Sorveglianza: l’azienda italiana che vuole sfidare i colossi NSO e Palantir

By Lorenzo Bagnoli

Published: 2021-11-17 · Archived: 2026-04-05 20:40:29 UTC

C*ybertranquillity* è il motto: tranquillità cibernetica. Alle infinite minacce virtuali, Cy4gate risponde offrendo ai suoi clienti servizi di difesa per garantire sicurezza e protezione. La campagna di marketing funziona, i numeri dell’azienda sono solidi. Al lancio del 24 giugno 2020 sul listino dell’Aim, il mercato borsistico per piccole e medie imprese, è un successo. Il titolo sale del 28% il primo giorno e del 110% in sei mesi. L’offerta pubblica iniziale va meglio del previsto e Cy4gate vince il primo premio «per la migliore strategia di utilizzo del mercato dei capitali nella sezione di raccolta fondi sul Mercato AIM di Borsa Italiana per l’anno 2020». Oggi le performance sono meno clamorose e secondo le analisi di TeleBorsa il titolo, data la sua volatilità, «risulta essere al centro dell’attenzione soprattutto di quegli investitori propensi al rischio». In termini di bilancio la società è solida: nel 2020 ha registrato entrate pari a 12,5 milioni di euro, un aumento di circa il 69% rispetto all’anno precedente.

Nata come *joint venture* tra Elettronica Group ed Expert System nel 2014, Cy4gate è la prima società italiana che combina *cybersecurity* in senso stretto, servizi di intercettazione per polizie internazionali e *intelligence* ad ampio spettro, quella che Cy4gate definisce Continuous Intelligence. Elettronica è un’azienda che vende apparecchiature di bordo in ambito militare, dalla marina all’aviazione, tecnologie per la “guerra elettronica” come strumenti anti-drone, sistemi per la rilevazione di minacce e per la sorveglianza delle comunicazioni. Expert System, invece, lavora nel settore dell’intelligenza artificiale e sviluppa un software, *COGITO*, in grado di analizzare e comprendere le informazioni contenute nei testi.

L’inchiesta in breve

- Cy4gate ha registrato entrate pari a 12,5 milioni di euro nel 2020, un aumento di circa il 69% rispetto all’anno precedente. Il suo obiettivo è quello di sfidare i due competitor, NSO e Palantir, aziende note per gli abusi delle proprie tecnologie da parte di regimi autoritari e per l’impiego di strumenti di monitoraggio dei social media.
- Cy4gate ha registrato contratti in quasi tutto il mondo: Emirati Arabi, Arabia Saudita, Pakistan, Qatar, Asia Centrale (non specifica dove), America Latina (almeno Argentina e Messico), ma ci sono anche la Nato e progetti europei. Molti di questi Paesi sono già stati coinvolti in abusi delle tecnologie di sorveglianza in passato.
- D-SINT è la piattaforma di Cy4gate per sfidare Palantir: un sistema che monitora i social media e altri database per estrarre informazioni grazie ad algoritmi di intelligenza artificiale, tra cui quelli di riconoscimento facciale e di oggetti, e prendere così decisioni con il supporto dei dati.
- Epeius invece è il sistema per le intercettazioni con cui Cy4gate vorrebbe sfidare NSO. Il sistema sarebbe in grado di prendere il controllo degli *smartphone* ed estrarre informazioni private. Cy4gate ha già però

avuto alcuni passi falsi con Epeius, la Procura di Napoli ha infatti sospeso l'uso del sistema per alcuni disservizi.

- Cy4gate, NSO e Palantir hanno visto nella pandemia di Covid-19 un'opportunità per espandere il proprio mercato: tutte e tre hanno infatti offerto sistemi o per il tracciamento dei contatti o per aiutare nell'analisi dei dati legati alla pandemia—in molti casi queste operazioni sono finite al centro di scandali.

In Italia Cy4gate non ha concorrenti: nessuno è in grado di offrire tutti questi servizi e prodotti insieme. All'estero, invece, i nomi dei grandi *competitor* – i quali hanno ancora un volume d'affari che non è nemmeno comparabile con quello dell'azienda italiana – sono Palantir e NSO Group. È la stessa Cy4gate a riconoscerli come *competitor* e punti di riferimento, includendoli in presentazioni e parlandone in interviste.

La prima è una società americana il cui nome è indissolubilmente legato al settore militare americano e di cui uno dei fondatori – Peter Thiel – è stato un grande finanziatore di Donald Trump. La seconda è il gruppo israeliano che ha creato *Pegasus*, lo *spyware* che ha infettato i telefoni di politici, attivisti e giornalisti di mezzo mondo protagonista dell'inchiesta Pegasus Project e recentemente incluso nella *blacklist* degli Usa delle aziende con cui non fare affari.

I prodotti con cui Cy4gate ha intenzione di sfidare NSO e Palantir sono due rispettivamente: un software per le intercettazioni, *Epeius*, e una piattaforma in grado di raccogliere e analizzare informazioni presenti online o raccolte direttamente dai dispositivi elettronici e digitali, *D-SINT*.

In un'intervista del dicembre 2020 al canale Youtube specializzato Vivere di dividendi l'allora amministratore delegato Eugenio Santagata – oggi a Telsy, azienda che si occupa di sicurezza delle infrastrutture di telecomunicazioni che appartiene al gruppo Telecom – specificava che per alcune attività di *cyber intelligence* offensive, quelle che hanno bisogno delle autorizzazioni di magistratura e governi, «noi passiamo dalla parte di chi fa *ethical hacking* e quindi dalla parte dei buoni». Con questa considerazione Santagata sembra accorpare due diversi prodotti di Cy4gate: la raccolta di informazioni pubbliche online da un lato e dall'altra le intercettazioni tramite *spyware* per conto di organi inquirenti. All'interno del mercato della sorveglianza in continua espansione, è quest'ultimo il settore dove ci sono stati i maggiori abusi. Al centro degli scandali ci sono state spesso aziende italiane come l'ex Hacking Team (ora nota con il nome di Memento Labs), Area SpA, e RCS, accusate di malfunzionamenti delle proprie tecnologie, presunte violazioni dell'export o abusi.

Sorveglianza globale

Paesi o aree geografiche dove l'azienda Cy4gate dice di avere esportato propri prodotti, siglato contratti e sviluppato il proprio business. In molti casi l'azienda non offre dettagli sull'identità dell'acquirente

La rivale Palantir

Il software con il quale Cy4gate sfida Palantir sul terreno delle piattaforme di intelligence si chiama *D-SINT*, acronimo di Digital Signal Intelligence: raccoglie, processa e mette in correlazione dati che hanno formato e provenienza diversi, dalle immagini dei social network fino alle informazioni presenti nel *dark web*. «L'informazione giusta, al momento giusto, alle persone giuste, nel modo giusto», afferma l'azienda in una brochure di presentazione. L'analisi è facilitata dall'uso del software *COGITO*, sviluppato da Expert System (una

delle due società da cui è nata Cy4gate), e dal software di riconoscimento facciale e di oggetti sviluppato da iCTLab, spin-off dell'Università di Catania. L'integrazione – si legge in una presentazione del 2019 – permetterà di effettuare ad esempio una ricerca su un individuo all'interno di testi, all'interno di database di immagini, o su Twitter e lo stesso vale per gli oggetti.

Le due aziende erano anche in procinto di sviluppare un'opzione per il riconoscimento vocale «relativo a possibili intercettazioni telefoniche o file audio raccolti in database o da dispositivi portatili». Sempre nelle slide, le due aziende sottolineano però una criticità nell'uso di questo tipo di algoritmi per il riconoscimento: «Data la crescente polarizzazione del focus sulla questione della privacy, questo ambito rappresenterà un fattore critico per l'utilizzo dei dati raccolti e analizzati».

Screenshot tratto dalla presentazione tenutasi durante il Workshop "AI for Cybersecurity" del 18 marzo 2019 presso il Centro Congressi Auditorium della Tecnica. Oggetto della presentazione sono le capacità della piattaforma D-SINT che può sfruttare anche algoritmi di riconoscimento facciale e di oggetti sviluppati da iCTLab

È un mercato per pochi quello delle piattaforme di *intelligence* come *D-SINT*, in grado di analizzare una molteplicità di dati provenienti da qualsiasi tipo di fonte, sia pubbliche sul web sia database privati. Negli ultimi anni si è distinto, tra luci e ombre, il gruppo Palantir Technologies, il cui software, scrive *Bloomberg* in un articolo del 2018, è in grado di «conoscere tutto su di te».

Palantir è stata fondata nel 2003 dal *venture capitalist* Peter Thiel, tra i co-fondatori di PayPal che nel 2016, scrive *Buzzfeed*, ha cercato di trasformarsi nel filantropo finanziatore dell'*alt-right* americana, la galassia di destra eversiva – che mescola insieme cospirazionismo, tratti di anticapitalismo e suprematismo bianco – che sostiene strenuamente l'ex presidente degli Stati Uniti Donald Trump. Sin dalla sua fondazione Palantir ha collaborato con CIA e Pentagono in Afghanistan e Iraq, ricevendo finanziamenti da In-Q-Tel, la società di investimento non profit legata alla stessa CIA che promuove l'innovazione nel settore tecnologico. Palantir non si occupa direttamente di intercettazioni ma permette di analizzare i dati già raccolti, fornendo analisi e mostrando collegamenti: in questo modo è più facile prendere decisioni.

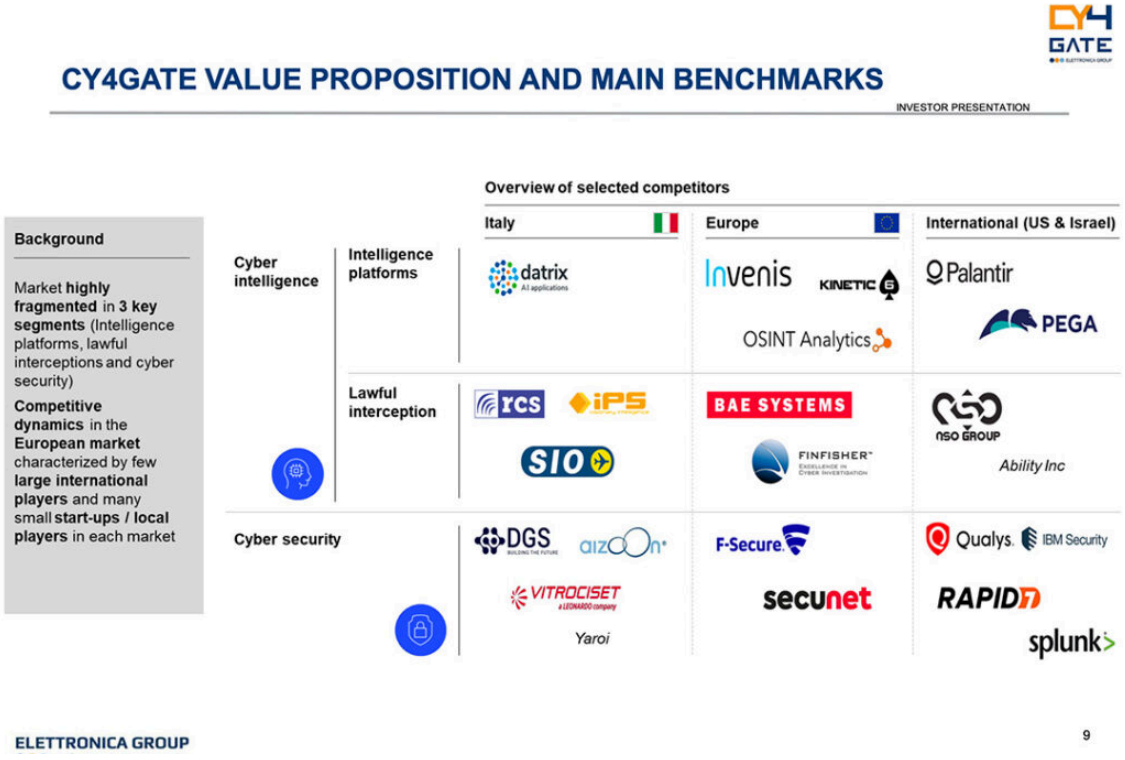
Oltre agli impieghi nel settore militare, i software prodotti da Palantir sono stati utilizzati dalla United States Immigration and Customs Enforcement (ICE), l'agenzia federale statunitense che si occupa delle frontiere, per individuare e deportare immigrati irregolari. Palantir ha fornito anche un software di polizia predittiva alle forze dell'ordine della città di Los Angeles per monitorare, identificare e sorvegliare persone ritenute sospette: alcune analisi del funzionamento del software sembrano già indicare che a pesare in maniera significativa sulle decisioni siano pregiudizi su base razziale. Su Palantir, però, sembrano emergere anche altre ombre. Secondo Intelligencer, una sezione del *New York Magazine*, ex appartenenti all'esercito e ufficiali dell'*intelligence* hanno sottolineato come il successo di Palantir sia più legato al fatto di avere un'interfaccia pulita e semplice per vedere i dati e non all'effettivo utilizzo di una tecnologia avanzata.

Alla prova della pandemia

Sia Cy4gate, sia Palantir, con il perdurare della pandemia hanno cercato di introdursi anche nel mercato della sanità europeo. Cy4gate nei primi mesi della pandemia, ha annunciato la creazione del sistema HITS, Human Interaction Tracking System, un sistema di tracciamento dei contagi da coronavirus. Hits era stato proposto anche al governo, che poi ha preferito Immuni, al contrario di altre aziende private che hanno adottato il software di Cy4gate.

Palantir è riuscita ad agganciare i sistemi sanitari nazionali. I nuovi contratti legati alla pandemia sono tra le ragioni del +49% nel flusso di cassa messo a bilancio dalla società nel secondo trimestre del 2021. Il governo greco ha siglato un accordo segreto per condividere dati sanitari della popolazione con Palantir e, a seguito dello scandalo emerso, l'Autorità per la privacy greca ha avviato un'indagine e il governo avrebbe concluso ogni collaborazione e fatto cancellare i dati.

Un accordo simile c'è stato anche nel Regno Unito con il National Health Service (NHS), il servizio sanitario nazionale, dove però due cause giudiziarie portate avanti da organizzazioni della società civile, openDemocracy e Foxglove, hanno spinto il governo britannico a promettere di concludere l'accordo con Palantir. Simili problemi sulla trasparenza degli accordi e delle finalità dei dati raccolti, hanno messo Palantir al centro delle attenzioni politiche anche negli USA.



Screenshot tratto dalle slide della presentazione per la Conferenza Virtuale dell'AIM datata 27 maggio 2021. Nella foto si vedono i competitor selezionati da Cy4gate nei rispettivi settori di mercato. Oltre a Palantir e NSO, ci sono anche altri nomi noti in Italia come IPS, RCS, e SIO, tutti coinvolti nel settore delle intercettazioni per le procure.

Anche NSO Group, la società israeliana protagonista del Pegasus Project che collabora con le agenzie di *intelligence* di mezzo mondo, in tempi di pandemia ha cercato di sviluppare un software per il *contact tracing*. *Fleming*, questo è il nome del software, ha però avuto difficoltà fin dal lancio. L'azienda è stata accusata di aver utilizzato durante il lancio dati personali di trentamila persone reali, ignare che i dati dei propri spostamenti fossero usati nelle presentazioni dei prodotti, circostanza che sarebbe una violazione della privacy. Il cattivo risultato sul fronte tracciamento rischia di trasformarsi in una perdita economica, dato che già gli indicatori hanno spinto la società di rating Moody's a declassare l'affidabilità creditizia a B3 a maggio 2021.

I software per competere sulle intercettazioni

NSO è un punto di riferimento soprattutto per le intercettazioni e le attività di sorveglianza della polizia. Qui Cy4gate offre tre sistemi: *Epeius*, *Hydra* e *Gens.AI*. *Epeius* è uno *spyware* che può essere installato sugli smartphone e i dispositivi di una persona per monitorare le sue attività ed estrarre, ad esempio, copia dei dati delle chat e foto, dati sulla posizione e email. *Hydra* invece permette di monitorare la navigazione online, individuando le applicazioni usate, i siti web visitati, e se si fa uso di VPN o del Tor Browser – due tecnologie che permettono di navigare in modalità più sicura e nascondere la propria identità. L'utilizzo di *Epeius* e *Hydra* è «riservato alle Forze di Polizia e alle Agenzie di Intelligence Italiane ed estere», si legge in un documento di Cy4gate.

Gens.AI, invece, permette di creare e gestire dei falsi profili da usare sui social network, facilitando le attività di indagine: in questo modo gli agenti possono interagire con le persone senza destare sospetti.

Le prime tracce pubbliche di *Epeius* sono emerse in collegamento con l'Italia, secondo un articolo di *Motherboard* pubblicato a febbraio 2021 che ha rivelato la presenza di una finta pagina WhatsApp in italiano che avrebbe permesso l'installazione di un modulo in grado di inoculare *Epeius*. Non è chiaro quale fosse lo scopo della pagina, se utilizzata per attività dell'*intelligence* italiana o per intercettazioni durante le indagini di polizia. Quel che è certo, però, è che l'azienda ha già problemi con le procure italiane: la procura di Napoli ha infatti sospeso l'uso di uno *spyware* gestito da SIO e riconducibile a Cy4gate per colpa di «un grave disservizio».

Cy4gate ha infatti siglato a marzo 2020 un accordo con la società SIO S.p.A., una delle aziende italiane che si occupano di noleggiare apparecchiature per intercettazioni alle Procure della Repubblica. L'accordo, i cui dettagli sono riportati nel documento di ammissione all'AIM, concede a SIO «l'utilizzo in esclusiva del captatore informatico *Epeius*» e a Cy4gate sarà riconosciuta la «totalità del corrispettivo corrisposto dalle Procure utilizzatrici di *Epeius* per la corretta "infezione" di un dispositivo (da remoto o in loco)» e una percentuale del fatturato annuo realizzato da SIO grazie all'uso di *Epeius*: del 50% se il fatturato è sopra ai 4 milioni di euro o del 60% se inferiore.

Secondo le stime di Cy4gate, l'accordo con SIO permette di avere accesso a circa 70 nuove procure e raggiungere una quota pari al 70% di un mercato, quello delle intercettazioni di polizia, stimato dalla stessa azienda sui 36,3 milioni di euro.

In un comunicato stampa del 10 febbraio 2021, Cy4gate ha confermato che i disservizi della procura di Napoli sono dovuti a dei malfunzionamenti e che, nel caso specifico, la situazione «è stata prontamente individuata e sottoposta a scrupolosa analisi». Secondo fonti intervistate da *Motherboard*, in alcuni casi il software per le intercettazioni avrebbe fatto apparire una notifica sullo schermo della persona indagata, rischiando di destare sospetti.

L'inarrestabile ascesa di Cy4gate

NSO, punto di riferimento nonostante i guai

Il Dipartimento del Commercio degli Stati Uniti il 3 novembre scorso ha inserito NSO in una *blacklist* dove vengono inserite aziende i cui software sono stati usati per «prendere di mira in modo doloso funzionari governativi, giornalisti, uomini d'affari, attivisti, accademici e dipendenti delle ambasciate», come recita il comunicato stesso. Chi è inserito nella lista non può più acquistare tecnologia da società statunitensi, che a loro volta hanno ovviamente il divieto di vendere alle aziende che si trovano sulla lista stessa. L'iniziativa è stata presa dal Dipartimento del Commercio a seguito delle rivelazioni del Pegasus Project.

Per quanto sempre più discusso e controverso, NSO Group resta un punto di riferimento del settore. Cy4gate non fa eccezione: «I nostri *competitor* principali sul settore governativo sono israeliani e sono anche un punto di riferimento perché abbiamo nel tempo imparato molto da loro», diceva nell'intervista di dicembre 2020 a Vivere di dividendi Eugenio Santagata, allora Ad di Cy4gate.

Come dimostrano i contratti ottenuti da Cy4gate, l'azienda si è inserita in mercati controversi, competendo con società che sono state investite da scandali a causa dei contratti stretti con forze dell'ordine di regimi autoritari.

Come NSO, che infatti è coinvolta in due casi di rilievo collegati proprio agli Emirati Arabi, Paese dove anche Cy4gate è molto attiva. A inizio ottobre 2021 una corte britannica ha confermato che il primo ministro emiratino, lo sceicco Mohammed bin Rashid al-Maktoum, ha fatto spiare lo smartphone della propria ex moglie e dei suoi legali usando il software *Pegasus*. NSO aveva rescisso il contratto per l'utilizzo del proprio software dopo essere venuta a conoscenza dell'accaduto.

L'altro caso, invece, riguarda l'ingegnere, blogger, e attivista Ahmed Mansoor, che negli anni è stato oggetto di attacchi con tre diversi software: nel 2011 con quello di FinFisher, nel 2012 con quello di Hacking Team, e nel 2016 con quello di NSO sfruttando una vulnerabilità il cui prezzo è stimato intorno al milione di dollari. In tutti e tre i casi, le tecnologie sono riconducibili alle azioni del governo degli Emirati. Mansoor è stato arrestato nel 2017 e deve scontare una pena di 10 anni per quello che, secondo Human Rights Watch, è stato un processo ingiusto con accuse fittizie.

Alla luce delle ombre che avvolgono i due competitor NSO e Palantir, Cy4gate ha dichiarato a *IrpiMedia* di condannare «ogni forma di utilizzo improprio o fuori dalla cornice di legittimità di prodotti che nascono con una chiara, specifica ed esclusiva finalità: supportare gli enti preposti nella prevenzione e repressione di crimini efferati». Inoltre, «Cy4Gate opera esclusivamente nell'alveo delle norme nazionali e internazionali vigenti e mette la propria tecnologia a disposizione delle *law enforcement agencies* con l'intento di contribuire alla prevenzione e repressione di reati nell'interesse esclusivo delle comunità di cui gli utilizzatori sono i principali tutori», ha dichiarato una portavoce dell'azienda.

Malgrado i recenti passi falsi con le procure italiane, Cy4gate non sembra fermarsi. A giugno 2021 era presente alla conferenza ISS World Middle East and Africa, un evento che fa parte di una serie di conferenze annuali che si svolgono in tutto il mondo dove si ritrovano aziende di sorveglianza, governi ed esperti di sicurezza e intelligence. Nella copia archiviata dell'agenda dell'evento si legge che Cy4gate avrebbe tenuto due sessioni: una su Gens.AI e l'altra sulla piattaforma di *cyber intelligence* e «come controllare e combinare insieme in tempo reale tutte le informazioni recuperate dal target sotto sorveglianza, facendo leva su più classi di sensori attivi e passivi». Il prossimo appuntamento è con ISS World Europe che si svolgerà a Praga a dicembre.
