ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
NOVEMBRE 2018

INVESTIRE IN CYBERSECURITY

FABIO RUGGE

ISPI

Mentre i vincoli di bilancio della nostra manovra economica occupano le prime pagine dei media nazionali ed europei, attirare l'attenzione sul tema degli investimenti pubblici e privati nel settore della cybersecurity può forse apparire un esercizio di stile. Il tema è invece di drammatica attualità, e va affrontato con urgenza. Magari scoprendo, alla fine, che adottare oggi un lungimirante piano d'investimenti può metterci al riparo da danni ben più significativi nel medio-lungo periodo, e che abbiamo tutte le capacità e le energie per fare della sicurezza cibernetica una straordinaria opportunità di crescita per l'Italia nel mondo. A patto, certamente, di saper e voler cogliere la complessità della sfida che abbiamo dinnanzi.

Lo spazio cibernetico è divenuto troppo rilevante per la sicurezza nazionale per non essere anche l'arena nella quale questi interessi collidono tra loro. Su internet prosegue l'eterna competizione tra gli stati, con la particolarità che il dominio cibernetico è caratterizzato da un conflitto guerreggiato senza sosta e da una rilevante ambiguità quanto alla reale natura degli attori (che spesso possono anche essere non-statali), alle loro motivazioni ed alle reali finalità perseguite con gli attacchi – e dunque il rischio che la situazione "sfugga di mano" è molto più concreto. La natura asimmetrica dello spazio cibernetico, in cui l'attacco può essere fatto anonimamente e costa molto meno che difendere, assieme all'efficacia operativa delle campagne cibernetiche resa possibile dalla pervasività dei sistemi ICT, fanno ritenere che internet si confermerà, nei prossimi anni, un dominio in cui gli stati sono chiamati a proteggersi, anche militarmente, da sempre più rilevanti potenziali minacce alla propria sicurezza nazionale. Il che, a sua volta, implicherà in misura crescente la necessità di potenziare le difese a protezione delle reti più sensibili, quali ad esempio quelle che sostengono le infrastrutture critiche, che sono per la più gran parte in mano ai privati. Si tratta dunque

Counselor Fabio Rugge è Responsabile dell'Oservatorio ell'ISPI sulla Cybersecurity, in partnership con Leonardo

di una sfida organizzativa enorme, specie considerando il fatto che le opinioni pubbliche occidentali sono oramai poco inclini a considerare la sicurezza internazionale una priorità, ritenendola questione lontana. E ciò nonostante gli impegni internazionali che pure abbiamo sottoscritto nelle sedi che più ci sono care, come, ad esempio, durante il Vertice NATO di Varsavia del luglio 2016, dove, con il Cyber Defence Pledge, abbiamo assicurato che renderemo la sicurezza cibernetica nazionale una priorità, anche in termini di investimenti. Sono impegni che vanno oltre l'usuale enfasi dei Vertici, rispondendo piuttosto a un imperativo di ordine operativo: la sicurezza cibernetica, data la natura interconnessa delle reti e dei sistemi, è una catena forte tanto quanto i suoi anelli più deboli (che, peraltro, sono di norma i primi ad essere attaccati).

Più recentemente, al vertice NATO dello scorso luglio, il Ministro della Difesa Elisabetta Trenta ha proposto che gli investimenti per assicurare la resilienza cibernetica a livello nazionale siano ricompresi nel 2% del PIL che gli Alleati hanno deciso di riservare alle spese per la difesa. Nell'audizione alle Commissioni congiunte di Camera e Senato sulle linee programmatiche del suo Dicastero, poi, il Ministro Trenta ha confermato che la resilienza rappresenta una delle due priorità che informeranno l'azione del suo Dicastero, l'altra essendo il perseguimento di capacità duali, ossia di soluzioni che, pur ancorate alle competenze istituzionali e alle capacità operative proprie della Difesa, consentono ricadute positive sul Paese da un punto di vista tecnologico, industriale e, più in generale, di sicurezza nazionale. La proposta italiana parte da una constatazione incontrovertibile: così come evolve la minaccia alla nostra sicurezza nazionale ed evolvono le nostre dottrine e capacità per farvi fronte, nello stesso senso è ragionevole riflettere su come sia opportuno valorizzare meglio il ruolo che gli investimenti pubblici, magari assieme ad oculate politiche di sostegno agli investimenti privati, nella misura in cui essi contribuiscono ad innalzare la resilienza del Paese e, di riflesso, la nostra capacità di essere membri attivi (piuttosto che weakest links) dell'Alleanza.

Ma la sicurezza cibernetica non è solo un'essenziale dimensione dei futuri conflitti internazionali ed una delle componenti principali della supremazia tecnologica – che pure rappresenta forse uno dei fattori che più abilitano la sovranità nel XXI secolo. La minaccia cibernetica agisce anche al di là del classico scontro di potenza internazionale e ha lo stesso effetto, osservava il Presidente dell'ISPI, Amb. Giampiero Massolo, del monossido di carbonio: non la si percepisce ma esiste, e porta ad inesorabile asfissia. Lo si comprende bene se si osserva quanto tempo è necessario perché le aziende rilevino (magari grazie al supporto delle preposte autorità) un attacco ai loro sistemi ICT. Sebbene essi si siano significativamente accorciati negli ultimi anni[1], rimane il fatto che virtualmente tutti questi incidenti informatici hanno offerto all'attaccante il tempo necessario per esfiltrare dalle reti aziendali ogni dato potenzialmente sensibile. Anche senza dover attendere una "Caporetto 2.0" o un "11 settembre cibernetico", occorre quindi, da subito, porre attenzione a quanto già accade nel tessuto produttivo italiano. Ne fa stato da anni, del resto, la Relazione annuale al Parlamento del Sistema di Informazione per la Sicurezza della Repubblica, come pure non mancano le continue azioni di sensibilizzazione che provengo dalla Polizia Postale, dal mondo dell'associazionismo e da quello della ricerca. Per un Paese come l'Italia, che fa dell'innovazione la pietra angolare della propria crescita, e per la quale il furto del know-how scientifico, tecnologico ed aziendale comporta un danno diretto e grave alla capacità di rimanere competitivi nei mercati internazionali, il danno potenziale è incalcolabile. Specie se si considera che le piccole-medie imprese, vera spina dorsale della

nostra economia e dove pure risiede il 30% circa degli investimenti nazionali in ricerca e sviluppo[2], sono troppo spesso poco consapevoli dell'effettivo valore dei dati da esse gestiti e della reale minaccia spionistica che incombe su di loro da oltre frontiera (sebbene, magari, al soldo del competitor che ha gli stabilimenti produttivi di rimpetto), oppure ritengono troppo caro l'accedere a servizi di cybersecurity affidabili. Lo spiega bene Alberto Tripi nel suo contributo, quando ricorda che ben l'80% degli investimenti privati in Italia nel settore della sicurezza cibernetica avviene in seno alle grandi aziende. Le previsioni in materia di sicurezza cibernetica introdotte con la direttiva NIS e con il regolamento GDPR rappresentano importanti stimoli per indurre anche le medio-piccole aziende a porre attenzione alla protezione delle loro reti e dei dati che esse custodiscono, ma certamente non possiamo attenderci che la semplice istituzione di quadri regolamentari e l'associato rischio di sanzioni siano da soli sufficienti a proporzionare le difese del sistema Paese alla gravità della minaccia. Né è verosimile auspicare che le PMI italiane possano essere capillarmente protette in modo permanente da un "perimetro nazionale" che nello spazio cibernetico, semplicemente, non può esistere, nonostante i migliori sforzi dei nostri Servizi d'intelligence e l'azione repressiva della pur efficientissima Polizia Postale.

Anche dall'angolo visuale degli interessi privati in gioco, dunque, la sfida dinnanzi a noi è enorme. Ed è innanzitutto culturale, perché a mutare deve essere, in primo luogo, il modo in cui in azienda si pensa alla protezione delle reti e dei sistemi ICT, dimostrandosi all'altezza della rivoluzione organizzativa in atto: non possono esservi scuse per il management che fallisca nel promuovere, top-down, il necessario cambiamento su questi temi. Il vertice aziendale deve attestarsi quale centro di comando e controllo delle reti aziendali e delle informazioni strategiche, oltre che il primario custode della riservatezza delle comunicazioni ed il responsabile dell'integrità dei sistemi ICT. Una nuova sensibilità è necessaria anche nelle politiche del personale, e non solo nel senso che è necessario diffondere, a tutti i livelli, consapevolezza circa la minaccia cibernetica, oltre che a promuovere la scrupolosa aderenza alle policies di sicurezza aziendali (cyber hygiene & compliancy). Più critico – e difficile – appare infatti far sì che alle figure più direttamente coinvolte con la sicurezza cibernetica venga riconosciuto un ruolo adeguatoal rilievo che esse assumono, nel nuovo contesto di sicurezza, per la vita dell'azienda, e venga riservato un canale di comunicazione diretto con il vertice aziendale, rendendo così possibile anche un sostanziale reverse-mentoring, che non può prescindere dall'avvio di un diverso approccio, in azienda, alla gestione dei rapporti inter-generazionali. Si tratta di un aspetto critico, perché il brain drain nel settore della cybersecurity ha raggiunto una soglia allarmante, visto che, a fronte di una domanda di esperti in cybersecurity in assoluta esplosione, i brillantissimi giovani che riusciamo a formare lasciano troppo spesso il Paese perché attratti da salari certamente più alti, oltre che da responsabilità e status decisamente più rilevanti. Ed è infine imperativo fare squadra, perché questa è l'unica strategia sensata in uno scenario strategico asimmetrico quale quello cibernetico, dove diventa fondamentale ragionare in una logica di sistema, e dove occorre quindi imparare che il mio competitor sul mercato può e deve anche essere il mio alleato nell'*early warning*, nell'info-sharing e nella gestione delle emergenze.

Per far tutto questo, il Paese nel suo complesso – e ciascuno per la sua parte – è chiamato a concorrere alla messa in opera di un piano straordinario di investimenti strategici per la sicurezza cibernetica, non solo economici, ma anche – e, forse, primariamente – sociali e progettuali. Con

questo quinto dossier dell'Osservatorio sulla Cybersecurity dell'ISPI proviamo a darne conto, cercando, come di consueto, di presentare il tema da diverse prospettive, quali quelle relative agli investimenti sia pubblici (nel settore della difesa e della sicurezza nazionale, ma anche a sostegno della digital economy e degli investimenti privati) sia di aziende grandi e medio-piccole, di quelli a specifica protezione delle infrastrutture critiche nazionali o piuttosto a beneficio (magari secondo una logica di *dual-use*) dell'intero sistema Paese, degli investimenti (ancora: non solo economici) nella formazione e nelle politiche nazionali di retention dei talenti. Il tema della sicurezza cibernetica interseca trasversalmente praticamente tutti gli ambiti della vita civile, politica, strategico-militare ed economica, e va affrontato dunque secondo una logica olistica e centripeta. Riuscire ad imprimere questa logica rappresenta una sfida il cui esito definirà nel profondo il futuro del nostro sistema Paese.

1. Secondo uno studio di PWC,circa l'89% delle aziende ritiene che i propri team di sicurezza interna siano riusciti a rilevare le violazioni nel giro di un mese, mentre lo scorso anno questa tempistica è stata raggiunta solo dal 32%. Quest'anno, il 55% delle aziende ha impiegato una settimana o addirittura meno per individuare una violazione, rispetto al 10% del 2017.
2. .Dati Istat 2016.
3. https://www.ispionline.it/it/ricerca/cybersecurity