CYBER & SECURITY: LESSON LEARNED DALL'ESCALATION ISRAELE-HAMAS

Gianmarco Gabriele Marchionna

Analytica
FOR INTELLIGENCE AND SECURITY STUDIES

ANALYTICA FOR INTELLIGENCE AND SECURITY STUDIES

- CYBER SECURITY
  ISSN: 2784-8779

CYBER & SECURITY: LESSON LEARNED DALL'ESCALATION ISRAELE-HAMAS

Gianmarco Gabriele Marchionna

TORINO, NOVEMBRE 2023

www.analyticaforintelligenceandsecuritystudies.it

Analytica
FOR INTELLIGENCE AND SECURITY STUDIES

Abstract

Alla luce delle recenti tensioni tra Israele e Hamas , è possibile individuare alcune Lesson Learned, attraverso un'analisi del ruolo dei vari attori coinvolti nella sicurezza nazionale israeliana a partire dal ruolo della dimensione cibernetica . L'analisi dello scontro in corso tra Israele e Hamas si concentra sulle implicazioni cyber e di sicurezza. Oltre alle dinamiche digitali, l'analisi si estende alla sicurezza fisica e al coordinamento tra apparati di sicurezza, con attenzione alle conseguenze sulla sicurezza nazionale e delle infrastrutture critiche.
Le lesson learned mettono in luce l'importanza dell'integrazione e interoperabilità dei sistemi di sicurezza, sottolineando la necessità di risposte coordinate per affrontare le sfide emergenti. Questo approccio offre insights critici per lo sviluppo futuro di strategie di difesa in contesti simili.

Israele-Hamas: la dimensione cyber dell'attacco

Nell'ottobre 2023, a premessa dell'attacco condotto da Hamas al confine con Israele, il mondo ha assistito ad una serie di attacchi informatici di portata e intensità rilevanti. Questi attacchi sono stati eseguiti da gruppi di hacktivist con obiettivi e affiliazioni diverse. Tra i vari attacchi registrati, è interessante porre in evidenza alcuni di questi ed analizzarli dal punto di vista della loro rilevanza strategica nel contesto del conflitto israelo palestinese. Il 6 ottobre, il gruppo di hacktivist CyberAv3ngers ha attaccato il Noga - Israel Independent Systems Operator, la centrale elettrica principale del governo israeliano, con attacchi DDoS. Questi attacchi hanno preso di mira infrastrutture critiche in Israele, possibilmente perpetrati da attori locali o regionali, causando instabilità nel paese. Atti simili sono stati compiuti da Anonymous Sudan, sospettato di legami con la Russia, attaccando le applicazioni di allerta utilizzate per avvertire i cittadini degli imminenti attacchi di Hamas che ha avuto come conseguenza un effetto sorpresa implementato ed un maggior impatto sulla popolazione civile coinvolta nell'attacco. Gruppi russi come 'Killnet' e Anonymous Sudan hanno attaccato il sito web del governo israeliano e del Jerusalem Post. Un attore noto come "blackfield" ha minacciato di utilizzare dati sensibili di soldati israeliani per ulteriori attacchi e ha suggerito di prendere di mira gli Stati Uniti in futuro. I CyberAv3ngers hanno annunciato di aver compromesso ORPAK, un'azienda di gestione del carburante. AnonGhost ha pubblicato un elenco di obiettivi israeliani vulnerabili a CVE-2023-29489, una vulnerabilità XSS. Tutti questi eventi, per quanto possano apparire scollegati e di poco conto, se analizzati nella loro complessità dimostrano almeno due aspetti fondamentali: per erodere la resistenza emotiva della popolazione sottoposta ad attacco non è più necessario impegnarsi sul terreno con grandi manovre ma è sufficiente diffondere a mezzo stampa e social media immagini e comunicati dal forte impatto visivo intrisi di violenza ed emozioni primarie; in secondo luogo si può evidenziare la dimensione sempre più internazionale delle attività cibernetiche durante uno scontro.

Dall'analisi di questi attacchi è stato inoltre possibile estrapolare e categorizzare informazioni quantitative come, per esempio, la numerosità e le capacità offensive dei contraenti. Si osserva un aumento del numero di gruppi criminali informatici entrati nello scontro, mirando alle infrastrutture su entrambi i lati: 23 Gruppi pro-Israele; 103 Gruppi pro-Palestina; 4 Gruppi neutrali.
Non di minore importanza l'analisi dei target degli attacchi: gli hacktivist pro-Gaza stanno collettivamente mirando a Paesi come India, Egitto, Kenya, Francia, Germania, Italia, Regno Unito e Stati Uniti (oltre a Israele). D'altra parte, gli hacktivist pro-Israele stanno mirando a Iran, Iraq, Arabia Saudita, Libano e Qatar (oltre alla Palestina e Gaza).
Nonostante tutto, non possiamo ancora parlare di guerra cibernetica in senso stretto. La cyber warfare, infatti, rappresenta un settore strategico che impiega strumenti informatici e tecnologici per condurre operazioni tanto offensive quanto difensive e attività di spionaggio. Questa forma di conflitto moderno si estende a governi, organizzazioni e, in alcuni casi, può influenzare dinamiche sociali a livello globale ridefinendo il paradigma del conflitto, consentendo attacchi senza la necessità diretta di coinvolgere le forze armate tradizionali. In tal caso, la riflessione si orienta verso la cybersecurity, focalizzandosi sulla dimensione operativa digitale e informatica, strettamente correlata alla sicurezza nazionale e di natura trasversale ai quattro domini bellici tradizionalmente riconosciuti. Non trattandosi di guerra cinetica né statica, siamo fuori dal mondo della hybrid warfare, siamo in una dimensione operativa nettamente differente.
Inoltre, è utile sottolineare che dal punto di vista del diritto, si può parlare di cyber warfare quando è possibile riconoscere uno Stato aggressore ed uno Stato aggredito, ossia due entità giuridiche con sovranità esterna oltre che interna. Nel momento in cui si parla di entità non riconosciute internazionalmente (i.e. stati fantoccio, movimenti di liberazione nazionale o qualsiasi altro attore senza una sovranità esterna) allora non è possibile definire il confronto come guerra cibernetica ma di cyber operations e più generalmente di attacchi cyber.
Il problema della definizione però non riduce l'importanza del tema. Il mirato attacco alle infrastrutture critiche, come centrali elettriche e sistemi di trasporto, rappresenta un ulteriore terreno di scontro ed una ulteriore criticità a cui far fronte in caso di escaletion, con l'intento di interrompere servizi e creare instabilità sociale e logistica. Le operazioni di information warfare influenzano l'opinione pubblica e le decisioni politiche attraverso la manipolazione della narrativa pubblica e la diffusione di disinformazione. Strategie come il Social Engineering e il phishing sono finalizzate a manipolare le persone per ottenere accesso non autorizzato ai sistemi. Gli attacchi di ransomware, mediante la crittografia dei file delle organizzazioni, richiedono un riscatto per il ripristino dell'accesso, mentre il cyber-spionaggio coinvolge la raccolta di informazioni sensibili o segrete da parte di entità esterne.
Quanto descritto finora delinea la diversificata ed ampia gamma di minacce presenti nel contesto del confronto cibernetico, evidenziando la complessità e l'urgenza della difesa e della sicurezza digitale di pari passo con quella tradizionale. Da qui la necessità di adottare ed implementare strategie che coordinino tanto le minacce cibernetiche tanto quelle legate alla sicurezza fisica delle infrastrutture, necessità che si sta facendo via via più imperativa a causa della forte interconnessione globale tra sistemi ed infrastrutture.

Implicazioni Cyber e di Security

Israele ha a lungo ritenuto che l'aver reso il confine con la Palestina un luogo altamento tecnologico lo facesse diventare un divisorio impenetrabile dalla Striscia di Gaza. Tuttavia, a seguito dell'aggressione di Hamas, dichiarazioni riservate di funzionari militari israeliani ai media hanno portato alla luce significative lacune nel processo dell'elaborazione delle informazioni d'intelligence e nella difficoltà di coordinarsi tra compente cibernetica e human intelligence, consentendo in questo spazio ancora poco esplorato, una violazione sorprendentemente agevole del confine.
Nel corso di un attacco all'alba di sabato 7 ottobre 2023, oltre 1.500 terroristi hanno oltrepassato il confine israeliano, utilizzando mezzi diversi come pickup e motociclette. L'avanzata di Hamas è stata supportata dalla presenza dei cecchini in posizioni avanzate e dall'uso di droni esplosivi e bulldozer che hanno rallentato la mobilità delle truppe israeliane giunte sul posto per fermare l'imminente attacco e permesso il superamento della recinzione in circa 30 posizioni lungo il confine. Fin qui si delinea un attacco di stampo tradizionale, il fatto che le difese israeliane non abbiano retto all'urto di un attacco tradizionale è però da ricercarsi nella dimensione cibernetica. L'intelligence israeliana aveva sottolineato come nei giorni precedenti l'attacco ci fosse stato un importante aumento del traffico dati che avrebbe sovracaricato la rete di sorveglianza perimetrale del confine e permesso l'accesso al sistema rendendolo facilmente manovrabile. L'informazione è stata trascurata facendo rimanere il livello di guardia a livelli minimi, il quale ha reso inefficace la difesa del confine. Il successo dell'attacco di Hamas, che in un solo momento ha neutralizzato comunicazioni, centri di sorveglianza e sistemi di difesa ed attacco, è dunque da imputarsi tanto all'attacco cyber diretto alle strutture perimetrali tanto alla mancanza di attenzione da parte degli operatori destinati all'analisi.
Sul piano cibernetico, le personalità hacktivist si sono concentrate su attacchi volti a fungere da cassa di risonanza delle azioni compiute al confine dai miliziani di Hamas. In rete, nelle ore immediatamente successive sono stati postati e ricondivisi migliaia di video e foto delle atrocità commesse nei confronti della popolazione israeliana che viveva nei kibbuz e nelle zone limitrofe al confine andando ad aumentare il senso di insicurezza e di vulnerabilità nella popolazione. Racconti dalla narrazione forte volte a plasmare la percezione e le opinioni della popolazione si sono succedute in rete nei giorni successivi agli attacchi, coinvolgendo non solo la popolazione israeliana ma l'intera comunità internazionale. Il Medio Oriente con le sue continue tensioni regionali ha permesso che esso diventasse un luogo di grande prosperità per i gruppi di hacking, complice anche la disponibilità economica delle petromonarchie e la necessità di combattere attraverso metodi non convenzionali dei paesi regionali.

Con l'escalation del conflitto israelo-palestinese e i diversi attacchi ci si è ritrovati di fronte ad un problema che non solo potrebbe incidere sempre più pesantemente sulla sicurezza degli Stati ma che sarà complesso arginare in qualche modo. Gruppi ritenuti affiliati ad Hamas, Hezbollah e l'Iran sono attivi da anni nella regione, conducendo operazioni che vanno dallo spionaggio cibernetico e furto di dati alle operazioni di hacking e rilascio di informazioni, oltre al mirare ad infrastrutture strategiche di grande rilievo. In futuro, data la grande presenza di gruppi attivi, sia politicamente schierati che non, ci si potrebbe aspettare che vi sia una convergenza di intenti e che gruppi più piccoli e meno rintracciabili possano compiere attacchi in subappalto per occultare il ruolo di Stati sovrani direttamente coinvolti negli stessi. Tutto questo renderebbe ancora più complesso prevenire e perseguire i mandanti e gli esecutori degli attacchi, soprattutto se da essi dipendono danni a infrastrutture e/o persone fisiche. Di fatto, la diversità e l'adattabilità dei c.d. cyber threat actors iraniani li rendono un componente significativo e sfaccettato del panorama di minaccia globale in continua evoluzione.

È emblematico, infatti, il supporto che Hamas ha ricevuto da parte di aggressori filoiraniani. L'Iran ospita una varietà di threat actors sponsorizzati dallo Stato, il cui coinvolgimento si estende oltre il contesto specifico del conflitto tra Israele e Hamas. Questi presentano diversità in termini di dimensioni, capacità e motivazioni, e sono responsabili di una vasta gamma di operazioni cyber. Mentre alcuni di questi attori hanno chiari legami con il governo iraniano, molti hacktivist iraniani operano affermando di essere indipendenti. È importante riconoscere che i collettivi hacktivist emergenti – oltre ad essere utilizzati come strumento per oscurare la sponsorizzazione statale - possono influenzare l'opinione pubblica e rendere difficile l'attribuzione delle azioni offensive.

Nel monitorare l'evoluzione della situazione in Medio Oriente, è essenziale prestare attenzione all'Iran come possibile origine di azioni offensive informatiche dirette e operazioni per procura sostenute da gruppi affiliati, come Hezbollah e la stessa Hamas. Tra le finalità troviamo principalmente la compromissione dei sistemi di sicurezza, il blocco di siti web istituzionali attraverso la diffusione di simbologia, editing di contenuti e pratiche di gestione infrastrutturale, estorsione di denaro in seguito al furto di dati sensibili, spionaggio informativo e monitoraggio e intercettazione delle comunicazioni.

L’integrazione e l’interoperabilità: le Lessons Learned per la sicurezza nazionale

Alla luce del contesto appena ricostruito, emergono una serie di criticità relative alla security in generale, da quella tradizionale a quella cyber, e ai temi dell’integrazione e dell’interoperabilità dei sistemi, che andrebbe esteso nella stessa accezione agli apparati di sicurezza e di intelligence.

In primo luogo, per integrazione dei sistemi e in questo caso degli apparati intendiamo il processo di connessione e coordinazione di diverse componenti o sistemi all'interno di un'organizzazione. Si veda, ad esempio: l’automazione industriale, come integrazione di dispositivi di controllo degli impianti; la connessione e sincronizzazione di sistemi informatici per gestire dati, monitorare l’efficienza e facilitare le prestazioni; l’implementazione di reti e protocolli di comunicazione per lo scambio tra dispositivi e sistemi diversi. In secondo luogo, vediamo all’interoperabilità come la capacità di diversi sistemi di lavorare insieme in modo efficace, dove l’output di uno diventa input e richiesta per l’altro, senza la necessità di modifiche o interventi aggiuntivi. Si pensi allo scambio bidirezionale di dati tra sistemi, all’integrazione di componenti e alla sincronizzazione delle operazioni o alle capacità di un sistema SCADA (Supervisory Control and Data Acquisition), utilizzato per monitorare e controllare infrastrutture critiche e processi industriali in tempo reale.
Dall’escalation tra Israele e Hamas, al netto degli interventi di supporto citati come quello iraniano o di gruppi di attivisti affiliati a Hezbollah, emerge probabilmente una buona integrazione di sistemi e apparati di sicurezza nazionali israeliani che nel caso specifico non hanno funzionato correttamente in termini di interoperabilità. Infatti, la causa dell’insuccesso israeliano è da imputarsi probabilmente nella bassa interoperabilità tra sistemi di controllo e monitoraggio e gli apparati di sicurezza statali. Punto cruciale per apparati dove lo scambio informativo bidirezionale è base fondante, ancor più se i sistemi e le strutture del potere e informative non riescono a comunicare in settori cosiddetti essenziali. È in questo contesto che possiamo parlare dell’interoperabilità come fondamentale elemento connotativo tra comparti di intelligence, forza armate (sicurezza fisica e human terrain), cybersecurity (statali e parastatali) e human intelligence, incidendo principalmente sulla fuoriuscita di dati e informazioni sensibili, sul mancato riconoscimento della minaccia e del relativo rischio sia cyber che fisico, e sull’influenza che una potenziale leva motivazionale o persino economica ha scaturito nella popolazione civile al servizio dell’IDF, primi fra tutti gli informatori.
Proprio parlando di servizi essenziali impattati - citando la Direttiva europea NIS 2 - quali centrali elettriche, mezzi di trasporto, infrastrutture fisiche e digitali, servizi di telecomunicazioni e controllo, istituzioni e amministrazioni pubbliche, è possibile evidenziare come, a differenza del conflitto russo-ucraino in cui la cybersecurity ha svolto un ruolo centrale nella ridefinizione degli scontri e nel supporto all’azione cinetica, lo scontro in corso tra Israele e Hamas faccia emergere da un lato l’eguale importanza tra sicurezza fisica e cibernetica e dall’altro la rilevanza dell’intervento umano nell’analisi strategica nel rilevamento della minaccia.

Quanto riportato all'articolo 21 della NIS 2 fa scuola nel contesto dell'escalation israeliano. Nello specifico, se esaminiamo le integrazioni tra i sistemi che supportano le operazioni per la sicurezza nazionale di Israele, emerge che la catena di approvvigionamento rappresenta il punto critico di insuccesso nell'integrazione e nell'interoperabilità. Inoltre, è da evidenziarsi come una delle preoccupazioni principali degli analisti europei nel settore della cyber sicurezza fosse proprio la marginalizzazione del contributo umano al ciclo d'intelligence per l'analisi delle minacce attuali e future che è quanto accaduto nella Striscia di Gaza ad ottobre 2023. Le tecnologie sono un supporto valido ed imprescindibile degli apparati di sicurezza ma non possono sostituire in toto il ruolo della componente human nel supporto informativo, pena una visione parziale e miope delle minacce al sistema di difesa nazionale ed alla sua relativa sicurezza. È l'esempio di come un contesto caratterizzato da una complessa infrastruttura tecnologica, l'acquisizione di informazioni mediante pratiche di ricerca informativa tradizionale, consente di ottenere accesso ai sistemi di sicurezza dell'avversario.

In altre parole, nel contesto specifico, non possiamo evidenziare un vero e proprio fallimento del sistema informativo e di intelligence, come spesso presentato dai media. Piuttosto Israele ha affidato totalmente la sua sicurezza alla tecnologia e di conseguenza alla sicurezza informatica, tralasciando le altre componenti e la loro interoperabilità, automatica per quanto riguarda le tecnologie e naturale per quanto concerne un solido apparato di sicurezza e intelligence nazionale.

Dall'analisi della situazione tattica si evince come il conflitto stia andando verso un innalzamento costante dei livelli di violenza che coinvolge entrambe le parti, questo ci induce a pensare, valutando anche altri casi simili, che si potrebbe assistere ad un uso di attacchi cibernetici rivolti ad influenzare la percezione interna delle ostilità da parte della popolazione così che essa sia lo strumento di pressione politica con cui Israele o la popolazione palestinese spingeranno per un cessate il fuoco. Considerata la brutalità dell'attacco condotto il 7 ottobre e considerata la necessità strategica di mantenere la popolazione il più polarizzata possibile, gli attacchi potrebbero essere condotti attraverso azioni di disinformazione e manipolazione attraverso immagini e video dalla connotazione fortemente violenta che faccia superare il limite morale utile all'accettazione dello stato di guerra e delle violenze conseguenti. Non sono da escludere ripercussioni tattiche sullo scontro in corso a causa di attacchi cibernetici, ma al tempo stesso è necessario un monitoraggio accurato e costante che solo pochi enti e organizzazioni altamente integrate e interoperanti riescono a condurre.

La complessità di una guerra intersettoriale e multi-dominio e delle eventuali implicazioni di carattere geopolitico - alla luce degli schieramenti sbilanciati da un lato per tecnologie e dall'altro in termini di capabilities – fa subito riflettere sull'eventuale escalation provocata da una risposta fisica massiva da parte di Israele nei confronti dell'Iran, oltre che in Palestina. Tale azione sancirebbe il vero e proprio inizio di una guerra anche dal profilo cyber ma dalla connotazione interoperativa per settori, tecnologie e capacità in gioco. Uno scenario che fa ben riflettere anche i paesi occidentali, nella loro connotazione pubblica e ancor più privata, sull'importanza della sicurezza tout court senza riduzione di taluni sforzi e investimenti a favore di altri.

Fonti

CyberWire. (2023). 'Cyber phases of the conflict between Israel and Hamas. Disinformation and content control. Cyberespionage and supply chain vulnerability'. CyberWire.
Disponibile qui: https://thecyberwire.com/newsletters/daily-briefing/12/195

CYFIRMA. (2023). "Israle Gaza Conflict: The cyber perspective". Cyfirma.
Disponibile qui: https://www.cyfirma.com/outofband/israel-gaza-conflict-the-cyber-perspective/

Darkowl. (2023). 'Hacktivist Groups Use Defacements in the Israel Hamas Conflict'. Darkowl.
Disponibile qui: https://www.darkowl.com/blog-content/hacktivist-groups-use-defacements-in-the-israel-hamas-conflict/

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
Disponibile qui: https://eur-lex.europa.eu/eli/dir/2022/2555

Hegel, T. (2023). 'The Israel-Hamas War |Cyber Domain State-Sponsored Activity of Interest'. SentinelOne.
Disponibile qui: https://www.sentinelone.com/labs/the-israel-hamas-war-cyber-domain-state-sponsored-activity-of-interest/

Recorded Future. (2023). Hamas Application Infrastructure Reveals Possible Overlap with TAG-63 and Iranian Threat Activity. Recorded Future by Insikt Group.
Disponibile qui: https://go.recordedfuture.com/hubfs/reports/cta-2023-1019.pdf