Il web alla prova della "cyberguerra" in Siria

Stéphane Bazan
Ricercatore e responsabile del Dipartimento interdisciplinare di ricerca Web Science del Centre d'études pour le monde arabe moderne (CEMAM) dell'Università Saint Joseph, Beirut (Libano)

Christophe Varin
Direttore del Centre d'études pour le monde arabe moderne (CEMAM) dell'Università Saint Joseph, Beirut (Libano)

Nelle rivolte della Primavera araba il web è stato un aiuto per veicolare la mobilitazione sociale. Ma qual è la situazione in Siria, dove la presunta libertà della rete si è in realtà ritorta contro i ribelli stessi? Come i servizi segreti siriani sono riusciti ad assestare duri colpi alla loro rete, ingaggiando una cyberguerra inaspettata? Quali spunti di riflessione sulla libertà e la sicurezza del web offre questa vicenda? Un testo di pochi mesi fa ci aiuta a trovare qualche risposta.

Le rivolte esplose in vari Paesi arabi da due anni a questa parte e che ancora sono in corso hanno messo in luce alcune "competenze" indotte dall'uso delle piattaforme sociali disponibili sul web. Se l'impatto di queste competenze sul risultato finale delle rivolte è ancora oggetto di dibattito, non si può negare il ruolo svolto da questi strumenti nella comunicazione tra i militanti, nell'organizzazione delle proteste e nella diffusione di informazioni spesso inaccessibili attraverso le fonti tradizionali, quali la stampa o la televisione. Dal Golfo a piazza Tahrir al Cairo, da Bengasi a Tunisi, **l'opinione pubblica si è impossessata dei social media per farne mezzi straordinari di trasmissione dell'informazione**, sfruttando le potenzialità offerte da tecnologie contrassegnate dal dono dell'ubiquità e della mobilità, per non parlare dell'accesso gratuito, della facilità di utilizzo e anche della relativa libertà d'uso che esse consentono. In effetti, i movimenti di opposizione hanno

saputo sviluppare gli strumenti per trasmettere il loro messaggio: dai primi siti Internet degli anni '90, ospitati all'estero e aggiornati dagli esuli, ai nuovi account su Facebook, Twitter e YouTube, si è fatta strada una cultura della resistenza, aiutata talvolta dall'intervento "pedagogico" di organizzazioni straniere[1]. **I regimi repressivi si sono trovati in seria difficoltà nel dare una risposta efficace a questo attivismo on line**, sia per la mancanza di competenze tecniche disponibili, sia per la scarsa reattività davanti alla rapidità dei cambiamenti imposti da questa minaccia venuta dall'informatica. Del resto, lo stesso Tim Berners-Lee, inventore del World Wide Web, sostenne che esso evolve a una velocità superiore a quella della nostra capacità di osservarlo[2].

Agli occhi di chi osserva quanto sta accadendo in Siria (30.000 vittime al 1° ottobre 2012 secondo l'Osservatorio siriano dei diritti umani[3]) è ormai evidente che il conflitto, da sollevazione popolare, a volte assimilata alle manifestazioni o rivoluzioni della cosiddetta Primavera araba, si è trasformato in una guerra civile e fratricida con implicazioni regionali e internazionali. Tuttavia, pur essendo in parte cominciata su un campo virtuale, quello del web, **la mobilitazione on line in Siria non ha ottenuto i risultati sperati, contrariamente a quanto è successo in Egitto e in Tunisia**. Le ragioni di questo insuccesso vanno ricercate nel contesto particolare del web siriano (diverso per molti aspetti dal suo omologo tunisino o egiziano), ma anche nella natura delle strategie scelte dalle fazioni in lotta. La Rete stessa, presentata da alcuni come strumento liberatore in grado di fornire on line gli spazi di espressione di cui le società oppresse non dispongono, a poco a poco si è trovata accusata di essere diventata strumento di controllo, di inganno e repressione.

Sin dalle prime manifestazioni, si è studiata la Rete per cercare di trovarvi fenomeni che fossero paragonabili alle situazioni createsi in Egitto o in Tunisia. YouTube, Facebook, Twitter: la rivoluzione siriana – come le sue "sorelle" dell'anno precedente –, sembrava aver trovato il suo posto sui social network, facendo ancora una volta del web la "vetrina" della contestazione, a colpi di video girati con gli smartphone e di tweet infiammati che convocavano le manifestazioni del venerdì. Come per l'Egitto e la Tunisia, la rivoluzione è stata seguita in diretta dai quattro angoli del mondo, avendo come corollario il disegno strategico di mobilitare la comunità internazionale,

[1] Cfr «Egypt protests: America's secret backing for rebel leaders behind uprising», in *The Telegraph*, 28 gennaio 2011.

[2] Berners-Lee T. et al., «A Framework for Web Science», in *Foundations and Trends in Web Science*, 1 (2006) 1-130.

[3] Syrian Observatory for Human Rights, <www.syriahr.com>.

se non, addirittura, di scatenare un intervento militare – analogamente a quanto accaduto in Libia – per mettere fine alle violenze che infierivano sul territorio nazionale siriano. Si aggiunga poi che la prossimità simbolica degli usi e delle pratiche del web impiegati dai contestatori siriani con le manifestazioni o le rivolte sociali che si svolgevano contemporaneamente nelle capitali europee o americane (gli "Indignados" o, ancora, il movimento "Occupy Wall Street", che ha legato la sua azione alle manifestazioni egiziane di piazza Tahrir) ha generato una simpatia rafforzata dai legami del "virtuale" tra le cause degli uni e le lotte degli altri. La constatazione di questa prossimità ha permesso che si diffondessero alcune comode convinzioni; dato che il cybermilitante, da Tunisi a New York, dal Cairo ad Aleppo, utilizza gli stessi schemi e gli stessi modi operativi, si devono ottenere risultati se non identici almeno simili: presa di coscienza locale, mobilitazione internazionale, strutturazione della protesta e passaggio dal "virtuale" al reale, per riprendere qui un'espressione canonica.

In altri termini, queste rivoluzioni "tecnologiche" sarebbero dunque l'incarnazione del celebre slogan no global "Pensare globale, agire locale": poiché la tecnologia è globale, ciò che accade nel mondo arabo non dovrebbe tardare troppo a raggiungere altri spazi riluttanti a qualunque liberalizzazione. Non si può però dimenticare che, malgrado le immediate analogie, **il web non è identico ovunque e per tutti. Non lo si può considerare come il motore unico delle rivoluzioni**, né tanto meno come semplice cinghia di trasmissione della mobilitazione sociale attraverso le rivendicazioni veicolate dai social network. Non ci troviamo di fronte a un nuovo web arabo emerso da una primavera sociale, ma piuttosto a una tecnologia giunta a maturazione, i cui attori diventano finalmente i principali beneficiari. Ma queste «due magie»[4] – trasposizione di uno strumento micro verso una trasformazione macro – non si situano nello stesso tempo dell'azione politica, cosa che alcuni osservatori delle rivolte in questa regione del mondo sembrano aver dimenticato, non cogliendo il fatto che il web arabo non ha aspettato il 2009 per iniziare a esistere[5]. È possibile infatti far corrispondere l'emergere di un "biotopo web" in alcuni Paesi arabi con l'aumento della capacità di stoccaggio on line di certi siti amici, l'accesso sempre più democratizzato a nuovi dispositivi informatici che consentono l'accesso mobile al web e l'introduzione di connessioni ad alta velocità in molti

[4] Berners-Lee T., «The process of designing things in a very large space», in *Web Science*, <www.w3.org/2007/Talks/>.

[5] Bazan S. – Varin C., «Web Science in the context of the Arab Near East», <http://journal.webscience.org/327/2/websc i10_submission_2b.pdf>.

Paesi arabi. Tutte tappe essenziali per la crescita di un ecosistema web suscettibile di vedere emergere nuove forme di comunicazione e organizzazione sociale on line.

Il biotopo del web siriano

Il caso siriano tuttavia sembra muoversi in controtendenza rispetto questa logica. Già nell'ottobre del 2012 era incontestabile il fallimento delle attese della mobilitazione via web in Siria, sia sul piano organizzativo della contestazione sia su quello di una eventuale mobilitazione internazionale efficace. Per comprenderne le ragioni è necessario descrivere le caratteristiche del biotopo del web siriano nel 2011. **Al principio della mobilitazione, Internet è sotto il controllo totale del regime, l'accesso a numerosi social network è formalmente vietato, l'intera struttura di telecomunicazioni è sotto il monopolio statale** del Syrian Telecommunications Establishment (STE) e della Syrian Information Organisation (SIO), entrambi controllati dai vari servizi segreti (tra cui la Branche 225[6]), in particolare grazie all'uso di Thundercache, un software che consente di bloccare l'accesso a certi siti sulla base di una lista di parole chiave.

Un **biotopo** è un'area di limitate dimensioni di un ambiente in cui vivono organismi vegetali o animali di una o più specie, ad esempio uno stagno. Si tratta di uno degli elementi costitutivi di un ecosistema.

Messo sotto embargo tecnologico da Washington, il regime siriano si è rifornito essenzialmente in Europa e in Russia per attrezzare una rete Internet che si è lentamente sviluppata a partire dal 2000. Dopo un breve periodo di relativa apertura e di maggiore libertà nell'uso delle tecnologie dell'informazione e della comunicazione (corrispondente in parte all'arrivo al potere di Bashar al Assad, l'attuale presidente siriano; cfr la scheda a p. 316), il sistema, più repressivo, riprende il controllo e limita, prima di vietare del tutto, l'accesso a numerosi siti della rete mondiale. Constatando questa tendenza, **Reporters without Borders nel 2006 inserisce la Siria nella lista dei "Paesi nemici di Internet"** e nel suo rapporto denuncia che Internet è sotto controllo, poco affidabile tecnicamente e, soprattutto, lento e costoso. Con l'introduzione della rete 3G[7], la situazione degli internauti siriani ha visto qualche miglioramento, ma Syriatel – l'unico

Reporters without Borders (Reporter senza frontiere), fondato a Montpellier in Francia nel 1985 da quattro giornalisti, è un'associazione non profit organizzata per aree geografiche che opera essenzialmente in due settori: la censura in Internet e nell'uso dei new media e l'assistenza materiale, psicologica e finanziaria a giornalisti operanti nelle zone calde del pianeta. Nel loro sito, <http://en.rsf.org>, sono riportate molte notizie sulla situazione della censura del web in Siria.

[6] Dipartimento siriano per la sicurezza delle comunicazioni, incaricata del controllo di Internet.

[7] Per i termini informatici, si rimanda al Glossario a p. 308.

provider autorizzato in Syria – appartiene a Rami Makhlouf, influente cugino di Bashar al Assad. Nel 2007 viene vietato Facebook, perché secondo il regime rappresenta una minaccia americana. Lo stesso succede nel 2008 e 2009 anche a Wikipedia, Skype, Blogspot, Blogger e YouTube. Tutto ciò non impedisce alla famiglia Assad di essere molto presente su Internet, promuovendo se stessa e il regime su siti in arabo e in inglese o, ancora, attraverso una pagina Facebook, per non parlare dell'onnipresente contenuto prodotto dall'agenzia ufficiale di informazione SANA (Syrian Arab News Agency), generalmente presentato dal potere non come una strategia ufficiale, ma come il risultato di iniziative individuali della famiglia Assad.

Queste restrizioni o divieti hanno ricadute importanti sullo sviluppo di Internet in Siria, tanto sul piano economico quanto su

Glossario

3G: Il termine **3G** in telefonia indica l'utilizzo di reti e tecnologie di terza generazione, che consentono sia di fare e ricevere telefonate digitali sia il trasferimento di dati non-voce, quali e-mail, messaggeria istantanea, download da Internet di file di vari formati (musica, video, ecc.).

DEFACEMENT: Per **defacing** o **defacement** si intende, in campo informatico, un attacco a un sito che ne modifica o la home page o le pagine interne, all'insaputa del gestore del sito stesso.

HTTPS e MAN IN THE MIDDLE: La navigazione **HTTPS** indica che, per garantire la sicurezza nel trasferimento di dati, viene applicato un protocollo di crittografia, per impedire la intercettazione dei contenuti. Tale protocollo può essere violato da un attacco dell'**uomo in mezzo** (***man in the middle attack***), in cui l'attaccante è in grado di leggere, inserire o modificare messaggi tra due parti senza che nessuna delle due sia in grado di sapere se il collegamento che le unisce sia stato compromesso.

PROXY: Un **proxy** è un programma o dispositivo hardware che funziona come interfaccia tra un client (il computer da cui si accede a Internet, ad esempio) e il server reale, inoltrando richieste e risposte da uno all'altro. Ciò consente di:
- rendere più veloci i tempi di risposta (il proxy può rispondere direttamente senza inoltrare la risposta al server reale);
- accentrare tutte le richieste tra client e server. In ambito enterprise costituisce un importante punto di controllo e filtraggio del traffico Internet mentre per gli "open proxy" (quelli accessibili a tutti su Internet) diventa un ambìto "punto di osservazione" per "vedere" le abitudini di navigazione di chi lo utilizza;
- garantire un maggiore livello di privacy mascherando il vero indirizzo IP del client e rendendo più difficoltosa al server l'esatta individuazione del computer da cui giunge la richiesta.

TROJAN HORSE: Un **trojan** o **trojan horse** (cavallo di Troia) è un malware – ovvero un software creato per scopi illegali o comunque fraudolenti – le cui funzionalità sono celate all'interno di un programma apparentemente innocuo e che spesso mirano ad acquisire, totalmente o in parte, il controllo del computer su cui il trojan viene inconsapevolmente installato.

VPN: Il **VPN (Virtual Private Network)** è una rete di telecomunicazioni privata instaurata tra soggetti che utilizzano un sistema di comunicazione pubblico come Internet. I dati vengono quindi trasferiti attraverso Internet, protetti da protocolli di sicurezza e sistemi di crittografia, per garantirne l'accesso solo ai membri della VPN ed evitare il rischio di intercettazioni.

quello strategico della creazione di una società dell'informazione. La Siria, come altri Paesi del mondo arabo, produce pochissimi contenuti on line, l'attività di e-commerce è ridotta e le sue università restano ai margini delle comunità scientifiche che si formano sul web[8]. Al contempo, vengono emanati provvedimenti che mirano ad assicurare il controllo dall'interno sui contenuti e sulle persone[9]. **Di fronte a queste barriere, molti internauti siriani sviluppano nuove competenze per riuscire ad aggirare i sistemi di sicurezza e a padroneggiare i metodi più avanzati di pirateria informatica**, nonostante i materiali in parte obsoleti a causa del blocco tecnologico imposto alla Siria. A poco a poco, le loro capacità tecniche raggiungono anche utilizzatori meno esperti, arrivando così a creare una cultura dell'"aggiramento" delle connessioni Internet. Grazie alle reti VPN, ai server proxy e altre connessioni pirata, gli internauti siriani sono presenti sulla rete, sempre a loro rischio e pericolo. Queste comunità, grazie alle loro abilità, hanno giocato un ruolo essenziale nel sostegno on line sia ai ribelli sia al potere.

Lo "spinternet" del regime siriano sul web

Inaspettatamente, all'inizio del 2011 Damasco sembra procedere a un cambio radicale che Evgenij Morozov, giornalista e sociologo bielorusso esperto di nuovi media, definisce come «spinternet»[10]: quando le prime manifestazioni sono già scoppiate, **a partire dal febbraio 2011 il regime riapre le porte dei social network e ferma il filtraggio di YouTube, Facebook e Twitter**.

Lungi dall'essere un segnale di apertura, questa decisione rivela che il regime siriano ha imparato la lezione delle rivolte egiziane e tunisine. **Da allora, per i contestatori la Rete inizia a diventare una immensa trappola**. Da marzo 2011, molti siriani, già utenti abituali della Rete grazie agli accessi illegali, cominciano a connettersi regolarmente sui social network e a unirsi ai gruppi di protesta. La pagina Facebook intitolata «Syrian Revolution», creata nello stesso mese, arriva a raccogliere rapidamente più di 140.000 membri[11]. Rassicurati, vari gruppi di attivisti creano spazi dove vengono elencati i vari abusi del regime, come ad esempio gli stupri commessi

[8] Nedelec A., *Les logiciels libres au Proche-Orient. Le cas de la Syrie. Société de l'information au Proche Orient*, CEMAM, Beirut 2007.

[9] Cfr Baiazy A., *Syria's Cyber Wars*, 2011, <www.mediapolicy.org/wp-content/uploads/Syria-Cyber-Wars-06-01-2012-proof2.pdf>.

[10] Morozov E., *L'ingenuità della Rete. Il lato oscuro di Internet*, Codice edizioni, Torino 2011.

[11] Clayton M., «Syria's Cyberwars: using social media against dissent», in *The Christian Science Monitor*, 25 luglio 2012, <www.csmonitor.com/USA/2012/0725/Syria-s-cyberwars-using-social-media-against-dissent>.

dall'esercito siriano durante le operazioni di repressione[12], o dove si possono vedere video clandestini. Ma questa attività on line lascia tracce e i dati identificativi utilizzati per accedere a questi siti sono facilmente reperibili dai funzionari dei servizi segreti siriani e tutte le tecnologie utilizzabili vengono messe a disposizione dei loro esperti informatici: falsi video, apertura di account fittizi su social network come Facebook che permettono di raggruppare i dissidenti, attacchi del tipo "Man in the middle" (uomo in mezzo), che consiste nell'introdurre falsi certificati di sicurezza nelle navigazioni HTTPS protette di Facebook. **La repressione on line si adatta all'attività di questi cyberdissidenti, copiando le loro stesse pratiche, al fine di identificarli e quindi arrestarli**. Al momento degli interrogatori, vengono loro estorti codici d'accesso e password, dando così ai servizi segreti la possibilità di identificare intere reti di oppositori in Siria e all'estero. Come sottolinea Morozov[13], la fede professata da Google nella formidabile capacità di liberazione delle tecnologie è rovesciata dal regime siriano, come già aveva fatto il regime iraniano all'epoca della rivoluzione verde del 2009-2010 contro la irregolare rielezione del presidente Mahmoud Ahmadinejad[14]. Tra febbraio e giugno 2011 in Siria vengono arrestati una ventina di influenti internauti, vengono per lo più espulsi, qualche volta eliminati.

L'Esercito elettronico siriano

Nello stesso periodo, diversi siti specializzati, come l'Information Warfare Monitor, cominciano a tracciare le attività di un gruppo di hacker che si identificano come Syrian Electronic Army (Esercito elettronico siriano). Si tratta delle **prime azioni visibili di una iniziativa semiufficiale di contrattacco condotta dal regime siriano sul web**. Supportato dai servizi segreti siriani, esso ha accesso privilegiato ai server della Syrian Computer Society (di cui Bashar al Assad è stato in passato presidente). Alcuni dei suoi membri provengono dalla Syrian Hackers School, una «accademia virtuale di pirateria informatica» aperta a tutti i sostenitori del regime su Facebook[15]. Il 20 giugno 2011 Assad, in un discorso alla nazione[16], si è

[12] Cfr ad esempio la notizia riportata sul sito di Al Arabiya, «International women's group begins mapping sexual violence in Syria», 1 aprile 2012, in <http://english.alarabiya.net>.

[13] Morozov E., *L'ingenuità della Rete*, cit.

[14] Simon J., «Repression Goes Digital», in *Columbia Journalism Review*, aprile 2012.

[15] Information Warfare Monitor, «Syrian Electronic Army: Disruptive Attacks and Hyped Targets», 25 giugno 2011, <www.infowar-monitor.net>.

[16] Discorso alla Nazione del Presidente Assad, 20 giugno 2011, <http://www.al-bab.com/arab/docs/syria/bashar_assad_speech_110620.htm>.

addirittura congratulato con questo vero e proprio esercito «all'interno della realtà virtuale». Se pure altri Paesi all'interno dei servizi segreti sono in grado di condurre una cyberguerra, questo **è stato il primo caso di riconoscimento quasi ufficiale, da parte di uno Stato, di un "esercito elettronico" in grado di condurre attacchi per proprio conto**. Le azioni dell'Esercito elettronico siriano ovviamente non sono mai rivendicate a nome del regime, poiché esso non si descrive come un gruppo organizzato intorno a una struttura ufficiale, ma come un semplice raggruppamento di sostenitori del regime di Assad. Tuttavia la libertà d'azione e il supporto tecnico di cui esso dispone lasciano davvero poco spazio ai dubbi. La scelta dei bersagli e il fatto di annunciare le proprie azioni qualche giorno prima dimostrano che l'Esercito elettronico siriano obbedisce a una strategia ben precisa. Esattamente come nei metodi della repressione classica esso, pur agendo per via informatica, incute il timore di conseguenze terribili per gli obiettivi scelti.

Questa intromissione nello spazio digitale personale degli oppositori è percepita allo stesso modo di un'intrusione di miliziani nel cuore di una casa. Le azioni consistono principalmente in attacchi definiti di *defacement*, cioè di sfregio, contro siti web identificati come bersagli strategici o simbolici. Secondo l'Information Warfare Monitor, sono stati oggetto di simili attacchi più di 950 siti, mentre l'Esercito elettronico siriano ha rivendicato di averne colpiti circa 130. Sempre secondo l'Information Warfare Monitor, la maggior parte di questi siti ha poca importanza strategica, e in realtà sono ancora meno, poiché condividono indirizzi IP comuni. La posta in gioco in questo caso è più di tipo "qualitativo" che "quantitativo": significa mostrare capacità d'azione, abilità nell'uso delle tecniche di hackeraggio e testare la vulnerabilità dei bersagli, senza proporsi di colpire subito obiettivi davvero strategici. Ad esempio, il numero di siti israeliani presi di mira non supera la decina, mentre gli attacchi condotti contro Facebook consistono generalmente nel modificare i profili di personalità siriane di opposizione, oltre che nel creare – come già detto – account fittizi. **Tutto ciò però pone gli utenti dei social network in uno stato di profonda incertezza circa la veridicità delle informazioni pubblicate in nome della ribellione**: l'inserimento sui social network, come Facebook, Twitter e YouTube, di contenuti falsi creati dagli hacker dell'Esercito elettronico siriano danneggia gravemente quelli effettivamente postati dall'opposizione, perché è assolutamente impossibile per un internauta essere sicuro della loro origine e garantire la veridicità delle informazioni così diffuse.

Su un piano più tecnico, l'Esercito elettronico siriano e la Syrian Hackers School hanno diffuso sulle loro pagine Facebook "Bunder

F 1.0", un eccellente programma di DDoS (Distributed Denial of Service), cioè di attacco per negazione del servizio, che permette di modificare le home page di molti siti Internet. Queste vengono sostituite da immagini e testi che esaltano i meriti del regime o che contengono insulti contro i nemici. Vari siti britannici sono stati violati in questo modo, per punire il Regno Unito per il suo aperto sostegno al Consiglio nazionale siriano e all'Esercito siriano libero. Più recentemente, l'Esercito elettronico siriano ha diffuso numerosi virus e *trojan horses* (cavalli di Troia), il che potrebbe indicare un cambiamento di strategia tecnica. Ma in genere le aziende proprietarie dei social network reagiscono timidamente alle manovre dell'Esercito elettronico siriano: la sua pagina Facebook, che descrive chiaramente la sua identità e le sue intenzioni, ha dovuto essere ritirata diciotto volte per non aver rispettato le regole di utilizzo del sito. L'Esercito elettronico siriano ha quindi scelto di nascondersi dietro un indirizzo decisamente meno evidente, meno suscettibile di attirare l'attenzione degli strumenti di controllo di Facebook, e quest'ultima pagina è arrivata a contare fino a 20.000 membri prima di essere a sua volta ritirata dal social network.

Ma se l'Esercito elettronico siriano lascia spesso i cyberoppositori siriani "disarmati", una sfida di altre dimensioni è sopraggiunta **durante l'estate 2011, quando il gruppo di hacker internazionali "Anonymous" si è deciso a lanciare un contrattacco informatico al regime di Damasco**. L'8 agosto 2011 il gruppo ha rivendicato, sotto il nome di OpSyria[17], diversi attacchi di tipo "DDoS" contro siti ufficiali siriani. Secondo il sito CyberwarNews[18], legato al gruppo "Anonymous", i siti dei Comuni di Tartus, Homs, Latakia e Aleppo presi di mira da questi attacchi antiregime hanno cominciato ad "affiggere" sulle loro pagine on line statistiche riguardanti le vittime della repressione in corso. Anche il sito del ministero della Difesa non è sfuggito all'operazione e la sua home page per un certo periodo si è aperta con il logo di "Anonymous" e una serie di messaggi chiaramente ostili al regime siriano. Lo stesso gruppo di attivisti si è reso ugualmente celebre rivelando attraverso il sito di Wikileaks[19] il presunto contenuto della casella di posta elettronica del presidente siriano, di sua moglie e di un'altra ottantina di persone a loro vicine.

[17] Cyber War News, *Message From Anonymous – Operation Syria #OpSyria*, 11 settembre 2011, <www.cyberwarnews.info>.

[18] Cyber War News, *2316 Reasons why Assad is finished, #OpSyria leaves Government websites with a message*, 25 settembre 2011, <www.cyberwarnews.info>.

[19] Jamet C., «Les emails édifiants du couple el-Assad», in *Le Figaro*, 15 marzo 2012.

Il web siriano come arma di dissenso a larga scala

Innegabilmente, a causa dell'azione dell'Esercito elettronico siriano **la mobilitazione dei contestatori diventa sempre più difficile con il passare del tempo, poiché si svolge in un clima di diffidenza**. Con la diffusione di falsi messaggi, false informazioni e falsi video sui social network e, più in generale, sul web, è diventata sospetta tutta la Rete, rafforzando così un contesto di circospezione, inganno e dubbio. In mancanza di una piattaforma di opposizione riconosciuta e rispettata (simile ad esempio al blog Nawaat in Tunisia, <www.nawaat.org>), la struttura gerarchica, organizzata ed esperta dei servizi segreti siriani dispone di un vantaggio strategico certo e quasi decisivo su un'opposizione divisa, poco preparata alle tecniche della guerra virtuale e i cui mezzi di mobilitazione on line non si possono efficacemente trasmettere a una base sconnessa, diffidente e poco disposta a rispondere a interlocutori virtuali e spesso anonimi. La guerra informatica e i suoi danni in termini di "dissenso a larga scala" confermano il pessimismo delle analisi di Evgenij Morozov che abbiamo sopra ricordato. Addirittura, in determinate circostanze **la Rete può diventare un fattore di dissenso all'interno della stessa opposizione a Bashar al Assad**, e non sono mancati esempi di truffa informatica come quello dell'ormai celebre «Ragazza gay di Damasco», un blog che si diceva tenuto da una ribelle siriana gay, e che si è poi rivelato opera di un giornalista scozzese[20]. Pur non essendo direttamente legato alla strategia del regime, questo caso è stato sfruttato dal clan Assad per screditare sistematicamente i contenuti messi on line dagli oppositori. In un recente articolo pubblicato sul sito dell'agenzia Reuters[21], Peter Apps constatava che ad agosto 2012 questa guerra informatica sul web era ancora in corso e si andava intensificando per via dell'indecisione militare sul campo.

A conferma di questa constatazione, la Reuters rivelava che il suo servizio di blog aveva dovuto essere interrotto in seguito alla comparsa di vari messaggi che riferivano dei rovesci militari dei ribelli, che poi si sono rivelati falsi. Ancor più grave, l'account Twitter @ReutersTech ha dovuto essere sospeso dopo essere stato piratato e utilizzato per inviare informazioni che denigravano le azioni dei ribelli dell'Esercito siriano libero. Vogliamo qui sottolineare lo sforzo prodotto dalla pagina web del *New York Times* «Watching Syria's

[20] Gonzalez-Quijano Y., «Les spin doctors du Net: la vraie vie de la jeune femme lesbienne de Damas», 28 giugno 2011, in *Culture et politique arabes*, <http://cpa.hypotheses.org/2817>.

[21] Apps P., «Disinformation flies in Syria's growing cyber war», 7 agosto 2012, <www.reuters.com>.

War»[22], che tenta di collocare i contenuti disponibili su YouTube nel loro giusto contesto: i video vengono analizzati e valutati in termini di realtà informativa; ciò che il quotidiano è in grado di verificare è giustapposto alle domande che ogni video solleva. Tuttavia, secondo alcuni specialisti della cyberguerra queste azioni di propaganda di guerra hanno un impatto molto limitato sul campo, dove l'obiettivo strategico resta innanzitutto quello di braccare gli oppositori[23]. Se la strategia dei ribelli siriani sul web sembra a volte inefficace e votata all'insuccesso, nemmeno le azioni della repressione sembrano avere l'unanimità tra i sostenitori del regime. I contenuti proposti, le tecniche di scrittura e i bersagli presi di mira sono rapidamente identificabili e le reazioni dei proprietari dei servizi web sono generalmente immediate. A riprova della poca efficacia di quei metodi, il sito TechPresident segnala un cambiamento di strategia da parte del regime con l'utilizzo sempre più frequente di programmi di tipo RAT (Remote Access Trojan), come DarkComet, Backdoor.bruet o ancora Blackshades[24]. Questi malware si introducono nei computer degli oppositori a partire dai collegamenti su Facebook o Skype e agiscono come spie. **La cyberguerra sembra dunque avere un futuro migliore nel controllo e nell'identificazione degli utilizzatori della rete che nella disinformazione e nella propaganda**.

Molti autori, a cominciare da Morozov, sin dalle prime manifestazioni del 2009 in Iran hanno mostrato i limiti delle tecnologie web nella cyberguerra e i pericoli che l'"Internet-centrismo" dei guru del web fa pesare sui decisori politici delle grandi nazioni. Se l'obiettivo dei ribelli era quello di portare a conoscenza del mondo intero le atrocità commesse dalle truppe e milizie di Bashar al Assad, questo è stato raggiunto. I social network svolgono piuttosto bene il loro ruolo: la messa on line, la diffusione e la condivisione dei contenuti sono assicurate. Le cifre sono disponibili, le immagini a portata di clic. Ma a quale scopo? **L'onnipresente copertura degli avvenimenti in Tunisia, Egitto, Libia, Yemen e Siria alla fine ha annegato il messaggio nel cuore di un magma informativo difficile da decriptare**. Le mobilitazioni egiziane e tunisine sono ormai lontane e la complessità della situazione siriana, completamente impantanata, ha finito per stancare l'opinione internazionale, che è si è rivolta ad altri avvenimenti.

[22] *New York Times*, «Watching Syria's War», <http://projects.nytimes.com/watching-syrias-war>.

[23] Cfr ad esempio KLIMBURG A., citato sul sito dell'*Österreichisches Institut für Internationale Politik*, 7 agosto 2012, <www.oiip.ac.at>.

[24] Cfr GOLDMAN L., «In Syria's Civil War, Cyber Attacks are the "New Modern Warfare"», TechPresident, 8 agosto 2012, <http://techpresident.com>.

Fare della Rete un luogo sicuro?

L'esempio siriano solleva dunque alcune questioni sulla attuale natura del web. Tim Berners-Lee non ha concepito il suo programma per liberare i popoli, ma per combinare i sogni di una memoria universale prodotta da tutti e accessibile a tutti grazie alla tecnologia ipertestuale. La Rete non è più un posto sicuro per gli individui, ma per le informazioni non lo è mai stato. I regimi iraniani, siriani o cinesi l'hanno capito bene: il web è soprattutto una realtà tecnologica ed è a questo livello "di base" che fornisce di fatto i migliori servizi: collegamenti ipertestuali camuffati che scatenano virus e malware, indirizzi IP e URL che permettono di creare destinazioni ingannevoli, introduzione di codici HTML che deformano i siti e protocolli non protetti. **Internet non è un luogo sicuro, e visto il numero dei suoi utilizzatori è diventato persino un luogo pericoloso**. Una questione ritorna frequentemente negli studi sulla cyberguerra siriana: le "armi" dei belligeranti sono di fatto i siti, le piattaforme sociali, le connessioni che utilizziamo tutti i giorni per postare i ricordi delle nostre vacanze o comunicare con i nostri amici. Questi strumenti non sono servizi pubblici, ma spazi che appartengono ad aziende private, che spesso chiudono gli occhi sui contenuti di propaganda, gli account illegali, le conseguenze legate al *defacing* di pagine o all'assenza di sicurezza per gli utilizzatori.

La cyberguerra in Siria non sarebbe stata possibile senza il web e le sue piattaforme collaborative. Questa situazione interroga chiaramente gli scienziati che cercano di comprendere il web per farlo evolvere verso un funzionamento più sicuro, più protetto. Ma **la natura pericolosa, fondamentalmente decentralizzata e onnipresente di questo sistema di informazione gioca a favore di coloro che si augurerebbero di vederlo più controllato**, più regolato, persino più docile. Paradossalmente, gli interessi del regime di Bashar al Assad, che si basano evidentemente su considerazioni più pragmatiche, sono in sintonia in questo caso con quelli delle società occidentali. A riprova di ciò, in occasione della conferenza ACM Web Science che si è tenuta alla Northwestern University (Illinois, USA) nel giugno 2012, il problema del web come «luogo libero e sicuro» è stato posto ai numerosi informatici, sociologi, educatori presenti: se la maggior parte di loro dà prova di ottimismo, le proposte, da parte di alcuni, di aprire server nazionali di dati che consentano di utilizzare il *crowdsourcing* per identificare i delinquenti, possono far riflettere.

Il ***crowdsourcing***, o «esternalizzazione aperta», consente di sostituire il lavoro di una persona con la collaborazione volontaria di molte persone.

Titolo originale «Le Web à l'épreuve de la "cyberguerre" en Syrie, pubblicato in *Etudes,* 12 2012, 595-606. Traduzione di Cinzia Giovari, adattamento delle note, glossario e neretti a cura della Redazione.

Siria

Dati

Capitale: Damasco (1,7 milioni di abitanti).

Altre città: Aleppo (2,1 milioni), Homs (650mila).

Popolazione: 22,5 milioni (stima 2012); siriani con meno di 25 anni: 45,7%.

Superficie: 185.180 kmq.

Lingue: arabo (ufficiale); curdo, armeno e turco sono parlate dalle principali minoranze. Alcuni villaggi usano ancora l'aramaico, antica lingua franca.

Religioni: musulmani sunniti (74%); altri musulmani (alauiti, drusi) (16%); cristiani (8%).

Pil procapite: 5.100 dollari (stima 2011).

A due anni dallo scoppio della rivolta contro il regime (15 marzo 2011), in Siria continua una guerra civile che vede scontrarsi le forze del regime di Bashar al Assad e una galassia di forze di opposizione (la maggiore è l'Esercito siriano libero) e che ha causato 70mila morti, circa 900mila rifugiati all'estero e 2,5 milioni di sfollati interni.

Grande poco più di metà dell'Italia e con circa 22 milioni di abitanti, la Siria divenne indipendente nel 1946 e nel 1963 un colpo di Stato portò al potere il partito laico e nazionalista Ba'th. Nel 1970 conquistò il potere Hafiz al Assad, militare e membro del Ba'th appartenente a un clan della minoranza alauita (musulmani di matrice sciita), che stabilizzò il Paese attraverso una delle dittature più oppressive del mondo arabo. Nel 2000 gli successe il figlio Bashar, che ha conservato le strutture dittatoriali del regime. Alle prime proteste il presidente ha risposto con alcune concessioni, ma ha sempre rifiutato di dimettersi, reagendo alle ribellioni con violenza crescente, ricorrendo al sostegno dei militari, dei servizi di sicurezza e delle milizie *shabiha* di estrazione principalmente alauita.

Prima degli sconvolgimenti bellici, l'economia siriana era fortemente controllata dallo Stato. Con la crisi politica e militare, il Paese è stato condannato a pesanti sanzioni da parte dei Paesi occidentali, nel 2012 il Pil ha avuto una contrazione del 20%, l'inflazione è salita al 30%. Vasti settori della popolazione vivono una crisi umanitaria alla quale la comunità internazionale fatica a dare risposta.

L'ONU non è riuscita a dare soluzioni politiche alla crisi: i sostenitori esteri del regime di Damasco sono la Russia, che considera Damasco il principale alleato nella regione e ha posto il veto ad alcune iniziative del Consiglio di Sicurezza, e l'Iran, che sostiene il potere degli alauiti in funzione antisunnita. Arabia Saudita e Qatar sono i principali sponsor della rivolta sunnita, insieme alla Turchia.

Tra le formazioni militari antiregime vi sono forze jihadiste, come il Fronte al-Nusra, alle quali i Paesi occidentali non intendono dare pieno appoggio, anche se sono favorevoli al rovesciamento del regime. La Siria degli ultimi quarant'anni ha pesantemente limitato le libertà democratiche e violato i diritti umani, pur costruendo equilibri di convivenza tra le componenti etniche e religiose, ormai infranti. I timori sul futuro siriano riguardano la possibilità che prevalgano le opposizioni sunnite intenzionate a rifondare il Paese su basi religiose o che il Paese si frantumi del tutto lungo linee etnoreligiose.

Francesco Pistocchini