sistema nazionale di sicurezza cibernetica*, 19 gennaio 2016, p. 2.

I soggetti ascoltati dal Comitato Parlamentare per la Sicurezza per la Repubblica sono stati tutti coloro che "hanno avuto contatti con la Hacking Team e hanno utilizzato il software Galileo per le loro attività investigative: [...] il capo della polizia, il comandante generale della Guardia di finanza e il comandante generale dei Carabinieri, e successivamente il Ministro della giustizia, on. Orlando, i vertici del SIS, Autorità delegata, direttore del DIS e direttore dell'AISE, vertici delle Forze dell'ordine".[39]

Tale quadro mostra chiaramente come la Hacking Team fosse *de facto* divenuta un tassello fondamentale del sistema di intelligence italiano del quale l'attacco evidenzia la persistente presenza di vulnerabilità sotto il profilo della cyber security.

Gli indicatori statistici che segnalano una particolare esposizione ad attacchi informatici operati con malware sono noti: il Microsoft Security Intelligence Report nel 2014 riportava per l'Italia un tasso di esposizione a malware superiore alla media mondiale[40] e il nostro Paese si posizionava ai primi posti del mondo per la diffusione di malware[41]. L'attenzione alla collaborazione con il settore privato nella cyber security è stata incrementalmente potenziata a partire dal *Piano Nazionale per la Protezione Cibernetica e la sicurezza Informatica* del dicembre 2013 che prevede tale partnership nella gran parte dei suoi 'obiettivi operativi', dallo sviluppo di relazioni fiduciarie, alla creazione di tavoli istituzionali, dal rafforzamento nella condivisione delle informazioni, all'individuazione comune di requisiti minimi di difesa cibernetica[42].

Mancavano, tuttavia, elementi cardine che potessero garantire un'attenuazione dei danni - economici, politici e in termini di sicurezza – nel caso di attacchi o problemi ai fornitori degli *spyware* utilizzati, come verificatosi con l'attacco ad Hacking Team.

La mancanza di un unico organo referente del settore pubblico verso i privati rende più difficile il coordinamento tra le varie componenti, rallentando talvolta la velocità del flusso di informazioni tra il centro politico e la componente operativa che opera la partnership con il

[39] Senato della Repubblica e Camera dei Deputati, Comitato Parlamentare per la Sicurezza della Repubblica, *Relazione annuale 2015 trasmessa alle Presidenze delle Camere il 17 febbraio 2016*, pp. 25 ss.
[40] Cyber Security National Lab (2015), Il Futuro della Cyber Security in Italia, ottobre 2015, p. 30.
[41] http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
[42] Presidenza del Consiglio dei Ministri, *Piano Nazionale per la Protezione Cibernetica e la sicurezza Informatica*, dicembre 2013.

settore privato[43]. Allo stesso modo la mancanza di trasparenza negli accordi di cooperazione – per i quali mancano specifiche normative- ha fatto sì che l'interlocuzione tra il settore privato e quello pubblico fosse lasciato all'arbitrio delle persone coinvolte che spesso agivano al di fuori dell'*accountability* istituzionale.

Infine sottolineiamo come la Hacking Team si fosse ormai affermata come monopolista della partnership privata: l'assenza di una diversificazione del rischio da parte dell'interlocutore pubblico ha fatto sì che gran parte delle vulnerabilità siano emerse con un singolo attacco, suscettibile di rivelare un numero di informazioni sensibili altrimenti non accessibile se si fosse ricorsi ad una molteplice platea di fornitori privati che, idealmente, avrebbero potuto collaborare per fronteggiare le rispettive vulnerabilità agli exploit.

Il superamento dell'impasse causato dall'attacco al principale fornitore di sistemi di 'sicurezza offensiva' alle istituzioni italiane non può che passare dalla costruzione di "una struttura leggera centralizzata multidisciplinare, in parte governativa, in parte privata e in parte legata al mondo della ricerca, in grado sia di far fronte a una serie di servizi e attività di ricerca sia di giocare un ruolo primario nelle linee attuative del processo dinamico di implementazione del Piano Strategico Nazionale di Sicurezza Cibernetica."[44]

La decisione di ricorrere ad un unico fornitore nazionale per i sistemi di 'sicurezza offensiva' (la vendita spyware e malware è disciplinata a livello comunitario dal regolamento 428/2009 su, aggiornato dal regolamento delegato n. 1382/2014)[45] può essere compresa alla luce della mancanza di una reale volontà di cooperazione tra Stati sul fronte cibernetico e dal timore che il ricorso a software di provider stranieri possa offrire a questi una possibilità di spionaggio informatico in particolar modo in settori economici sensibili che abbisognano di una particolare sensibilità difensiva dell'intelligence nazionale[46].

[43] Mele S., (2014) "La cooperazione tra pubblico e privato nella cyber-security, p. 13.
[44] Cyber Security National Lab (2015), Il Futuro della Cyber Security in Italia, ottobre 2015, p. 61.
[45] Regolamento del Consiglio No. 428/2009 del 5 Maggio 2009 "Setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items."
[46] Sistema di informazione per la sicurezza della Repubblica (2016), *Relazione sulla politica dell'informazione per la sicurezza 2015*, pp. 16-18.

3. Trojan di Stato?

Un'altra importante implicazione dell'utilizzo diffuso di spyware quali RCS Galileo è quella legale, che ha portato molti esperti a chiedersi se nel perimetro della nostra Costituzione possiamo delegare un potere così grande e delicato a una simile tecnologia[47]? Il garante della privacy Antonello Soro aveva avanzato forti riserve sull'opportunità dell'utilizzo di questi software che bypassano tutte le modalità tradizionali e la garanzie costituzionali previste dalle tecniche classiche di intercettazione, perquisizione e sequestro di documenti.

Una prospettiva inquietante è quella evidenziata da Bruce Schneier circa le potenzialità del RCS Galileo di poter fungere da *evidence planting* ovvero di poter inserire file e dati falsi e compromettenti nei computer intercettati[48], potenzialità, tuttavia, non ancora confermate dalle analisi effettuate sul software.

Separandoci per un attimo dal piano analitico dell'opportunità politica e dell'*interesse nazionale* legato al mondo dell'intelligence, si pone la controversia in merito all'uso nell'arena giudiziaria dei trojan come strumento di acquisizione della prova.

Le intercettazioni compiute per mezzo di Trojan -sebbene persistano divergenze giurisprudenziali in merito – possono essere incluse nell'alveo dell'art. 266-bis del Codice di Procedura Penale in materia di "intercettazioni di comunicazioni informatiche o telematiche": le proposte di inserire una disposizione ad hoc nel Codice per disciplinare l'utilizzo dei trojan[49] non ha trovato seguito concreto né è sono state recepite disposizioni in merito nella *Dichiarazione dei diritti in Internet* elaborata dalla Commissione per i diritti e i doveri in Internet[50].

---

[47] Milella L., "Antonello Soro: "Mail, cellulari e tablet, rischio Hacking team, può spiarci sempre"", *Repubblica*, 15 luglio 2015.

[48] Bruce Schneier (2015), Hacking Team is Hacked, 6 luglio 2015. Disponibile a: https://www.schneier.com/blog/archives/2015/07/hacking_team_is.html

[49] Rinaldi L., "Caso Hacking Team, perchè serve una normativa chiara contro i Trojan", Wired, 20 luglio 2015.

[50] Camera dei Deputati, 28 luglio 2015, disponibile a http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/TESTO_ITALIANO_DEFINITVO_2015.pdf

Le Sezioni Unite della Corte di Cassazione hanno avuto modo di pronunciarsi in data 28 aprile 2016 sul 'caso Scurato', dalla pronuncia emerge un via libera all'uso di trojan su dispositivi portatili - come pc, tablet e cellulari – limitatamente a procedimenti relativi a delitti di criminalità organizzata, anche terroristica, inclusa l'associazione per delinquere (ed escluso il mero concorso di persone nel reato)[51].

La sentenza si pone in discontinuità con una precedente pronuncia della Cassazione del 2015 (sentenza n. 27100), che escludeva l'utilizzabilità come prova delle captazioni mediante virus informatico, in mancanza di una preventiva indicazione dei luoghi da parte del giudice[52].

La pronuncia sul caso Scurato nel consentire margini di manovra maggiori per gli inquirenti – e per i servizi d'intelligence – nell'utilizzo di tecnologie di intercettazione ha fatto tornare di attualità la discussione sulla proposta di 'trojan di Stato'.

La dizione – impropria – si riferisce nel caso specifico a disegni di legge[53] che, sostenendo la necessità di approntare una difesa più efficiente verso la minaccia terrorista incanalata dai social media, prevedono "la possibilità di consentire alle Forze di polizia l'utilizzo di nuovi programmi informatici che permettano l'accesso da remoto ai dati presenti in un sistema informatico al fine di contrastare preventivamente i reati di terrorismo commessi mediante l'uso di tecnologie informatiche o telematiche."[54]

Una problematicità mai sottolineata dalla letteratura esistente sul tema è quella che riguarda la stessa fonte del 'trojan di Stato': lo Stato o le sue articolazioni regionali, come nel caso dello scandalo del 2011 che riguardò il *Bundestrojaner*[55] adoperato dalle forze di polizia di Baviera, Baden-Württemberg, Brandeburgo e Bassa Sassonia[56],

[51] *La Stampa*, "Intercettazioni col trojan, parziale sì della Cassazione" 29 aprile 2016; Sent. No. 6889/2016 'Scurato'.
[52] Sent. 27100/2015 Sez. VI Penale, 26 maggio 2015, para. 3.
[53] Ultima la proposta di legge n. 3470 presentata dalla deputata Greco concernente la modifica dell'art. 266-bis CPP.
[54] Ibid. p.2 disponibile a http://www.camera.it/_dati/leg17/lavori/stampati/pdf/17PDL0037810.pdf
[55] http://www.zeit.de/2011/42/Bundestrojaner
[56] La scoperta dell'esistenza del *Bundestrojaner* suscitò scandalo anche perché veniva dopo una pronuncia della Corte Costituzionale Tedesca del 2008 che aveva dichiarato illegale l'uso di Internet come strumento di spionaggio da parte delle autorità federali e statali (salvo un numero limitato di eccezioni). *Spiegel Online International*, "Germany's New Right to Online Privacy", 28 Febbraio 2008, disponibile a: http://www.spiegel.de/international/germany/the-world-fromberlin-germany-s-new-right-to-online-privacy-a-538378.html

acquistano gli spyware da imprese private che non agiscono come garanti dell'interesse nazionale, ma che operano secondo logiche di mercato (talvolta contravvenendo alle disposizioni in merito all'esportazione di dual-use technologies sancite dal *Wassenaar Arrangement* e dal citato regolamento 428/2009).

L'assenza di meccanismi che possano garantire l'accountability e meccanismi di rendiconto da parte dei fornitori dei sistemi digitali d'intercettazione, uniti a una tendenza autarchica che porta i principali Stati europei a preferire le imprese nazionali di produzione di software per il controllo da remoto di pc (che si trovano ad agire da semi-monopoliste nelle forniture), alimenta le ricadute sulle intelligence e le forze dell'ordine nazionali qualora si verifichino attacchi[57].

Mentre in Europa la forbice tra politiche sempre più concessive in merito all'utilizzo di trojan e spyware e mancanza di meccanismi di controllo sui fornitori privati va aprendosi[58], gli Stati Uniti muovono progressivamente nella direzione opposta: sembra presumibile che la cyber security americana opererà in un perimetro giuridico e operativo di maggiore prudenza nel caso in cui le attività operative coinvolgano direttamente o indirettamente cittadini americani[59].

4. L'etica degli Hacker

Una visione panottica dei Paesi cui la Hacking Team aveva fornito il software RCS Galileo, e dello status dei diritti umani negli stessi[60] ci aiuta a capire quanto gli interessi commerciali – e non l'interesse nazionale – siano il principale motore dell'attività delle aziende

[57] Il citato *Bundestrojaner* veniva prodotto dall'impresa tedesca DigiTask.

[58] In Spagna l'uso di trojan è previsto dal 2013 per mezzo di una revisione dell'art. 350 del *Codigo Procesal Penal*, in Francia l'utilizzo è regolato dalla legge n. 604 cd. LOPPSI2 approvata l'8 febbraio 2011; rispettivamente *El Pais, La policía podrá usar troyanos para investigar ordenadores y tabletas* e testo della legge n. 604 disponibile a http://www.assembleenationale.fr/13/ta/ta0604.asp

[59] Cyber Security National Lab (2015), Il Futuro della Cyber Security in Italia, ottobre 2015, 80. Caso emblematico è la pronuncia del 7 maggio 2015 con la quale la Second Circuit Court of Appeals di New York ha rovesciato il pronunciamento del giudice di primo grado e contestato alla NSA di aver svolto attività di sorveglianza nei confronti di cittadini americani (raccolta di meta dati) che oltrepassano ciò che è consentito dal Patriot Act.

[60] Human Rights Watch, *World Report 2016*, disponibile a: https://www.hrw.org/world-report/2016

produttrici di software di controllo da remoto di PC e di altri strumenti digitali[61].

Allo stesso modo, le aziende concorrenti erano impegnate nella vendita delle loro tecnologie di sorveglianza a regimi repressivi: la compagnia anglo-tedesca *Gamma International* (Fin Fisher) assieme alla compagnia svizzera *Dreamlab Technologies* avevano fornito nel 2011 al Turkmenistan una *Infection Proxy Infrastructure* applicabile su scala nazionale, mentre la francese *Amesys* aveva venduto il sistema di monitoraggio 'Eagle' al regime di Gheddafi[62], non mancavano però imprese italiane come Area SPA impegnata in vari progetti con il regime di Bashar Assad[63].

Dal 2012 – grazie ai contributi di diverse NGOs e del Citizen Lab di Toronto – il software prodotto da Hacking Team è stato identificato ed associato ad attacchi nei confronti di dissidenti politici, giornalisti, attivisti per i diritti umani e vi sono prove certe che esso sia stato utilizzato da almeno 21 governi[64].

La politica commerciale della Hacking Team, stando alle dichiarazioni del CEO Vincenzetti, si sarebbe configurata come *super partes*, svincolata da potenziali violazioni dei diritti umani commesse per mezzo delle strumentazioni fornite (fintantoché i Paesi non rientrassero nel novero di quelli soggetti a sanzioni di natura internazionale)[65].

Un'ulteriore riflessione politica e legale sulle implicazioni del caso dovrebbe non tanto scrutinare l'etica commerciale della Hacking Team in quanto impresa né le carenze tecniche dei sistemi prodotti[66] – purché le sue condotte non fossero in violazione delle normative nazionali ed europee – quanto i fattori che hanno fatto sì che le forze dell'ordine ed i servizi di intelligence italiani, rilevanti partner

[61] Un resoconto dettagliato sulle violazioni dei diritti umani connesse all'esportazione di *dual-use technologies* viene fornito da: Coalition Against Unlawful Surveillance Exports, (2015) *A critical opportunity: bringing surveillance technologies within the EU Dual-Use Regulation*.
[62] Ibid. pp. 7 e 11.
[63] Locatelli G., "Le aziende che ci spiano in Rete", *l'Espresso*, 14 maggio 2012.
[64] Privacy International, (2015) *Briefing for the Italian Government on Hacking Team's surveillance exports*, p. 4
[65] Si vedano le dichiarazioni del CEO Vincenzetti su: Kushner D, (2016) "Fear This Man", Foreign Policy.
[66] A tal proposito: Marczak et al. (2014), When Governments Hack Opponents: a Look at Actors and Technology, *23rd USENIX Security Symposium*, 20-22 Agosto 2014, San Diego (CA), disponibile a: https://www.usenix.org/conference/usenixsecurity14/technicalsessions/presentation/marczak

commerciali di HT[67] – non si siano rivolti ad una più vasta platea di fornitori, instaurando invece, una relazione bilaterale con la sola HT.

I rapporti tra le istituzioni italiane e Hacking Team sono andati rafforzandosi e non sono stati incrinati dalle evidenze di violazioni di diritti umani perpetrate per mezzo della strumentazione fornita dall'impresa né dalle presunte violazioni dell'embargo verso Sudan e Russia che anzi, come ricordato, il Governo italiano ha smentito.

Diverse sono state le reazioni oltreoceano, dove contratti dal valore di milioni di dollari legavano Hacking Team a DEA e FBI[68]: il senatore dell'Iowa Charles Grassley – presidente della commissione giustizia – ha presentato un'interrogazione per chiedere chiarimenti sul rapporto intercorrente tra le due agenzie statunitensi e l'azienda italiana[69] a cui sono seguite, nel termine di pochi giorni, le comunicazioni di FBI e DEA che annunciavano la cessazione di ogni rapporto commerciale con Hacking Team[70].

5. Conclusioni

L'attacco subito da Hacking Team ha costituito un momento di rottura nella cyber security italiana, è mancata però l'abilità o la volontà politica per far sì che questo potesse tradursi in un momento di discontinuità e di miglioramento rispetto alle strategie passate: all'auspicata intensificazione della partnership tra pubblico e privato non è corrisposta una riflessione su un miglioramento qualitativo di questo rapporto, attraverso una maggiore accountability e trasparenza da parte delle imprese private operanti nel campo della cyber security. Allo stesso tempo la recente pronuncia della Cassazione – pur non giungendo ad avallare un 'trojan di Stato' - ampia i margini di intervento per trojan e spyware andando nella direzione di una concezione maggiormente securitaria dei sistemi di

[67] Dati disponibili su https://wikileaks.org/hackingteam/emails e come riportati dal Corriere della Sera: http://media2.corriere.it/corriere/pdf/2015/fatture.pdf

[68] Bicchierai L.F., "The DEA Has Been Secretly Buying Hacking Tools From an Italian Company", *Motherboard*, 25 aprile 2015.

[69] United States Senate, Committee on the Judiciary, 15 luglio 2015, disponibile a: https://www.judiciary.senate.gov/imo/media/doc/2015-07-15%20CEG%20to%20FBI%20DEA%20DOD%20(Hacking%20Team%20Sudan%20Violations).pdf

[70] US Department of Justice, Office of Legislative Affairs, *Letter of Assistant Attorney General Peter J. Kadzik*, 14 luglio 2015, Washington

intercettazione offensivi. La cancellazione dei contratti da parte di DEA e FBI rispecchia quanto affermato dal senatore Grassley: "è di vitale importanza che le nostre forze dell'ordine e quelle militari abbiano gli strumenti tecnologici necessari per investigare su criminali e terroristi così da poter garantire la sicurezza pubblica, ma è anche importante che li acquistino da fronti responsabili, etiche e che agiscano secondo la legge"[71], le istituzioni italiane sembrano aver recepito in maggior misura la prima parte, mentre vi è il timore che un ripensamento sui fornitori dei sistemi di sicurezza digitale possa essere legato più a circostanze fortuite e transeunti che ad una visione complessiva di lungo termine.

[71] United States Senate, Committee on the Judiciary, 15 luglio 2015, p.2

Bibliografia Primaria

CLUSIT, (2016), Rapporto 2015 sulla sicurezza ICT in Italia.

Cyber Security National Lab (2015), Il Futuro della Cyber Security in Italia, ottobre 2015.

Derechos Digitales, a cura di Perez De Acha G. (2016), Hacking Team: malware para la vigilancia en América Latina, marzo 2016.

Federazione Internazionale Dei Diritti Dell'uomo (2014), "Surveillance Technologies "Made in Europe": Regulation Needed to Prevent Human Rights Abuses, Position Paper, no. 648 Dicembre 2014.

Frediani C. et al. (2015), Attacco ai pirati. Tutti i segreti del datagate italiano, La Stampa, Torino.

Mele S., (2014) "La cooperazione tra pubblico e privato nella cyber-security", per www.sicurezzanazionale.gov

Nichols R. et al. (2014), "Cybersecurity for Government Contractors", Briefing papers, Westlaw, no. 14-15, aprile 2014.

Teti A., (2013) "Cyber intelligence e cyber espionage", Gnosis, no. 3/2013.

Documentazione Primaria

CAMERA DEI DEPUTATI
X Commissione Permanente, 20 aprile 2016, pp. 225-248

Proposta di legge no. 3544, Istituzione del sistema nazionale di sicurezza cibernetica, 19 gennaio 2016.

Proposta di legge n. 3470, Modifica all'articolo 266-bis del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche, 2 dicembre 2015.

Comitato Parlamentare Per La Sicurezza Della Repubblica, Relazione annuale 2015, 17 febbraio 2016.

Citizen Lab, (2014) "Mapping Hacking Team's "Untraceable" Spyware", Munk School of Global Affairs, Toronto. Available at: https://citizenlab.org/2014/02/mapping-hacking-teamsuntraceable-spyware/

Presidenza Del Consiglio Dei Ministri, (2014) Piano nazionale per la protezione cibernetica e la sicurezza informatica.

Sistema Di Informazione Per La Sicurezza Della Repubblica, (2016) Relazione sulla politica dell'informazione per la sicurezza 2015.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies