Minaccia cyber: le elezioni al Parlamento Europeo

A cura di Giulio Terzi di Sant'Agata

Global Committee for the Rule of Law “Marco Pannella”

Gennaio 2019

Natura della minaccia

Negli ultimi quattro anni sono esponenzialmente aumentate le interferenze via Internet nel dibattito politico e nella formazione del consenso da parte di "attori esterni" all'America e all'Unione Europea. Il fenomeno è stato oggetto di misure preventive, di deterrenza e contrasto negli Stati Uniti e in diversi Paesi dell'Unione. Esso mina le fondamenta stesse della Democrazia rappresentativa basata su un'informazione libera. I fatti sono gravi e pienamente documentati ormai da anni. Si tratta di una realtà che coinvolge non solo i "social media" e l'intelligence. Si riflette anche sull'informazione del pubblico, sui blog e sui media tradizionali. Vengono così sovvertiti presupposti sui quali si basano tutte le consultazioni elettorali. Allo stesso tempo le acquisizioni massicce di dati tramite le piattaforme costituiscono per "attori statuali" e organizzazioni criminali un incentivo – economico, oltre che politico – ad intensificare ulteriormente il loro modus operandi. Le grandi imprese informatiche hanno per troppo tempo avuto un atteggiamento ambiguo, a secondo delle loro convenienze e modelli di business incentrati sull'illimitato aumento dei loro utenti, dei ricavi pubblicitari, delle capacità di lobbying.

In vista delle consultazioni del prossimo Maggio l'elettorato europeo si sta mostrando sempre più consapevole e preoccupato. Un recente sondaggio della Commissione Europea su 27.000 cittadini nei diversi Stati membri ha rivelato che circa i due terzi degli intervistati sono preoccupati da possibili attacchi cyber intesi a manipolare "in modo coperto" le elezioni europee. I britannici più degli altri, e questo appare significativo alla luce del riflusso che si sta manifestando sulla Brexit. Il 67% si è detto altresì preoccupato dall'utilizzo dei dati personali per "mirare" il messaggio politico, con riferimento allo scandalo Facebook, Twitter, Cambridge Analytica che avrebbe influito sulle presidenziali americane e sul Referendum Brexit. L'ampia maggioranza ha convenuto che il modo migliore per affrontare il problema è: trasparenza nei "social media"; pubblicazione di nomi e riferimenti

degli inserzionisti; diritto di replica ai candidati nelle elezioni politiche; estensione ai "social" dell'obbligo del silenzio nella immediata fase pre elettorale, come già avviene per i media tradizionali. In Italia gli organismi preposti alla sicurezza dello Stato si sono espressi da tempo con molta chiarezza.

La Relazione 2017 al Parlamento sulla politica dell'informazione per la Sicurezza offre un quadro della minaccia cibernetica per il nostro paese. Riferendosi agli attacchi verificatisi in quell'anno il Documento sottolinea le "campagne di influenza che, prendendo avvio dalla diffusione online di informazioni trafugate mediante attacchi cyber, hanno mirato a condizionare l'orientamento delle opinioni pubbliche, specie quando sono state chiamate alle urne. In particolare, tali campagne hanno dimostrato di saper sfruttare, con l'impiego di tecniche sofisticate e di ingenti risorse finanziarie, sia gli attributi fondanti delle democrazie liberali (dalle libertà civili agli strumenti tecnologici più avanzati), sia le divisioni politiche, economiche e sociali dei contesti d'interesse, con l'obiettivo di introdurre, all'interno degli stessi, elementi di destabilizzazione e di minarne la coesione. La nostra intelligence ha dato quindi una valutazione precisa della minaccia e opera per neutralizzarla.

Il contesto internazionale

Nel Luglio 2016 la campagna presidenziale americana stava imboccando lo sprint finale. Hillary Clinton era data in netto vantaggio su Trump. Leaders democratici con ottime relazioni con il mondo newyorkese di Trump manifestavano tuttavia, in privato, le loro forti inquietudini. Non solo per le sue tesi "anti-sistema", "l'America First", l'eredità dei Tea Parties, le durissime critiche all'Amministrazione Obama, i cambiamenti drastici di linea che Trump voleva su Medio Oriente, Russia, Iran e Cina. I democratici segnalavano i rapporti tra l'Organizzazione Trump e la Russia. Queste preoccupazioni esistevano in campo democratico ben da prima della pubblicazione da parte di Wikileaks dell'immensa quantità di documenti, mail e dati sottratti alla National Convention Democratica nel Luglio 2016.

Quell'attacco era stato preceduto nel 2015 da un'intensa attività di disinformazione russa sulla rete con migliaia di false identità e iniziative coordinate da un'unica strategia. FBI, inchiesta Mueller, ricerche effettuate – assai tardivamente – da Twitter, Facebook, Instagram e altre piattaforme accertavano che 180 milioni di americani erano stati oggetto di martellanti fake news e disinformazione di provenienza russa. Washington adottava in fasi successive sanzioni contro persone e organizzazioni russe. Nel 2018, all'approssimarsi delle elezioni di medio termine, il Presidente Trump denunciava anche delle attività di hackers cinesi contro candidati Repubblicani sfavorevoli a Pechino nella controversia commerciale con la Cina.

Il "Russia Gate" ha in ogni caso dominato il dibattito politico sin dal primo giorno di Trump alla Casa Bianca. Con polemiche incessanti sulla reale natura del rapporto dell'Amministrazione con la Russia. Se dubbi esistono su un'infinità di questioni che riguardano tale rapporto, il sospetto che Mosca abbia interferito pesantemente attraverso la rete nella politica interna americana è diventato da tempo una comprovata certezza. La Casa Bianca ha dovuto convalidare le decisioni del Congresso di sanzionare entità e agenti russi. Il Procuratore Speciale Mueller prosegue per ora l'inchiesta nonostante i cambiamenti voluti dal Presidente al Ministero della Giustizia prima che una nuova maggioranza democratica si insediasse alla House of Representatives.

L'inchiesta Mueller si è estesa a filiere che coinvolgono il genero di Trump, Jared Kushner, il figlio Donald Trump jr., l'ex Consigliere della Sicurezza Nazionale, Michael Flynn, per aver mentito al Congresso o all'FBI circa loro incontri con interlocutori russi. Mueller ha incriminato altre 30 persone, 4 del Team Presidenziale e dell'Amministrazione, 25 cittadini russi e 3 società di Mosca. Quanto accaduto negli Stati Uniti preoccupa molto i Governi europei. Pesanti interferenze russe si sono infatti prodotte nello stesso arco di tempo anche in Europa: per rafforzare la mano di forze politiche e segmenti di opinione pubblica inclini a collaborare con la Russia su una pluralità di fronti: indebolire Nato e

Unione Europea, lasciar campo libero a Mosca in Ucraina, nei "conflitti congelati" e nel Mediterraneo e in Medio Oriente. L'allerta in Europaè particolarmente elevata da almeno 3 anni.

Le lezioni apprese e il loro valore per l'UE

Un recente rapporto di Carnegie Endowment rilevava che *"l'aggressiva campagna della Russia nel prendere di mira le elezioni americane 2016 ha rivelato non soltanto la portata nella quale le tecnologie di informazione e comunicazione sono state utilizzate per minare il processo democratico, ma ha anche dimostrato la debolezza delle misure di protezione. Il Governo Statunitense è stato preso alla sprovvista dimostrando ancora una volta che le interferenze presentano un crescente rischio globale..."* in particolare per l'Europa.

Era così naturale che in preparazione delle diverse elezioni del 2017 i Governi europei cercassero di premunirsi contro le intrusioni cyber, specialmente della Russia. Un'analisi di quanto avvenuto in Germania, Francia, Olanda e Gran Bretagna consente di prevedere l'ulteriore intensificarsi della minaccia cyber e la direzione che essa prenderà nelle settimane che precedono le elezioni europee di Maggio. Il loro esito costituisce una sfida di grande importanza per Mosca. I rapporti tra il Cremlino e alcune forze politiche e di opinione in Europa sono consolidati e vanno ben al di là del "normale" attività dialogo politico. Le "lezioni apprese" in America e in Europa non possono che essere il punto di partenza.

In occasione delle elezioni olandesi del marzo 2017, L'Aia aveva messo a punto un sistema di protezione molto elevato: non soltanto perché allertate dalle vicende negli Stati Uniti, ma anche in ragione di attacchi già subiti dal Dutch Safety Board's nell'ottobre 2015 (ad opera degli hackers russi diAPT 28 e Fancy Bear) e poi della disinformazione russa – al tempo del referendum olandese del 2016 – sull'accordo commerciale UE-Ucraina e dell'abbattimento del volo MH17 da parte di ribelli filo-

russi in Ucraina orientale. Ma è stata la campagna contro l'accordo commerciale UE-Ucraina a rivelare una sua peculiare sofisticazione. Mosca è ricorsa a un gruppo di espatriati ucraini filo-russi in Olanda. L'intelligence dell'Aia ha documentato numerose "operazioni di influenza" russe nei confronti di ambienti economici, politici, scientifici, della difesa; con attacchi cyber, reclutamento di operatori, spionaggio, diffusione di false notizie e manipolazioni dell'opinione pubblica.

I Russi – dichiaravano pubblicamente fonti dell'Intelligence olandese – avevano persistentemente cercato di "penetrare il computer delle Agenzie di Governo e delle imprese". Di conseguenza il Governo dell'Aia decideva di affrontare le elezioni del marzo 2017 con misure incisive. Per le operazioni di voto eliminava i conteggi elettronici delle schede. Avviava una collaborazione con Facebook per un efficace "fact checking". A elezioni concluse, l'intelligence olandese – AIVD – riteneva di esser riuscita a evitare "un'influenza sostanziale" della Russia anche se una certa diffusione di informazioni false di origine russa era comunque avvenuta.

Il quadro è stato diverso in Francia. Nonostante gli sforzi dell'apparato di sicurezza per proteggere l'elezione presidenziale l'interferenza russa ha mirato soprattutto a indebolire EnMarche e il Presidente Macron. Azione che proseguirebbe - secondo studi effettuati dal Times di Londra su alcune piattaforme social-sostenendo i "Gilets Jaunes". SputnikFrance e Russia Today – RTFrance – sono stati estremamente attivi su Twitter nel periodo che ha preceduto l'elezione presidenziale. Analisi sulle loro coperture della campagna eseguite dall'Atlantic Council Digital Forensics Research Lab- rivelano un fortissimo pregiudizio contro Macron. Altre ricerche – di Reputation Lab, specializzato nel monitoraggio dei social media – hanno stimato che i servizi di RTFrance sulle presidenziali sono stati seguiti da 145.000 persone. Tra le teorie cospiratorie diffuse dalla rete l'affermazione che Macron fosse un agente per gli interessi finanziari americani, e gay.

La diffusione di tali storie era poi moltiplicata da un'attivissima rete di "trolls" automatizzati (bots) per radicare sulla rete tesi filorusse e antieuropeiste. Marine Le Pen ne beneficiava ma non era la sola. Vi erano altri candidati filo russi che utilizzavano notizie come quella pubblicata da una società di consulenza a Mosca di Fillon in vantaggio nella corsa elettorale nonostante le vicende giudiziarie che lo riguardavano. La "fake news" si basava su un asserito – ma inesistente – sondaggio eseguito da Sputnik. La Commissione Elettorale denunciava Sputnik.

In Gran Bretagna la House of Commons lanciava nel Settembre 2017 un'indagine sull'utilizzo dei social media da parte della Russia durante la campagna referendaria Brexit. Una grande opportunità per Mosca data la polarizzazione che ne derivava e gli effetti potenzialmente destabilizzanti nell'UE. Le prove dell'interferenza russa abbondano. In UK le agenzie stampa russe sono ben posizionate e vengono usate per alimentare scontento e divisione tra le regioni. Personalità dello Scottish National Party come Alex Salmond hanno ospitato nel Novembre 2017 talk shows su Russia Today. Mosca individuava già nel 2016 nella Scozia un'ottima base per la sua campagna di disinformazione e apriva sedi di Sputnik e Pravda a Edimburgo. Gli attacchi cyber di provenienza russa in settori critici, soprattutto media, telecomunicazioni, energia, non accennano a diminuire.

In Germania il Governo era in stato d'allerta per l'hackeraggio del Bundestag, della CDU, dei Ministeri delle Finanze e di quello degli Esteri. Tutto portava all'attribuzione degli attacchi ai russi di APT28-FancyBear, con il coinvolgimento di Putin secondo l'intelligence tedesca. Era stata orchestrata nel 2016 e diffusa persino dal Ministro degli Esteri russo – che accusava persino il Governo tedesco di "cover up" – la vicenda completamente inventata, ma che aveva subito sollevato un'ondata di indignazione e di rabbia di una ragazzina tredicenne russo-tedesca a Berlino, Lisa, asserita vittima di un rapimento per stupro compiuto da immigrati. I media russi ne avevano subito fatto un caso emblematico. Ma ritrovata, Lisa confessava di aver trascorso la notte con il fidanzato.

Preoccupazioni dagli Stati Uniti

Un quadro sempre più allarmato per le interferenze web nelle prossime elezioni politiche al Parlamento europeo, e ai Parlamenti nazionali, è stato tracciato nell'ultimo numero di Foreign Affairs da due autorevolissimi conoscitori della materia: Michael Chertoff, già Segretario di Stato Americano per la Sicurezza interna, e Anders Fogh Rasmussen, Segretario Generale della NATO sino al 2014. I due specialisti sottolineano come nei prossimi due anni si terranno più di 20 consultazioni elettorali in Europa e in Nord America. Gli elettori dovranno scegliere tra candidati che sostengono apertura e multilateralismo e altri che invocano l'isolazionismo, che appoggiano le posizioni russe e di altri regimi autocratici. Ogni singolo paese e processo elettorale, rimarcano i due autori, deve fare di più per proteggersi. Soprattutto si rende necessario uno sforzo collettivo per difendere le istituzioni democratiche, in un impegno al di sopra dei partiti che assicuri una "risposta transatlantica" alle interferenze esterne.

I paesi che si reggono sullo Stato di Diritto e sulle Libertà democratiche devono dare una valutazione ampia delle vulnerabilità che riguardano i loro sistemi elettorali. Governi e società civili devono sostenere in forma diretta la difesa dei paesi che sono più vulnerabili all'interferenza straniera, come ad esempio l'Ucraina. E' necessaria una collaborazione fra policy makers e imprese ad alta tecnologia, per fornire ai cittadini gli anticorpi contro la falsa informazione.

A livello politico si deve lavorare a fondo per affrontare le origini delle fratture sociali sfruttate dalla Russia e da altri "attori maligni". Considerevoli danni sono già stati fatti a partire dal referendum sulla Brexit nel 2016, dalle Primarie alle elezioni Presidenziali nel 2016, sino alle Presidenziali francesi del 2017. "L'ampiezza delle campagne di disinformazione russa sui social media, sostiene Foreign Affairs, è impressionante: all'approssimarsi delle elezioni politiche in Italia del marzo 2018, i sistemi "Bots" (diffusori automatici di disinformazione) sono stati responsabili

dell'aumento del 15% nell'attività Twitter di promozione di candidati di estrema destra". Falsi "accounts" Twitter hanno generato il 30% di tweets e retweets nell'agosto 2018 sull'assassinio di Alexander Zakharchenko, un leader ribelle filorusso in Ucraina. In Macedonia c'è stata l'impennata di nuovi "accounts" 40 giorni prima del referendum 2018 riguardante il cambiamento del nome, che la Russia non voleva perché avrebbe avvicinato la Macedonia alla Nato. Identità automatizzate sul web hanno incoraggiato i votanti a boicottare il referendum. Analoghi fenomeni nelle attività "Bot" si sono verificati in preparazione delle lezioni in Svezia lo scorso settembre e in Bosnia in ottobre. Le interferenze sono state mirate a rafforzare qualsiasi candidato o partico fosse giudicato favorevole ad adottare una linea morbida verso la Russia.

Come risultato di tutto questo, non sorprende certo che un sondaggio effettuato lo scorso anno da Dalia Research abbia segnalato percentuali rilevanti, nelle Democrazie Occidentali, di persone che si dicono deluse dai rispettivi Governi: il 64% degli intervistati dichiara che raramente il proprio Governo agisce nell'interesse pubblico. Nei paesi autocratici e totalitari, soltanto il 41% da analoghe risposte. Con il beneficio di inventario circa la sincerità e la libertà con la quale il secondo gruppo può manifestare le proprie opinioni, si tratta comunque di dati allarmanti.

Nell'aprile 2018 Microsoft ha lanciato il Defending Democracy Program per prevenire l'hacking, accrescere la trasparenza sulla pubblicità online, per accrescere soluzioni innovative per proteggere i processi elettorali e identificare gli attacchi cyber. Sotto la pressione della politica e del pubblico, Facebook, Google e Twitter si sono mossi nella stessa direzione.

Nel giungo 2018 è stata creata la Transatlantic Commission on Election Integrity, mirata a imprimere un salto di qualità alla cooperazione transatlantica. Anche in ambito G7 nel Vertice del giugno 2018 in Quebec, i leader che hanno partecipato

hanno deciso di coordinare gli sforzi nazionali per combattere le interferenze. Tuttavia, conclude lo studio di Foreign Affairs, troppi Governi o negano o non comprendono pienamente la gravità della minaccia. La Transatlantic Commission on Election Integrity sta quindi eseguendo una serie di valutazioni critiche sulle diverse situazioni paese, i diversi fattori che riguardano i processi elettorali e democratici, la legislazione, la vulnerabilità dello spazio cyber, le piattaforme social, la presenza di gruppi anti-occidentali che cercano di influenzare o pregiudicare le elezioni.

Conclusioni

Ci sono numerosi passi da fare per difendere meglio le nostre democrazie da attacchi e disinformazione sulla rete. Le elezioni europee sono vulnerabili. Un'azione tempestiva e coordinata tra i Paesi membri dell'Unione è urgente. La minaccia proviene dalla Russia, ma non solo. Si deve guardare anche in altre direzioni. L'origine degli attacchi è estera e interna. Le strategie per proteggere la formazione del consenso e le dinamiche elettorali sono ancora, in diversi paesi europei, a uno stadio embrionale.

Dalle "lessons learned" gli specialisti di sicurezza cyber hanno tratto tutta una serie di raccomandazioni. Esse vanno dal considerare i sistemi elettorali parte integrante delle infrastrutture critiche, con tutte le implicazioni che ciò comporta per difenderle e garantirne la "resilience", alle misure per prevenire e bloccare interferenze esterne nella formazione del consenso. Test frequenti di vulnerabilità dei sistemi, annunci pubblici circa contromisure e risposte previste in caso di attacchi, denuncia delle intrusioni e loro attribuzione quando possibile hanno avuto in diversi casi un efficace effetto dissuasivo, come nelle elezioni in Germania. I Governi devono coinvolgere a fondo partiti e candidati nella campagna per la sicurezza cyber, e acquisire il deciso sostegno dei Leaders.

La tutela della democrazia elettorale deve essere percepita come un fondamentale obiettivo politico, riguardare tutti i livelli amministrativi, nazionali e locali. In Francia, Germania e Gran Bretagna i Governi hanno direttamente fornito o consigliato ai Partiti esperti certificati. Devono essere disponibili piani di contingenza in caso di attacco riuscito, includendo le attività di contro-informazione come avvenuto in Francia. Gli elettori sono da considerare parte integrante di questi sforzi. In Svezia è stato lanciato un programma per insegnare nelle scuole superiori le tecniche per individuare e contrastare la propaganda Russa.

Il coordinamento del Governo con media tradizionali e social, attuato con successo in Svezia e altri Paesi europei attraverso l'eliminazione di false identità e notizie da Facebook, è altrettanto essenziale. Si tratta anche di incoraggiare tutti i media a agire in via volontaria contro la disinformazione. L'esperienza fatta in Francia con il programma CrossCheck e in Germania con Correctiv può essere molto utile anche per altri. Infine, la difesa dello Stato di Diritto nelle Democrazie liberali non può non essere avvertito come un impegno comune e condiviso nel mondo occidentale.

Allo stato delle cose non esistono ancora meccanismi istituzionalizzati ai quali affidarsi. Tuttavia il Servizio Europeo per l'Azione Esterna, il Centro Comunicazione della Nato, il Centro COE per il contrasto alle minacce ibride in Finlandia sono utili punti di sostegno per azioni coordinate a livello europeo e atlantico contro intrusioni e disinformazione. Ma la responsabilità primaria resta pur sempre nazionale. Il Governo deve saperne rispondere ai cittadini, in piena trasparenza.