Guerra ed elezioni nel “dark web”: una lezione dalla Svizzera

Le polemiche che stanno coinvolgendo il comitato parlamentare di sorveglianza dei servizi segreti (Copasir), presieduto da Adolfo Urso di Fratelli d’Italia, circa le interferenze e manomissioni che operano in rete sulla campagna elettorale, ci confermano che ormai gran parte della comunicazione politica passa per canali non visibili, in quello spazio insondabile che chiamiamo *dark web*, che altera radicalmente il processo di formazione dell’opinione pubblica, basato proprio sulla condivisione trasparente dei contenuti. **Singolare è il sostanziale silenzio dei partiti, come il Pd**. Che pure è colpito da queste strategie che sono, secondo dati riconosciuti internazionalmente, promossi prevalentemente da

centrali che operano direttamente alle dipendenze dei servizi russi.

Il report del servizio informazioni della Confederazione elvetica, rilanciato da "Repubblica" qualche giorno fa, denuncia, con un corredo di documenti, **l'uso di server russi dislocati nel territorio svizzero per interferire nei diversi Paesi europei**. In particolare, gli apparati di sicurezza di Zurigo guardano all'Italia come anello debole dell'Unione europea, proprio nel corso dell'attuale campagna elettorale. **Si denuncia un'attività di inquinamento dei flussi informativi, diretti individualmente a migliaia di singoli elettori. Il tutto nell'inattività completa delle autorità competenti del nostro Paese, a partire dall'Agcom**.

Appare interessante, proprio ai fini del contrasto di queste **strategie di infiltrazione**, l'attività e la struttura dell'ente che ha elaborato il report citato da "Repubblica": la **Centrale di annuncio e di analisi per la sicurezza dell'informazione**. Si tratta di un organismo istituito in Svizzera nel lontano 2004, a tre anni dall'11 settembre, quando i più avvertiti esponenti dei sistemi di sicurezza avevano già percepito le turbolenze che si sarebbero ripercosse lungo le reti digitali.

Il primo ottobre del 2004, infatti, viene costituita l'agenzia con il compito di monitorare lo scenario complessivo dell'informazione del Paese. L'elemento più originale e rilevante riguarda proprio la connessione fra sistemi informatici e quadro della comunicazione. L'agenzia svizzera, a differenza delle diverse agenzie italiane, ha il mandato di analizzare costantemente proprio le anomalie che collegano il mondo della rete ai fenomeni dell'informazione, con l'obbligo di formulare un rapporto semestrale su quanto affiora nell'infosfera.

Nel 2008, quattro anni dopo la sua costituzione, l'agenzia scrive nel suo settimo rapporto (gennaio-giugno 2008): "Questa

evoluzione esige un ripensamento: d'ora in poi ci si dovrà focalizzare sulla protezione dell'informazione e prescindere dalla protezione esclusiva dei computer e delle reti sui quali sono archiviate le informazioni, il che comporta una gestione rafforzata delle informazioni e dei dati, una classificazione delle informazioni e simili. Ciò presuppone, d'altronde, un'attenta ponderazione dei rischi che deve condurre a un adeguamento dei canali di distribuzione, dei diritti di accesso e dei luoghi di archiviazione al valore effettivo delle informazioni. Non ogni canale di distribuzione o luogo di archiviazione dell'informazione presenta la medesima sicurezza e non tutti i documenti di un'azienda sono ugualmente sensibili. In tal modo la sicurezza dell'informazione è integrata nel processo di management commerciale e strategico dei rischi". Indubbiamente una straordinaria capacità predittiva che permette ai dirigenti dell'agenzia di anticipare le minacce che da lì a qualche anno diventeranno reali in tutto il mondo. Solo cinque anni dopo, viene elaborata dai vertici militari del Cremlino la teoria della "guerra ibrida", che porterà poi alle clamorose azioni di intromissione nella campagna presidenziale americana del 2016 con Cambridge Analytica.

Importante ci pare proprio **l'identificazione della produzione personalizzata delle informazioni, più che delle infrastrutture di raccolta ed elaborazione, come vero epicentro delle azioni di manomissione e interferenza.** Il mondo del giornalismo come motore della distribuzione digitale delle notizie viene così integrato nelle strategie di cybersecurity (vedi il nostro precedente articolo).

Straordinariamente sensibili appaiono gli analisti svizzeri quando intuiscono – siamo ancora distanti dalle strategie che verranno praticate dagli Stati Uniti in Ucraina, nel 2014, e da Mosca in Occidente – che la deformazione e la personalizzazione dei contenuti in rete possa costituire un'arma di pressione politica sulle istituzioni di un Paese:

“L’*hacktivism* può basarsi su motivazioni nazionalistiche oppure incarnare una sorta di protesta pubblica, una forma di resistenza civile. Internet costituisce una tribuna pubblica e consente di attirare l’attenzione a livello mondiale con mezzi relativamente semplici. Inoltre Internet e le tecnologie dell’informazione svolgono un ruolo sempre più importante negli Stati moderni, circostanza che accresce il numero delle zone di attacco. Gli attori di un conflitto politico o di una controversia di qualsiasi genere possono sfruttare Internet e le tecnologie sia come strumento, sia come bersaglio. A tale scopo gli hacker motivati politicamente si avvalgono di numerosi mezzi illegali o perlomeno dubbi. Sovente si fa uso del *defacement* di pagine Web, ossia della deturpazione di pagine Web, come pure di attacchi DoS, ovvero di attacchi ai server nell’intento di pregiudicare uno o più dei suoi servizi. Ulteriori mezzi sono i *redirect*, il furto di informazioni, le parodie di pagine Web, il blocco virtuale delle sedi, il sabotaggio e il software appositamente sviluppato (…). Si può quindi presumere che in futuro i conflitti politici e le controversie saranno vieppiù scortati da *hacking* a sfondo politico. In merito va osservato che simili azioni possono accompagnare i conflitti e le guerre, ma non sono adatti al sostegno diretto alle operazioni di guerra. Pertanto l’amalgama che si opera volentieri tra *hacktivism* e ‘guerra informatica’ non corrisponde alla realtà”.

La guerra entrava così nell’orizzonte dell’*hacktivism* già da vari anni, diventando utente e promotore del nuovo giornalismo digitale. Si comprende, in questo passaggio, come **un’attenzione geopolitica alle dinamiche di rete permetta di cogliere la natura e gli effetti che questo mondo ormai produce nella realtà**, trasformando persino la guerra in **un caso di intelligence diffusa**. Una lezione per i nostri controllori e tutori della sicurezza digitale che, a metà campagna elettorale, ancora si interrogano sulle forme e i poteri per intervenire bonificando uno scacchiere ormai largamente presidiato da forze estere. Ma **anche un monito alla**

sinistra, che continua a stupirsi di come ceti sociali, territori e categorie produttive, mutino i propri orientamenti, e non reagiscano a sollecitazioni che sembrano clamorose.

Come diceva Cioran, alla fine degli anni Ottanta: “Non si abita un Paese, si abita una lingua”, intendendo che le forme di comunicazione determinano identità e cittadinanza ancora più che le tradizioni culturali o il senso di appartenenza territoriale. **E oggi la lingua è la rete**.