Aumenta la minaccia nel cyberspazio: tra capacità e vulnerabilità

La rivoluzione dell'informazione porterà alla guerra?

La storia suggerisce che le rivoluzioni militari sono più destabilizzanti quando sono in grado di creare non solo capacità ma, ancor più, vulnerabilità: è la vulnerabilità delle risorse e non la nuova capacità stessa che incentiva gli attacchi destabilizzanti.

Partendo da tale presupposto, possiamo affermare che la proliferazione della tecnologia digitale ha creato una nuova dimensione del confronto tra stati, anche attraverso il contributo di attori non statali e ha imposto la revisione della dottrina bellica così come la revisione degli strumenti delle relazioni internazionali. Come sottolinea Richard Danzig:

> *le «tecnologie digitali... sono un paradosso della sicurezza: sebbene concedano poteri senza precedenti, rendono anche gli utenti meno sicuri... la loro concentrazione di dati e potere manipolativo migliora notevolmente l'efficienza e la scala delle operazioni, ma questa concentrazione a sua volta aumenta esponenzialmente la quantità di dati che può essere sottratta o sovvertita da un attacco di successo. La complessità dell'hardware e del software crea grandi capacità che, a loro volta, generano ulteriori complessità*»[1] [2].

Da "WannaCry" al caso "Pegasus": due esempi di vulnerabilità

Quattro anni fa, nel maggio 2017, più di 200.000 computer in 150 paesi del mondo sono stati colpiti contemporaneamente da un virus *ransomware* chiamato "WannaCry", il quale, sfruttando una vulnerabilità del sistema Windows, era in grado di infettare i computer e criptare tutti i file presenti sull'hard drive. Solo pagando un riscatto (in bitcoin) era possibile ottenere la restituzione dei propri dati. Il paradosso è che Windows aveva messo a disposizione degli utenti un aggiornamento software in grado di risolvere la vulnerabilità del sistema un mese prima della diffusione del virus; ma la maggior parte degli utenti, ignorando l'aggiornamento, si è esposta ad una contaminazione su larga scala. Ma v'è di più: quattro anni dopo, ancora oltre 1.700.000 terminali risultano vulnerabili, di cui quasi 7.000 in Italia, e "Wannacry" continua a diffondersi occasionalmente. Il caso "Wannacry" è solo uno degli esempi dai quali emerge in maniera lampante come venga sottostimato il problema della sicurezza dei propri dati e, per estensione, delle reti informatiche[3].

E ancora, il cosiddetto "Progetto Pegasus". Come recentemente riportato dal *The Washington Post*, un programma militare di spyware, concesso in licenza da un'azienda israeliana ai governi per rintracciare terroristi e criminali, sarebbe invece stato utilizzato con successo in tentativi di hacking su smartphone appartenenti a giornalisti, politici, policy macker, influencer e attivisti per i diritti umani. I numeri di telefono sono apparsi su un elenco di oltre 50.000 numeri di utenti appartenenti a paesi noti per la sorveglianza dei propri cittadini; paesi che sarebbero clienti della società israeliana NSO

---

1 Danzig Richard (2014) '*Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*', Center for a New American Security.

2 Schneider Jacquelyn (2019) *The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war*, Journal of Strategic Studies, 42:6, 841-863, DOI: 10.1080/01402390.2019.1627209. In: https://doi.org/10.1080/01402390.2019.1627209.

3 Basileo Deborah (2020), *Tra Cyberterrorism e guerra dell'informazione. Scarsa consapevolezza e limiti normativi*, in #ReaCT2020, 1° rapporto sul terrorismo e il fondamentalismo in Europa, ed. START InSight.

Group, leader mondiale nello spyware privato[4]. Cosa prevede il Progetto Pegasus? Lo spyware israeliano Pegasus può infettare un dispositivo senza l'impegno o la conoscenza del bersaglio.
Si tratta di una soluzione di *intelligence* informatica leader a livello mondiale che consente alle forze dell'ordine e alle agenzie di sicurezza di accedere ed estrarre da remoto e in forma anonima i dati da qualsiasi dispositivo mobile. Fino all'inizio del 2018, i clienti della società NSO Group si affidavano principalmente a SMS e messaggi attraverso l'applicazione WhatsApp al fine di indurre gli obiettivi ad aprire un collegamento (link) malevolo funzionale ad infettare i dispositivi mobili degli utenti interessati dall'attività informativa e di controllo. Una tecnica che sfrutta il principio dell'Enhanced Social Engineering Message (ESEM), in grado di indirizzare il dispositivo mobile a un server in grado di controllare il sistema operativo e di fornire l'appropriato exploit remoto[5].

Quali le fonti della minaccia cibernetica?

Le minacce nel cyberspazio possono essere generate da almeno tre tipologie distinte di attori[6].

Il primo di questi attori è l'"hacker solitario", dove la natura solitaria in genere nasconde la presenza di più individui che operano in coordinamento tra di loro. Oggi, gli hacker solitari sono molto limitati nella loro capacità di infliggere danni di impatto strategico nazionale.

La seconda tipologia è rappresentata da gruppi non statali: "hacktivisti", criminalità organizzata, gruppi terroristici. Gruppi che hanno la capacità di infliggere danni economici sostanziali e disseminare il panico tra il pubblico – ad esempio prendendo di mira le banche o rendendo inaccessibili i siti web del governo – ma a cui manca la capacità di colpire in maniera efficace e distruttiva obiettivi di elevato valore. In genere, il livello di azioni che questi attori possono portare a compimento varia dagli attacchi *Denial of Service* alle frodi informatiche, al furto di identità. I gruppi non statali, di solito, non hanno le capacità per identificare e sfruttare le vulnerabilità dei codici complessi e per questo concentrano i loro sforzi nello sfruttamento degli errori umani, utilizzando tecniche di "*phishing*", in genere inviando *malware* tramite e-mail diffuse. I loro attacchi possono imporre danni significativi, ma non rappresentano una minaccia nazionale strategica.

La terza tipologia è costituita da attori statali che, disponendo di ampie risorse umane, scientifiche ed economiche, sono in grado di portare a compimento una campagna cibernetica multipla e a lungo termine contro un'ampia gamma di obiettivi e su una vasta area geografica. Gli attori di questo tipo sono spesso indicati come *Advanced Persistent Threats* (APT) e tendono a colpire obiettivi di alto valore attraverso azioni caratterizzate da elevati livelli di segretezza, sofisticate tecniche di raccolta di informazioni ed elevata capacità di sfruttamento delle vulnerabilità delle reti.

Gli attori statali concentrano le loro azioni sui sistemi informatici (IT) e sui database, da un lato, e attacchi ai sistemi di controllo industriale (ICS) dall'altro. Entrambe le tipologie di azioni producono effetti significativi: lo spettro della minaccia sui sistemi IT va dal semplice disturbo o fastidio (ad esempio, la modifica o la non accessibilità di siti Internet), fino a danni funzionali ed economici sufficientemente ampi da essere considerati una minaccia strategica. Tuttavia, negli ultimi anni, gli attacchi informatici hanno iniziato a rappresentare un'altra minaccia, che potrebbe essere persino più distruttiva di quella che rappresentano per l'infrastruttura IT: la minaccia di acquisizione o limitazione del controllo del processo industriale e produttivo con l'intento di provocare un pericoloso impatto cinetico[7].

---

4 Priest Dana, Timberg Craig, Mekhennet Souad (2021), *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, The Washington Post, July 18.

5 Mazoomdaar Jay (2021), *Explained: Here's how NSO Group's spyware Pegasus infects your device*, The Indian express July 22, New Delhi.

6 Tor Uri (2017) *'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence*, Journal of Strategic Studies, 40:1-2, 92-117, DOI: 10.1080/01402390.2015.1115975. In: https://doi.org/10.1080/01402390.2015.1115975

7 *Ibidem*.

Bibliografia

Basileo Deborah (2020), *Tra Cyberterrorism e guerra dell'informazione. Scarsa consapevolezza e limiti normativi*, in #ReaCT2020, 1° rapporto sul terrorismo e il fondamentalismo in Europa, ed. START InSight.

Danzig Richard (2014) '*Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*', Center for a New American Security.

Mazoomdaar Jay (2021), *Explained: Here's how NSO Group's spyware Pegasus infects your device*, The Indian express July 22, New Delhi.

Priest Dana, Timberg Craig, Mekhennet Souad (2021), *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, The Washington Post, July 18.

Schneider Jacquelyn (2019) *The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war*, Journal of Strategic Studies, 42:6, 841-863, DOI: 10.1080/01402390.2019.1627209. In: https://doi.org/10.1080/01402390.2019.1627209.

Tor Uri (2017) *'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence*, Journal of Strategic Studies, 40:1-2, 92-117, DOI: 10.1080/01402390.2015.1115975. In: https://doi.org/10.1080/01402390.2015.1115975