IL FOGLIO – 1° APRILE 2022

La nuova architettura della sicurezza globale è fatta così

Discorso di Jeremy Fleming tenuto il 31 marzo 2022 in un incontro a porte chiuse all'Università nazionale dell'Australia

Il mondo è cambiato dalla mia ultima visita qui a Canberra: la pandemia, il dominio della tecnologia e dell'informatica, il ruolo della Cina, la fine della campagna in Afghanistan e ora l'invasione di Vladimir Putin in Ucraina. Ognuno di questi potrebbe essere visto come un cambiamento storico. Presi tutti insieme, si sommano a un periodo di sconvolgimento generazionale. Le conseguenze economiche, sociali e geopolitiche si stanno ancora manifestando – e lo faranno per decenni a venire. E questo accade anche per il mondo della sicurezza nazionale, dove le minacce che affrontiamo e i modi che scegliamo per contenerle stanno cambiando rapidamente. Si parla molto della necessità di progettare una nuova architettura di sicurezza globale. La mia opinione è che tutto ciò stia già accadendo. E' già tutto diverso. E so che lo sentite qui. L'annuncio di questa settimana di importanti aumenti nelle spese per difesa e l'intelligence dimostra che anche l'Australia si trova in questa nuova realtà.

Che ci crediate o no, sono passati solo 36 giorni da quando Vladimir Putin ha lanciato un attacco unprovoked, non giustificato e premeditato in Ucraina. E' stato scioccante sotto ogni punto di vista, ma non è stato sorprendente. Abbiamo visto questa strategia, abbiamo visto costruirsi il quadro dell'intelligence, e ora vediamo che Putin cerca di portare avanti il suo piano. Ma sta fallendo. E il suo piano B è stato ancor più barbaro contro i civili e le città. Chiaramente, gioca secondo regole morali e legali diverse dalle nostre. Troppi ucraini e troppi russi hanno già perso la vita. E al di là dei bilanci, molti, molti altri hanno perso la loro vita. Le Nazioni Unite stimano che in poco più di un mese, più di dieci milioni di persone sono già fuggite dalle loro case. E' una crisi umanitaria che non sarebbe mai dovuta accadere. E non è ancora finita.

Detto questo, sembra sempre di più che Putin abbia valutato male la situazione. E' chiaro che ha sottovalutato la resistenza del popolo ucraino. Ha sottovalutato anche la forza della coalizione contro le sue azioni. Ha sottovalutato le conseguenze economiche delle sanzioni. Ha invece sopravvalutato la capacità dei suoi militari di assicurarsi una rapida vittoria. Abbiamo visto i soldati russi – a corto di armi e di morale – rifiutarsi di eseguire gli ordini, sabotare il proprio equipaggiamento e persino abbattere accidentalmente i propri aerei. E anche se crediamo che i consiglieri di Putin abbiano paura di dirgli la verità, quello che sta succedendo e la portata di questi errori di valutazione devono essere chiarissimi al regime. Questa settimana, il ministero della Difesa russo ha dichiarato che ridurrà drasticamente le operazioni

di combattimento intorno a Kyiv e in una città del nord. Sembrava che fossero stati costretti a fare un cambiamento significativo. Ma poi hanno continuato a lanciare attacchi. Messaggi contrastanti o disinformazione deliberata – dovremo vedere come si svilupperà.

Il tutto si aggiunge all'errore di calcolo strategico: i nostri leader ci avevano avvertito su cosa avrebbe fatto Putin. E' diventata la sua guerra personale, il prezzo lo pagano persone innocenti in Ucraina e, sempre di più, anche i russi. La grande ironia è, naturalmente, che attraverso le sue azioni, Putin ha portato su di sé esattamente ciò che stava cercando di evitare – un'Ucraina con un rinnovato senso nazionalista, una Nato che è più unita che mai, e una coalizione globale di nazioni che condanna le sue azioni. Dopo poco più di un mese, è troppo presto per definire con sicurezza tutte le implicazioni di questa crisi, ma ho intenzione di delineare alcuni aspetti che mi colpiscono davvero.

Inizierò con l'importanza del fronte dell'informazione. La Russia ha scritto il manuale della guerra ibrida. I media statali, i media online e gli agenti di influenza sono tutti utilizzati per confondere le motivazioni e giustificare le azioni militari. Li abbiamo visti usare questo metodo in Siria e in molti altri teatri. Il loro obiettivo è promuovere la disinformazione, è seminare sfiducia nelle prove ed è amplificare le false narrazioni. E' anche quello di assicurarsi che il quadro reale di ciò che sta accadendo non venga esposto dentro la Russia. Ed è lì che si sta conducendo la più pericolosa guerra di disinformazione. Sappiamo che la campagna di Putin è afflitta da problemi – morale basso, default logistici e un alto numero di vittime russe. La catena di comando e controllo è nel caos. Abbiamo visto Putin mentire al suo stesso popolo nel tentativo di nascondere l'incompetenza militare. E tutto questo significa che cerca un controllo brutale dei media e dell'accesso a internet, cerca la repressione delle voci dell'opposizione, e sta facendo forti investimenti nella propaganda e nei servizi segreti. Ma anche in questo caso, è chiaro che Putin abbia sbagliato i calcoli. L'operazione di informazione del presidente Zelensky ha dimostrato di essere estremamente efficace. E' agile, multi-piattaforma, multimediale e adeguata ai diversi pubblici. Basta guardare il modo in cui la bandiera dell'Ucraina – un campo di girasoli sotto un cielo azzurro – e vederla sventolare ovunque, anche fuori dal Gchq, per capire quanto bene sia arrivato il messaggio. Ed è un messaggio sostenuto da campagne di informazione in tutto il mondo. Nel Regno Unito, si concentra su una nuova cellula d'informazione governativa che identifica e contrasta la disinformazione del Cremlino rivolta al pubblico britannico e internazionale. Riunisce le competenze di tutto il governo per sfidare le false narrazioni. Si occupa di fatti, non di falsità, assicurandosi che la realtà sia raccontata correttamente. E sempre più spesso, molte di queste "verità" provengono dall'intelligence. E' già una caratteristica notevole di questo conflitto quanto l'intelligence sia stata declassificata rapidamente per anticipare le azioni di Putin. Dagli

avvertimenti sulla guerra, all'intelligence sulle operazioni false flag progettate per fornire una falsa premessa all'invasione. E più recentemente, ai piani russi per rivendicare falsamente l'uso ucraino di armi chimiche vietate. Su questo e molti altri argomenti, vengono rilasciate informazioni segrete per assicurarsi che la verità venga ascoltata. A questo ritmo e su questa scala, è davvero senza precedenti. A mio avviso, vale la pena raccogliere informazioni solo se le usiamo, quindi accolgo senza riserve questo nuovo sviluppo. Naturalmente, altri aspetti di questo confronto si manifestano nel cyberspazio. Ci sono stati commenti che esprimevano sorpresa per il fatto che i russi non hanno fatto un grande attacco informatico. Penso che molto di questo non centri il punto. Mentre alcune persone cercano "Pearl Harbour" informatici, non abbiamo mai capito che un attacco informatico catastrofico fosse centrale nella la loro dottrina militare. Questo non vuol dire che non abbiamo visto l'informatica in questo conflitto. L'abbiamo vista, e molto.

Attraverso il National Cyber Security Centre, che è parte del Gchq, abbiamo visto l'intento costante da parte della Russia di interrompere il governo ucraino e i sistemi militari. Abbiamo visto ciò che sembra una certa fuoriuscita di attività che colpisce i paesi circostanti. E abbiamo sicuramente visto indicazioni che suggeriscono che gli attori informatici russi stiano cercando obiettivi nei paesi che si oppongono alle loro azioni. Quindi, così come rendiamo omaggio alle azioni coraggiose dell'esercito ucraino, dovremmo rendere omaggio anche alla sicurezza informatica ucraina. Noi e altri alleati continueremo a sostenerli nel rafforzare le loro difese. E a casa, stiamo facendo tutto il possibile per assicurarci che le imprese e il governo seguano con urgenza i piani per migliorare i livelli di base della resilienza informatica.

Ora la mia terza osservazione su questo conflitto è la misura in cui gli attori non statali sono coinvolti e hanno voce in capitolo nel suo esito. Alcuni di questi sono sui campi di battaglia in Ucraina. E' chiaro che la Russia stia usando mercenari e combattenti stranieri per aumentare le sue forze. Ciò include il gruppo Wagner, attivo in Ucraina dall'annessione illegale della Crimea da parte della Russia nel 2014. Il gruppo lavora come un ramo ombra dell'esercito russo, fornendo una copertura per le operazioni più rischiose. Recentemente, abbiamo visto come Wagner stia cercando di cambiare marcia. Abbiamo capito che il gruppo è ora pronto a inviare un gran numero di personale in Ucraina per combattere a fianco dei russi. Stanno cercando di trasferire forze da altri conflitti e di reclutare nuovi combattenti per rafforzarsi. E' probabile che questi soldati vengano usati come carne da cannone per cercare di limitare le perdite militari russe. Ma non è solo nella sfera militare che vediamo l'influenza e il potenziale di altri attori. Abbiamo visto gruppi di cyber hacking e ransomware che giurano fedeltà a entrambe le parti. Abbiamo visto aziende di tutto il mondo prendere le distanze dall'economia russa. Abbiamo visto i fornitori di tecnologia farsi avanti per assicurarsi che l'Ucraina possa

rimanere connessa, o per affrontare la disinformazione. Tutto questo sta rendendo lo spazio molto complicato, e in qualche modo, ben oltre il controllo dei governi. E' un altro promemoria dell'interconnessione del mondo di oggi. E poiché nessuna singola entità detiene la soluzione intera, evidenzia la necessità che le istituzioni globali lavorino efficacemente in coalizione.

L'aggressione di Putin ha certamente galvanizzato la Nato. La guerra ha innescato una risposta internazionale senza precedenti: 141 paesi l'hanno condannata all'Assemblea generale delle Nazioni Unite. In tutta Europa i paesi stanno ribaltando approcci decennali alla loro politica di difesa; e stanno anche investendo di più. E più lontano, anche in questa regione, paesi come l'Australia e il Giappone si stanno allineando. Sta anche mostrando, in netto rilievo, quei paesi che scelgono di sostenere Putin o di astenersi dal fare una scelta. E queste scelte influenzeranno l'ordine globale e la nostra sicurezza nazionale per i decenni a venire. E naturalmente, qui in questa regione, le questioni più preoccupanti riguardano le scelte che la Cina fa mentre pensa ai suoi interessi a lungo termine.

Ora, la posizione della Russia su questo è chiara. Ha fatto la scelta strategica di allinearsi con la Cina, poiché la Cina è più potente ed è in diretta opposizione agli Stati Uniti. Nella crisi attuale, la Russia vede la Cina come un fornitore di armi, come un fornitore di tecnologia, come un mercato per i suoi idrocarburi e come un mezzo per aggirare le sanzioni. Sappiamo che entrambi i presidenti, Xi e Putin, danno grande valore alle loro relazioni personali. Ma il calcolo di Xi è più sfumato. Non ha condannato pubblicamente l'invasione, forse pensando che questo lo possa aiutare nel suo scontro con gli Stati Uniti. E, con un occhio alla riconquista di Taiwan, la Cina non vuole fare nulla che possa limitare la propria capacità di muoversi in futuro. E' anche possibile che la Cina creda che la Russia fornirà ulteriore slancio e sostegno ai suoi mercati digitali e ai suoi piani tecnologici. Stiamo vedendo che la Cina coglie l'opportunità di acquistare idrocarburi a buon mercato dalla Russia in questo momento, per soddisfare anche le proprie esigenze.

Ma ci sono rischi per entrambi i paesi (forse più per la Cina) nell'essere allineati in modo tanto stretto. La Russia capisce che, a lungo termine, la Cina diventerà sempre più forte militarmente ed economicamente. Alcuni dei loro interessi sono in conflitto; la Russia potrebbe essere esclusa dall'equazione. Ed è altrettanto chiaro che una Cina che vuole stabilire le regole di una nuova governance globale non si trova del tutto a suo agio in un'alleanza con un regime che volontariamente e illegalmente le ignora tutte. Questo possiamo metterlo bene a fuoco quando pensiamo al futuro degli ecosistemi tecnologici e alle norme e alla governance che guidano il loro utilizzo. E per me, questo riguarda tanto i valori quanto la tecnologia, ed entrambi sono vitali per il vantaggio competitivo di un paese: ecco perché è sempre più al centro della competizione geopolitica.

Storicamente, lo sviluppo della tecnologia era in gran parte guidato e posseduto dall'occidente. I valori condivisi tra le nazioni coinvolte facevano sì che gli standard industriali per le tecnologie emergenti tendessero a essere globali. L'investimento nella tecnologia portava status, ricchezza e sicurezza. Oggi siamo in un'epoca diversa: la leadership tecnologica si sta spostando verso est, sta causando un conflitto di interessi, di valori, e sono in gioco sia la prosperità sia la sicurezza. Ora, ovviamente la Cina è un player sofisticato nel cyberspazio. Ha l'ambizione crescente di proiettare la propria influenza oltre i suoi confini e un comprovato interesse per i nostri segreti commerciali. Ha anche una visione concorrente riguardo al futuro del cyberspazio ed è sempre più influente nel dibattito sulle regole e gli standard internazionali. La Cina sta usando tutti gli elementi del potere statale per controllare, influenzare il design e dominare la tecnologia, il cyber e la fibra.

Se non si fa nulla, è sempre più evidente che le tecnologie chiave da cui tutti dipendiamo per la prosperità e la sicurezza non saranno plasmate e controllate dall'occidente in futuro. Se non agiamo – con i nostri alleati, con i nostri partner e con il settore privato – i valori antidemocratici diventeranno di default per vaste porzioni di tecnologia futura e per gli standard che la governano. Non c'è dubbio che i paesi democratici sono in un momento di resa dei conti.

Ho affrontato temi piuttosto grandi, con una grande posta in gioco. Dobbiamo fare un passo avanti, e ci sono molti modi per farlo, ma mi sembra che due cose siano particolarmente importanti. La prima è che dobbiamo trovare nuovi modi per collaborare e cooperare con i nostri partner. Per chi di noi si occupa della sicurezza nazionale, si tratta di garantire che le relazioni esistenti siano solide, che i Five Eyes, la Nato e in questa regione l'Asean siano solidi. E si tratta di lavorare con le imprese in modi nuovi e davvero collaborativi. Per farlo, dobbiamo assicurarci che la nostra controfferta – agli stati che non hanno ancora deciso da che parte stare – sia persuasiva e coerente. Troppo spesso non lo è. E il secondo è che in qualsiasi cosa facciamo, dobbiamo assicurarci di rimanere fedeli ai nostri valori, quelli che hanno fatto il successo dei nostri sistemi e delle nostre democrazie e che lo faranno anche in futuro. Sta emergendo una nuova architettura della sicurezza globale: questo cambiamento richiederà decenni per essere definito. Ma quello su cui posso essere chiaro ora è che il modo in cui affrontiamo queste sfide sarà importante quanto la nostra risposta. E tutti noi in questa stanza oggi dobbiamo fare la nostra parte nel darle un seguito.