L'Espresso

Fino a prova contraria

Giancarlo Capozzoli

GC: Il discorso della cyber security è strettamente legato ad un discorso più generale di sicurezza e di interesse nazionale. Ecco, dottor Vitale, le chiederei di chiarirci innanzitutto questi aspetti...

AV: Il tema della sicurezza nazionale oggi ha assunto dimensioni molto più complesse rispetto al passato. Se da un lato è diminuita quella che per secoli è stata la minaccia principale, e cioè il conflitto militare, i rischi e le minacce sono aumentati enormemente, anche perché oggi al concetto di sicurezza nazionale si è sovrapposto anche il concetto di sicurezza globale.

GC: Che comunque va tenuto da conto...

AV: Assolutamente. Prendiamo ad esempio la questione ambientale, che oggi, è considerata uno dei rischi maggiori, a livello globale. Tornando alla sua domanda, dunque, dobbiamo tener ben presente che se le misure di contrasto all'aumento della temperatura globale adottate dalla comunità internazionale dovessero fallire le conseguenze avrebbero anche un impatto diretto sulla sicurezza nazionale dei singoli Paesi, perché non bisogna dimenticare che la sicurezza nazionale, oltre alla salvaguardia dell'unità e integrità territoriale e delle istituzioni democratiche deve garantire anche, sia la salvaguardia degli interessi strategici sia la sicurezza dei cittadini e dell'ambiente nel quale vivono. E' evidente quindi che le strategie di sicurezza nazionale devono ampliare il loro raggio d'azione ed includere i rischi globali. Si può anche avere un'ottima strategia di sicurezza nazionale, ma le singole risposte dei Paesi di fronte a questioni di portata globale, come i cambiamenti climatici o anche le pandemie - e lo stiamo sperimentando sulla nostra pelle - rischiano di essere inefficaci a contrastare adeguatamente questi fenomeni.

GC: Ad esempio, i progetti che riguardano le *smart cities* e le città del futuro, dovrebbero essere un argine a questo problema fondamentale, dell'ambiente, comunque...

AV: Sì, ma fino a certi livelli. Vediamo di chiarire meglio la questione. Al giorno d'oggi circa il 52% della popolazione mondiale vive nei centri urbani. In Italia e in Europa questa percentuale è del 70%. Si prevede che nel 2050 la percentuale del 70% sarà raggiunta anche dal resto della popolazione mondiale. Altro aspetto da prendere in considerazione è che l'80% circa delle transazioni economiche avviene nelle aree urbane. Ovviamente i centri urbani sono i luoghi dove si concentra il maggior consumo energetico ma anche quelli che sono maggiormente responsabili per le emissioni dannose per l'ambiente prodotte dall'uomo. Pertanto se oggi i centri urbani possono essere considerati una delle principali cause del "male" ambientale, i progetti delle *smart cities* che prevedono investimenti verso il *green* e il digitale nel prossimo futuro contribuiranno, e lo dobbiamo sperare fortemente, alla soluzione al problema stesso.

GC: Questi progetti riguardano le società occidentali, le società più avanzate, da un punto di vista sociale e tecnologico. Mi chiedo e le chiedo se è possibile applicare lo stesso criterio ad alcune realtà delle grandi metropoli dell'Africa o dell'Asia, ad esempio. Dove, voglio dire, c'è una scarsa attenzione non solo per le questioni dell'ambiente, ma proprio per una quasi totale assenza del rispetto minimo delle condizioni di vita così come la conosciamo qui da noi.

AV: La questione che pone è molto rilevante, perché comporta la consapevolezza che dovrà esserci molta più cooperazione, molta più partecipazione anche di tecnologia, anche per questi paesi in via di sviluppo, al fine di aiutarli ad uscire da queste condizioni a cui ha fatto cenno.

GC: Per quella che è stata la mia esperienza in Africa, mi sembra un progetto utopico. Voglio dire... In Senegal e in Kenya, i due paesi che ho avuto occasione di raccontare, circolano, ad esempio, le vecchie automobili che in Italia e in Europa non possono più circolare, con scarichi tossici che hanno degli effetti dannosi per la popolazione locale e per l'ambiente globale, evidentemente. Inoltre in questi paesi non mi sembra che ci sia molta attenzione per la raccolta differenziata, per usare un eufemismo...

AV: Anche se utopico, è necessario anzi direi indispensabile proprio per quello che abbiamo detto all'inizio, i rischi globali necessitano risposte globali. Noi in Italia, dobbiamo investire oltre il 60% del Recovery plan nel *green* e nel digitale. Sarà fondamentale portare avanti quei progetti interessanti di *smart cities* a cui abbiamo fatto cenno. Ma, ribadisco, se gli altri Paesi restano indietro, c'è il rischio concreto che le condizioni globali peggioreranno. Anche considerando la crescita demografica dei paesi in via di sviluppo.

GC: In che modo la crescita demografica è in stretta correlazione alla questione ambientale?
AV: Dunque, secondo un report del 2021, entro la fine del secolo la popolazione globale raggiungerà i 10 miliardi. Se si considera che agli inizi del secolo scorso la popolazione mondiale non superava i 2 miliardi possiamo renderci conto di come l'aumento di 8 miliardi di persone in 2 secoli abbia contribuito a cambiare la faccia del pianeta. Più del 70% Come accennato, vivrà nelle aree urbane, con una età media di 31 anni. Bisogna tener presente che la media europea è molto più alta di questa. Ciò significa che chi cresce di più sono proprio i paesi in via di sviluppo. Pertanto, se oggi la popolazione che vive in Africa produce un certo inquinamento, tra qualche anno, quando sarà aumentata, produrrà un maggiore inquinamento.

GC: Certo, capisco. Eppure una delle città più inquinate è Pechino...
AV: ...pur essendo la Cina un Paese con un alto sviluppo tecnologico. Ma per esperienza diretta, potrei dirle di Città del Messico o di Buonos Aires. Nel mondo ci sono molte megalopoli dove l'inquinamento è causa principale di malattie diffuse tra la popolazione anche perché si usano benzine molto più inquinanti di quelle usate in Occidente in quanto meno raffinate. L'inquinamento di queste megalopoli non resta confinato lì ma si spande per l'atmosfera e alla fine, come effetto dei cambi climatici, le conseguenze le subiamo tutti. Come detto prima, o c'è una gestione globale del problema oppure la situazione non può che peggiorare.

GC: In sostanza quel che possiamo e dobbiamo fare è strettamente legato a quello che possono fare gli altri paesi contemporaneamente. Lei ha fatto cenno ad una maggiore digitalizzazione delle nostre città, delle nostre società. Così ci avviciniamo anche ad altre questioni più tecniche. Le chiederei di evidenziarci maggiormente quella stretta correlazione tra il campo della tecnologia e della sicurezza cyber...
AV: Sono aspetti, quelli cyber e quelli tecnologici, strettamente collegati, evidentemente. Quello che credo sia un tema molto attuale è cercare di capire e di far capir quanto e perché sia importante per tutti, quella che è la sicurezza informatica.

GC: Perchè riguarda tutti noi....
AV: Esattamente. Perché, ormai tutti noi utilizziamo strumenti e tecnologie, che sono connessi ad internet. Credo che oltre il 60% della popolazione globale sia connessa ad internet, al giorno d'oggi. Se calcoliamo l'età compresa tra i 16 e i 60 anni la percentuale è anche maggiore: il 90% è connesso, e questo significa che lo siamo tutti. A parte la fascia molto avanzata con l'età e quelli al di sotto dei 14 anni. Dunque, è un problema comune. Per questo motivo, la sicurezza informatica dovrebbe essere qualcosa di cui tutti dovremmo essere a conoscenza.

GC: Lei opera proprio in una società che si occupa di sicurezza informatica.
AV: Esattamente. La società si chiama *Obsidium* cioè assedio proprio per evidenziare che la minaccia cibernetica ci circonda come quando le città venivano assediate dai nemici. E abbiamo usato una parola in latino appunto, anche per sottolineare l'italianità della nostra impresa e il fatto che i romani erano maestri nell'edificare le difese.

GC: Mi aveva accennato al fatto che *Obsidium* si sia specializzata su un aspetto specifico della sicurezza.
AV: Si, la *cyber offensive security*. Della parte offensiva della difesa, voglio dire.

GC: Ci dica qualcosa in più, per farci capire meglio. E' notizia recente che l'Italia sia uno dei cinque paesi al mondo maggiormente colpiti da attacchi cibernetici....
AV: Ci sono diversi rapporti che vengono fatti in Italia per comprendere l'andamento della minaccia informatica. Nel 2020, a livello globale, i casi noti di attacchi che hanno avuto successo e che sono stati riportati, cioè solo quelli noti, sono stati oltre 1800, con un aumento del 12% rispetto all'anno precedente. C'è da sottolineare che molte grandi società colpite da attacchi *cyber*, tendono a tenere questi attacchi nascosti, per questioni di prestigio. Anche se le regole che le nazioni stanno scrivendo, tra cui il nostro Paese, stanno comportando l'obbligo della comunicazione di avvenuto attacco alle autorità nazionali di controllo e gestione degli incidenti *cyber*. Un altro report del 2020 sottolineava che su 730 attacchi portati e resi disponibili, che hanno cioè avuto successo, sono stati esposti 20 miliardi di dati. La spesa necessaria per la *remediation*, cioè l'impegno finanziario per porre rimedio al danno, è stata di 4 milioni di dollari, circa. Questa quantità di denaro non tiene conto degli eventuali riscatti che sono stati pagati agli "attaccanti" ma è solo quello che è servito, per "tappare la falla", se mi lascia passare il termine, e ripristinare i sistemi. Se si aggiungono le somme pagate per i riscatti, ammesso che si riesca ad avere questo dato con esattezza, l'incremento finanziario è notevolissimo. Pensi solo che secondo un altro autorevole report, la quantità di denaro richiesta come riscatto nei 14 maggiori attacchi di *ramsomware* compiuti nel 2019 ammonta a 75,4 milioni di dollari. Ma tenga presente che questo rappresenta solo la punta dell'iceber, la parte sotto la superficie è molto più grande e comprende tante piccole richieste di riscatto, a volte anche di
poche centinaia di euro, per ripristinare l'uso di singoli personal computer di utenti singoli.

GC: Report importanti che ci fanno capire quanto questa tendenza sia in aumento...
AV: Bisogna porre rimedio a questo costante aumento. C'è sempre più gente connessa e ci sarà una

maggiore digitalizzazione diffusa, grazie anche alla diffusione dell'*internet of things* e di quelle *smart cities* a cui abbiamo fatto cenno prima e che diventeranno sempre più la nostra realtà.

GC: Da quel che dice, si rischia che il problema diventi più grave e più grande...
AV: E' semplice: più cose saranno connesse, maggiore sarà la digitalizzazione, più grande sarà la dipendenza delle persone dalla tecnologia e maggiore sarà l'interesse degli hacker. E' chiaro quindi che il concetto di sicurezza deve evolvere e crescere contestualmente a questi sviluppi. L'approccio che finora si è opposto, almeno a mio modo di vedere, è stato di tipo semplicistico e cioè quello di mettere su una difesa senza però tenere conto delle capacità dell'attaccante. In sostanza si è continuato ad applicare la formula del virus e dell'antivirus tanto per semplificare il concetto.

GC: Il vecchio sistema delle mura...
AV: Esattamente. Per difendersi, si costruivano le mura senza considerare le potenzialità di chi attaccava. Il problema è che se si costruisce un muro così tanto per mettere una difesa, non si può essere certi che questo muro regga all'attacco. Come detto, questa è la tendenza. In *Obsidium*, ma non siamo certamente i soli, siamo convinti che sia necessario fare una attenta analisi della minaccia stessa e poi andare a testare il muro per vedere se regge. Tra le tante mie esperienze lavorative, ho avuto modo di confrontarmi anche con il mondo dell'analisi e delle relative tecniche, e credo che quella che meglio si adatti al nostro caso sia quella che utilizzando un acronimo si definisce la *SWOT analisys: strengt, weakenesses, opportunities threat*. Una analisi che permetta di avere la conoscenza dei punti di forza, dei punti di debolezza, delle opportunità, e delle minacce.
GC: La differenza si vedrebbe subito...
AV: E' chiaro che se si costruisce solo il muro, per quanto ci si doti di un punto di forza, non si ha una analisi della minaccia e non si conoscono le armi usate da chi ci sta attaccando. Il muro posto a difesa, da un certo punto vista, potrebbe essere sovradimensionato o non dimensionato abbastanza e pertanto non reggere.

GC: L'analisi della minaccia diventa quindi fondamentale.
AV: C'è un altro aspetto da considerare. Nella *SWOT analisys* abbiamo parlato di opportunità che ci sono, delle opportunità da sfruttare che si possono cogliere se si va oltre l'aspetto semplicemente difensivo. Molti strateghi dicono che la migliore difesa è l'attacco: la *cyber offensive security* di fatto consiste nel mettere insieme gruppi di hacker etici, che stanno nel lato buono della forza e si oppongono al lato oscuro come i Jedi della famosa saga, che grazie alla perfetta conoscenza delle tecnologie e procedure utilizzate dagli hacker malevoli, sono in grado di condurre un attacco alle "mura" e verificare se reggono ovvero dove è possibile creare brecce e penetrare le difese.

GC: E' una strategia militare...
AV: In ambito militare venivano fatte le esercitazioni a partito contrapposto, proprio per questo motivo: serviva a testare la difesa eretta e provarla.

GC: Altrimenti tutte le strategie sarebbero vincenti.
AV: D'altra parte, se funzionasse il sistema della semplice difesa, il trend dei casi, a cui abbiamo fatto cenno e che abbiamo visto in crescita, dovrebbe essere in calo. Invece, come detto, c'è un aumento del 12% solo nell'ultimo anno e la tendenza è di crescita costante. Ciò nonostante oggi ci siano molte società che offrono piattaforme di difesa molto evolute e supportate anche dall'intelligenza artificiale. La questione che sfugge è che questi hacker malevoli hanno la capacità di insistere e la creatività della mente umana va oltre questi strumenti di difesa per quanto complessi. Provano e riprovano diverse procedure di attacco, finché non hanno successo nei loro intenti criminali.

GC: Il fattore umano non può essere replicato dalle macchine. E' una questione che mi fa chiedere se l'intelligence artificiale supererà il lavoro delle spie...
AV: Onestamente, io credo l'intelligenza artificiale, il *machine learning*, il *digital twin*, la robotica e le altre tecnologie collegate nel futuro potranno forse sostituire l'uomo in molte attività ma non credo che la creatività, l'immaginazione, l'imprevedibilità e la genialità dell'essere umano posso essere ricreate e duplicate virtualmente. Ad oggi il fattore umano è fondamentale e penso resterà tale ancora per molto tempo. L'intelligenza artificiale però può dare una grande mano in moltissimo settori, incluso la cyber security.

GC: Penso alla Open Source Intelligence.
AV: Oggi i dati globalmente disponibili e più o meno accessibili sono una quantità smisurata e non a caso si parla di big data. Secondo le stime, al momento ci sono circa 44 zettabyte, equivalenti a 440 miliardi di gigabyte, di dati in circolazione nel mondo digitale. Per dare qualche esempio, ogni giorno vengono effettuate circa 6,5 miliardi di ricerche di cui la metà attraverso smartphone. Vengono inviate circa 2,8 milioni di e-mail al secondo e i dati generati al giorno ammontano a 2,5 quintilioni di gigabyte di dati. Ogni minuto vengono caricate su faceebook oltre 147000 foto, scambiati su whatsup oltre 41 milioni di messaggi, caricati su instagram oltre 347.000 post, spesi on line 1 milioni di dollari. L'*Open Source Intelligence* ha la possibilità di accedere se non a tutte, alla stragrande maggioranza di queste informazioni in quanto fanno parte di quelle che vengono considerate pubblicamente disponibili. E' chiaro che le applicazioni oggi

disponibili di "*artificial intelligence*" possono dare una grande mano nel districarsi in questa messe di dati andando ad esempio a selezionare ed estrapolare le questioni più attinenti. Sono piattaforme che aiutano a velocizzare e ottimizzare la ricerca ma poi la valutazione ultima del dato spetta all'uomo; per cui sono strumenti che comunque devono essere affiancati ad analisti specifici di settore che sanno che cosa serve e sanno che istruzioni dare a chi utilizza le macchine, proprio per indirizzarli. C'è da aggiungere che la pratica dell'*Open Source Intelligence* nata in seno ai servizi di Intelligence governativa oggi si è diffusa in molte aziende, soprattutto le multinazionali, e con essa l'utilizzo di queste piattaforme.

GC: Servono a conoscere e a raccogliere informazioni. Torniamo alla *cyber offensive security*. Se ho ben capito deve essere fatta in maniera rigorosa.

AV: E' uno strumento che permette di capire le proprie vulnerabilità e che tipo di soluzione portare. Per spiegare più chiaramente: sono hacker molto talentuosi, ma etici appunto, che fanno la parte dei cattivi, che grazie a procedure molto rigorose scoprono queste falle dei sistemi testati. Procedure rigorose proprio al fine di garantire che i dati acquisiti, una volta individuata la vulnerabilità, non vengano trasmessi.

GC: Lo scopo è quello di capire, una volta riusciti a penetrare in un sistema, che tipo di danni si riesce a fare.

AV: Esattamente. E proprio perché si penetra in un sistema, quindi, bisogna garantire la massima trasparenza su come viene condotta l'attività nei confronti degli enti, siano essi governativi o privati, che decidono di attuare la *cyber offensive security* . Allo stesso tempo bisogna garantire una gestione rigorosa ed estremamente confidenziale e riservata dei dati sensibili di cui eventualmente si viene in possesso.

GC: Mi sembra' fondamentale.

AV: Se c'è una falla, non basta tapparla, perché le vulnerabilità cambiano. Con la *cyber offensive security* si può quantificare il danno che si potrebbe subire se attaccati e penetrati, si può utilizzare l'opportunità di capire che cosa potrebbe accadere se qualcuno entra nel sistema e porvi rimedio in diversi modi. Creando, ad esempio, una gestione diversa di mantenimento dei dati, creando diversi muri e una fortificazione a più strati. Lasciando i dati di poco interesse a livelli più esterni e tenendo invece i dati più sensibili al riparo.

GC: Un sistema di sicurezza maggiore e più forte.

AV: Bisogna essere onesti, neanche la *cyber offensive security* può garantire l'impenetrabilità di un sistema. Offre però sicuramente qualcosa in più rispetto al puro aspetto difensivo. Consente di cogliere l'opportunità di fare "*remediation*" a priori e senza subire danni aumentando quindi la resilienza complessiva dell'infrastruttura in esame. Questo aspetto delle opportunità è molto importante da dovere e sapere sfruttare.

GC: Come è nata la vostra società?

AV: *Obsidium* è nata nel 2018 dall'iniziativa di persone che avevano maturato una esperienza diretta nella costruzione di impianti tecnologici e quindi si erano resi conto della fragilità e vulnerabilità di queste strutture nei confronti della minaccia cibernetica. .

GC: L'alternativa sarebbe sconnetterli dal web...?

AV: Certo, però ciò comporta perdere molte funzionalità in termini di costi e efficacia ed è in controtendenza rispetto all'evoluzione tecnologica di cui abbiamo prima parlato. Comporta dei danni enormi. Tornando alla nascita di *Obsidium*, volendo fare qualcosa per cercare di ovviare al problema, i soci fondatori decisero di puntare sulla *cyber offensive security* in quanto mentre il mondo della *cyber security* era ben presidiato quello della *cyber offensive security* lo era meno.

GC: Il muro ci deve stare per poterlo testare... per intenderci....

AV: Esattamente. Ed inoltre, si è deciso di concentrarci in un ambito, in un settore di nicchia, che vuole fornire un servizio. Non si vende nessun software né hardware ma si fornisce un servizio, quello appunto finora descritto e cioè test avanzati e complessi di attacco ad una infrastruttura informatica in tutte le sue componenti, hardware, software, umana e infrastrutturale.

GC: Come detto, sono attacchi molto complessi portati da hacker buoni molto specializzati...

AV: Sì sono attività estremamente complesse che necessitano di *skill* elevati da parte delle persone ma anche procedure e tecnologie proprietarie per poterle effettuare.

GC: Sulla base di questa analisi complessa, viene studiata la vulnerabilità.

AV: Esattamente. Tanto per farle un esempio attuale, oggi una vulnerabilità è il fattore umano e una delle tecniche per aggredirlo è il *phishing*. Per spiegarci sinteticamente: si trova l'elemento debole e attraverso quello si entra nel sistema e se ne acquisisce il controllo bloccandolo. Molti dei recenti attacchi condotti con *ransomware* hanno utilizzato questa tecnica.

GC: Mi viene da riflettere su quanto questa vulnerabilità sia stata accentuata anche dallo *smart working*, dovuta alla crisi pandemica...

AV: Assolutamente. Bisogna avere anche delle regole comportamentali da seguire poi, proprio per prevenire queste vulnerabilità stesse.

GC: Mi diceva che *Obsidium* si è dedicata quasi esclusivamente a questa nicchia...

AV: E' una società che è nata in collaborazione con l'Università degli Studi di Bologna, in un connubio

virtuoso tra mondo accademico e privato, tra impresa e l'Università.

GC: Questo tipo di attività che come abbiamo sottolineato all'inizio, ancora non viene percepito come molto importante...
AV: Anche per una questione economica: istallare un meccanismo di difesa ha dei costi elevati e fare test avanzati di attacco ha costi anche maggiori. Inoltre, c'è un aspetto di diffidenza legato a questo tipo di servizio. Si dà la possibilità a qualcun altro, di esterno comunque, di entrare nel proprio sistema, esponendo tutti i propri dati.

GC: Si viene a sapere tutto quello che c'è dentro un dato sistema.
AV: Noi abbiamo cercato di dare molta importanza a questo aspetto di garanzia. Abbiamo creato un ambiente circoscritto e controllato che è stato chiamato *Castrum* nel quale viene condotta tutta l'attività. Senza addentrarmi in ulteriori dettagli, posso dire che alla protezione e segregazione dei dati dei quali eventualmente si entra in possesso è stata riservata la massima attenzione proprio perché rappresenta il punto più critico dell'attività di *cyber offensive security.*

GC: Come detto finora, si è pensati prima alla difesa del sistema.
AV: La sicurezza informatica o *cybernetica* è oggetto continuo di attenzione da parte del legislatore sia comunitario che nazionale. In Italia ci stiamo muovendo con la cosiddetta legge sul perimetro *cyber* e regolamenti associati. In ambito comunitario ci sono molte iniziative. Cito il pacchetto sulla *digital finance*, emanato lo scorso settembre dalla Commissione Europea. Cito questo pacchetto perché include la proposta di un regolamento che riguarda la resilienza informatica che tutte le entità finanziarie dei Paesi EU dovranno garantire per tutelare i cittadini che usufruiranno dei servizi offerti da queste entità. Questa proposta di regolamento include, oltre agli aspetti di *cyber security* anche aspetti di *cyber offensive security* in quanto prescrive per queste entità l'obbligo di sottoporsi regolarmente a test complessi di attacco per verificare/validare la tenuta delle difese. In sostanza la UE sta regolamentando il discorso finora fatto e riconosce l'importanza della *cyber offensive security* come strumento essenziale nell'ambito delle strategie di difesa *cyber*.

GC: ...proprio perché ci si è resi conto che non basta creare il muro intorno, ma essere certi che il muro regga. Volevo chiederle del ruolo dell'intelligence nella *cyber security*, e alcune questioni di intelligence economica che mi sembrano strettamente connesse.
AV: Ho già citato la legge sul perimetro *cyber* che è un buon passo avanti del nostro Paese in questo settore. Penso inoltre che l'iniziativa del Sottosegretario Gabrielli per la costituzione di una Agenzia nazionale Cyber sia un ulteriore passo in avanti. La minaccia cibernetica investe tutti i settori del Paese. Il ruolo dell'intelligence resta fondamentale per capire chi potrebbe condurre attacchi, contro chi potrebbero essere effettuati e con quali mezzi e tecnologie. Il resto però spetta ad altre istituzioni. Cito ad esempio il ruolo della Difesa in quanto la minaccia *cyber* è uno degli aspetti compreso nel concetto di guerra ibrida di cui si discute da qualche anno anche in ambito NATO. Parliamo quindi di attacchi *cyber* condotti da attori statuali e non nei confronti di infrastrutture critiche del Paese per indebolire la tenuta sociale o economica dello stesso in un conteso di conflittualità latente tenuta sotto la soglia di rilevamento.

GC: Il concetto di guerra ibrida nel confronto tra stati e stati e stati e attori non statuali ha fatto superare il concetto di guerra convenzionale...
AV: Nel concetto di guerra ibrida, il conflitto convenzionale è diventato uno dei tanti metodi, forse il meno probabile, che può essere utilizzato in una competizione tra Stati. Il concetto prevede che possano essere utilizzati quale mezzi di offesa la politica, la diplomazia, le leggi, soprattutto quelle internazionali, le *fake news*, gli aspetti capaci di influenzare l'opinione pubblica in particolare quelli legati alle competizioni elettorali. Come avvenuto recentemente... E, ovviamente, la guerra cibernetica è parte integrante di questo concetto.

GC: A volte in maniera più cover, altre in maniera più subdola e psicologica...
AV: C'è un detto che dice che in guerra e amore tutto e concesso. Il concetto di guerra Ibrida si adatta molto bene a questo proverbio. Restando nell'ambito del *cyber warfare, l*a minaccia maggiore è quella dello spionaggio a mezzo *cyber* per ottenere informazioni strategiche in differenti settori incluso quello economico. Sono attacchi condotti tramite *software* che hanno il compito di penetrare all'interno dei sistemi senza poter essere rilevati quindi bypassando le difese, assumono il controllo dello stesso, ricercano i dati di interesse e li esfiltrano sempre senza che i dispositivi di controllo possano rilevare l'attività anomala.

GC: Se un attacco condotto dai cybercriminali ha come fine il pagamento di un riscatto, l'obiettivo degli hacker statuali e di alcuni Stati che si sa per certo che fanno questo tipo di attività, è quello di fare queste cose senza che nessuno se ne accorga... Penso alle *back door* di alcuni dispositivi...
AV: Le *back door* non provengono dall'attività di hacker ma sono strumenti di spionaggio o *disruption "by design*". Nel senso che sono inseriti nell'apparato tecnologico sia esso hardware o software che li adotta. Ecco perché è fondamentale, e la legge sul perimetro *cyber* lo prevede, che qualsiasi software e hardware utilizzato soprattutto per quel che riguarda le infrastrutture critiche

di un paese, sia sottoposto a controlli preventivi per essere certi che sia sicuro. Questo è il compito del centro di valutazione che verrà costituito presso il Ministero dello Sviluppo Economico sulla base della legge sul cosiddetto perimetro *cyber*.

GC: Oltre alle *back door* ci sono altri tipi di attacchi?
AV: Come ho detto prima le *back door* sono un caso a parte. Quando parliamo di attacchi ci riferiamo ad attività condotta con *malware*, *worms*, *trojan*, etc, da parte di hacker che possono essere governativi o più genericamente criminali.

GC: La *cyber security offensive* si occupa anche di questo tipo di attacchi?
AV: Lo scopo della *cyber offensive security* è cercare di replicare tutti i tipi di attacco che potrebbero interessare l'infrastruttura che si testa. Nella prima fase deve essere fatta una attività che è chiamata *threat intelligence* al fine di individuare sia chi potrebbe essere l'attaccante sia gli strumenti e le metodologie che potrebbe usare per attuarlo. Pertanto, se parliamo di una organizzazione governativa o di una azienda che sviluppa tecnologia militare di alto livello, è chiaro che l'interesse potrebbe essere di una organizzazione di tipo statuale, interessata a fare uno spionaggio di tipo *cyber*. Ma allo stesso tempo, una società con utili enormi, potrebbe essere di interesse di hacker criminali.

GC: Attacchi diversi, quindi...
AV: E a seconda del soggetto che deve essere testato vanno andrebbero organizzate tipologie di attacchi completamente diversificati. Ad esempio nel primo caso andrebbe utilizzato uno *spyware* proprio per cercare di spiare senza farsene accorgere; nel secondo caso un *ransomware* che blocca e cripta tutto il sistema al fine di chiedere un riscatto per il rilascio dei dati.

GC: Sono due tecnologie diverse da mettere in campo....
AV: Non c'è un'unica maniera per fare la *cyber offensive security*: le procedure le tattiche, le metodologia e le tecnologie da utilizzare dipendono dalla natura dell'obiettivo e dalla conoscenza del potenziale attaccante. Non c'è una ricetta valida per tutti, il servizio di *cyber offensive security* va attagliato all'entità che deve essere testata ed è anche per questo che è un servizio mediamente costoso. Chi propone la stessa soluzione a tutti, eventualmente con un *software* da far girare in automatico fa un altro lavoro.