Dipartimento di Scienze Politiche

Cattedra di
Sociologia della Comunicazione

MINACCE CYBER: TRA DIRITTI E SICUREZZA

RELATORE.
Prof. Michele Sorice

CANDIDATO
Giorgia Loperfido
MATR. 072892

ANNO ACCADEMICO 2015/2016

Ringraziamenti

Un primo doveroso ringraziamento va al mio relatore, il Professor Michele Sorice, per l'opportunità che mi ha dato.

Ringrazio la mia famiglia, e in particolare i miei genitori perché senza di loro non sarei sicuramente qui.

A mio padre, il cui pensiero mi sento si sinterizzare con l'aforisma "puoi lamentarti perché le rose hanno le spine, o puoi essere felice, perché le spine hanno le rose".

A mia madre, che mi ha insegnato che nel mezzo delle difficoltà nascono le opportunità, con la sua grande capacità di reinventarsi e il suo coraggio.

Ai miei nonni, Anna, Evelina, Enzo e Giovanni, sempre presenti sul mio cammino.

A Margherita, senza la quale non potrei nulla.

A Tania, parte importante della mia vita da ormai quasi dieci anni.

A me stessa, perché ci vuole molto coraggio per crescere e diventare ciò che si è. Questo è stato un anno piuttosto faticoso, pieno di ostacoli letteralmente piovuti dal cielo.

Ce l'abbiamo fatta.

A tante altre vittorie e a tanti altri obiettivi, che spero di raggiungere con la stessa voglia e con la stessa tenacia.

Indice

Introduzione

Questa tesi ha lo scopo di fare maggiore chiarezza riguardo ad un tema tanto controverso come il cyber terrorismo. Nonostante questo termine nasca addirittura negli anni ’80 grazie allo studioso Barry Collins, che lo coniò per indicare “l’uso del cyberspazio con fini terroristici”, è tornato in auge negli ultimi anni, in seguito agli attacchi dell’11 settembre e soprattutto all’avvento dell’ISIS.

Con il passare del tempo, il suo significato si è ampliato, spesso cambiando in base al paese di riferimento, fino ad identificarsi erroneamente con una serie di altri fenomeni. Infatti, è importante chiarire che il cyber terrorismo non è hacktivism, ovvero una sorta di resistenza “culturale e politica” condotta nel cyber spazio, né cyber crime, che ha invece scopo di lucro e riguarda le organizzazioni criminali, né un cyber attack, ossia un’azione aggressiva condotta da persone, stati o organizzazioni, e neanche cyber warfare.

Pur condividendo alcuni aspetti dei fenomeni sopracitati, il cyber terrorismo ha caratteristiche proprie. Esso unisce due realtà oscure, il mondo cyber e il terrorismo, e il suo scopo è quello di creare il panico per motivi politi, religiosi o ideologici. È tuttavia difficile pervenire ad una definizione che sia condivisa a livello internazionale.

Il primo capitolo si propone di inquadrare il contesto nel quale tale fenomeno si sviluppa, il cyber spazio, descrivendone le componenti e le funzioni, fino ad arrivare all’ambito più tangibile dei cavi sottomarini, che permettono nel concreto l’esistenza del cyber-spazio.

Il secondo si focalizza, invece, sull’effettiva esistenza di una minaccia terroristica in senso cyber, approfondendo le altre minacce che possono celarsi nella cyber sfera. Maggiore attenzione verrà dedicata alla propaganda dell’ISIS e alla sua sbalorditiva capacità di affascinare le menti dei giovani militanti.

Infine, il terzo capitolo tratterà del bilanciamento tra sicurezza e libertà su internet. Infatti, la difesa dei diritti umani è sempre stata profondamente legata al concetto di sicurezza, un rapporto che spesso si traduce in conflitto tra prerogative dell’individuo e quelle dello stato.

La trattazione si avvarrà di importanti casi di attualità, come lo scandalo Datagate e la sentenza Schrems, che hanno portato alla luce importanti falle nella tutela della privacy dei cittadini, dando vita ad un dibattito che si protrarrà ancora per molto tempo.

Capitolo I

L’ascesa della guerra cibernetica

Il mondo in cui stiamo mettendo piede è quello del cyberspazio, ovvero “the notional environment in which communication over computer networks occurs"[1], come ci spiega l'Oxford Dictionary, considerato dalla NATO come il il quinto *warfare domain.* Sempre di più oggi internet è al centro dell’attività economica, della vita di un’azienda e del cittadino. Questo dimostra come il nostro mondo ruoti sempre di più attorno all'informatica. Per spiegare cosa sia la cyber war, cominciamo dando una definizione di guerra. Come scrisse Carl Von Clausewitz, “la guerra è un atto di violenza il cui obiettivo è costringere l'avversario a eseguire la nostra volontà"[2]. Con ciò si intende dire che il prerequisito è la forza e che l’idea di guerra è imprescindibile dalla violenza. Inoltre, essa si è sempre concentrata sull’aspetto pubblico, implicando due schieramenti che si fronteggiano attraverso l'uso di armi allo scopo di annientare l'avversario.

Nella guerra cibernetica o cyberwar troviamo invece che gli attacchi sono raramente pubblici ma soprattutto che lo scopo non è uccidere o ferire i soldati dello schieramento nemico ma distruggere delle proprietà. Per distruzione di proprietà si intende ad esempio: programmi informatici che controllano una centrale nucleare o anche centrali elettriche che alimentano basi militari. Tutto ciò può riguardare più o meno da vicino anche la vita dei civili, andando quindi a colpire, grazie all'uso dell'informatica, i pilastri su cui si reggono le società moderne.

Inoltre, come scrive Thomas Rid in *Cyber War Will Not Take Place,* la violenza ″somministrata attraverso il cyber-spazio è meno diretta in almeno quattro modi: è meno fisica, meno emotiva, meno simbolica e di conseguenza meno strumentale agli usi più tradizionali della violenza politica″.

La più grande difficolta quando ci sono questi tipi di attacchi è stabilire da chi e da dove vengano sferrati. Infatti, per sua stessa natura, la guerra cibernetica è anonima e capace di espandersi con rapidità. Il fatto che internet sia alla portata di tutti in qualunque punto del pianeta aumenta le possibilità di poter attuare una guerra del genere senza, come ho appena detto, poter rintracciare efficientemente l'attentatore che, al fine di rendere più arduo questo compito, sfrutterà decine o centinaia di server di vari paesi prima di colpire l'obiettivo prescelto.

La guerra cibernetica si espande in due campi: attività di spionaggio e sabotaggio. Non a caso, uno dei primi e più efficienti attacchi informatici è stato quello a Natazan in Iran. In quel periodo, infatti,

[1] Oxford Dictionaries. “Cyberspace”. Ultima modifica 8 Agosto 2016. http://www.oxforddictionaries.com/it/definizione/inglese/cyberspace

[2] Carl Van Clausewitz. On War (Berlin: Ullstein 1832, 1980), 27

la tensione tra Israele e Iran cresceva, perché il primo minacciò il secondo di bombardare gli impianti nucleari iraniani in cui si supponeva che il regime di Teheran stesse arricchendo l'uranio. Al fine di ovviare a questa situazione, qualcuno inserì nella rete dell'impianto un virus informatico, denominato Stuxnet, proprio per attaccare i sistemi di controllo delle centrifughe. Il virus comincio ad infettare silenziosamente l'impianto nel 2008, per poi manifestarsi nel novembre del 2009. Secondo quanto si apprese in seguito, il governo USA avrebbe inserito, grazie all'aiuto del Mossad israeliano, il virus all'interno del sistema informatico della centrale.

Possiamo quindi dedurre che due sono gli elementi importanti in questo tipo di attacchi: possedere tecnologia all'avanguardia e un team di hacker in grado di attuare azioni sempre più complesse e delicate, come violare le difese dei paesi nemici, e il virus Stuxnet ne è un esempio.

Cyber terrorismo: origini e definizione

A coniare il termine cyber terrorismo fu negli anni '80 Barry Collins, al fine di spiegare l'impiego del cyber spazio per atti terroristici. Mentre nella decade successiva il dibattito si allargherà all'information warfare, in quel periodo la discussione era incentrata sul cyber terror e sul nuovo modo di concepire il mondo, alla luce dei rischi provenienti dalle nuove tecnologie. L'angoscia derivante da questa fase di profonda insicurezza può essere riassunta nella frase ″tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."[3]

L'interesse per questo nuovo campo, soprattutto nel periodo tra il 1997 e il 2001, portò numerosi studiosi ad interrogarsi su cosa fosse il cyber terrorismo, aumentando così la confusione sull'argomento. La nostra immagine del mondo cibernetico correva il rischio di diventare una grande diceria mediatica a cui eravamo costretti a dar credito senza i mezzi tecnici per interpretarla. Infatti, la sfida principale era quella di trovare una chiara definizione che si distanziasse da cybercrime, hacktivism, e anche dal cyber extremism.

In un primo momento, il cyber terrorismo è stato inteso come l'uso del cyberspazio da parte di organizzazioni terroristiche allo scopo di fare propaganda, oltre che spionaggio, e come mezzo offensivo. In seguito agli attacchi DoS, ovvero Denial of Sevice, ai danni dell'Estonia nel 2007, la sua definizione si è fatta più moderna e attenta alle eventuali ripercussioni reali, anche se rimane tuttora assai controversa. Una definizione condivisa potrebbe essere quella proposta da Akhgar, Staniforth e Bosco, ovvero:

[3] National Research Council. Computers at Risk: Safe Computing in the Information Age (Washington: National Academy Press, 1991)

> The use, making preparations for, or threat of action designed to cause a social order change, to create a climate of fear or intimidation amongst (part of) the general public, or to influence political decision-making by the government or an international governmental organisation; made for the purposes of advancing a political, religious, racial or ideological cause; by affecting the integrity, confidentiality, and/or availability of information, information systems and networks, or by unauthorised actions affecting information and communication technology based control of real-world physical processes; and it involves or causes:
> • violence to, suffering of, serious injuries to, or the death of (a) persons(s),
> • serious damage to a property,
> • a serious risk to the health and safety of the public,
> • a serious economic loss,
> • a serious breach of ecological safety,
> • a serious breach of the social and political stability and cohesion of a nation.[4]

Deep e Dark Web

Come detto in precedenza, internet è uno strumento potente per i terroristi, che fanno uso di bacheche online e chat room per condividere informazioni, coordinare gli attacchi, propagandare, raccogliere fondi e reclutare adepti. Questo non sempre può essere fatto nel World Wide Web, anche detto Surface Web, che costituisce solo il 4% del web, dove troviamo i siti indicizzati dai classici motori di ricerca come ad esempio Google, Yahoo ecc… Infatti, al di là di questa realtà superficiale, ci sono regioni opache chiamate Deep e Dark Web. Il primo fa riferimento ai cosiddetti siti ″nascosti″, che quindi non possono essere raggiunti attraverso i comuni motori di ricerca, ma ai quali si può accedere tramite un normale browser, se si conosce l'indirizzo. Qui possono essere svolte attività più o meno legali, ad esempio: accedere a forum web protetti da password, servizi di chat come Internet Relay Chat, condivisione di file, Peer-to-peer (P2P) e BitTorrent. L'anno scorso, un gruppo di hacker affiliato ad Anonymous, noto con il nome di Ghost Sec, ha attaccato la pagina web dell'ISIS su internet e sul Deep Web. Quest'azione fa parte di un più ampio progetto di Anonymous, che avrebbe lo scopo di eliminare l'ISIS su internet e sul Deep Web, dove i terroristi reclutano nuovi adepti per la Jihad.[5]

---

[4] Akhgar, Staniforth and Bosco. Cyber Crime and Cyber Terrorism Investigator's Handbook (Waltham: Syngress, 2014)
[5] Gibbs, Samuel. "Anonymous swaps Isis propaganda site for Prozac ad in trolling fight″. The Guardian, 26 Novembre 2015. Ultima modifica 27 Luglio 2016.

Il secondo, invece, il Dark Web o meglio Dark Net, dato che non utilizza il solito protocollo http, è un sottoinsieme del Deep Web, a cui si può accedere solo istallando un software specializzato, denominato TOR (The Onion Router) o I2P. Questi permettono di nascondere la propria identità in rete e il proprio indirizzo IP, facendo rimbalzare la connessione sui vari server sparsi per il mondo. Spesso, questo livello della rete è utilizzato per traffici illeciti, pornografia, attività criminali e transazioni illegali, effettuate tramite i bitcoin. Il Dark Web dà la possibilità di trasmettere informazioni anonimamente e rappresenta quindi il modo sicuro per comunicare tra attivisti, dissidenti ma anche per i terroristi. Per ragioni ovvie, questo spazio viene utilizzato anche dai servizi di intelligence e dalla polizia. Jared Cohen, direttore di Google Ideas, durante un talk su Waging a Digital Counterinsurgency presso Chatham House, disse: "terrorist groups like ISIS, they operate in the dark web whether we want them to or not".[6]

Ad ogni modo, rispetto al terrorismo per così dire ″tradizionale″, presenta pochi ma grandi vantaggi, come: anonimato, onnipresenza ed economicità. Tra i diversi obiettivi del cyber terrorismo troviamo network governativi, network finanziari, centrali elettriche. Questo perché sono innanzitutto più facili da danneggiare attraverso il cyberspazio e secondo perché la loro manipolazione è più probabile che crei il caos.

Cyber geography

Questa disciplina, come afferma il professor Kavé Salamatian dell'Université de Savoie, ha lo scopo di studiare le relazioni spaziali tra gli esseri umani e il cyberspace e, inoltre, ci fornisce elementi utili per comprendere come funziona la geopolitica dello spazio cibernetico.

Quando parliamo di internet e di cyberspazio, di solito facciamo riferimento ad un fenomeno virtuale e poco definito ma non è proprio così, perché il cyberspazio non potrebbe esistere senza infrastrutture fisiche che facciano da supporto e che sono appunto situate nello spazio geografico. Naturalmente, tutte queste infrastrutture necessitano di uno spazio geopolitico e dipendono sia dai limiti geografici che fisici, politici ed economici.

Le infrastrutture di cui parliamo possono essere singoli device, come smartphone o computer, ma possiamo considerare come parti fisiche di internet anche server e data center (dove si elaborano i dati di internet), Internet Exchange Points (che agevolano lo scambio dei dati), Network Operation Centers (che monitorano e gestiscono il traffico) ma soprattutto i cavi in fibra ottica, che permettono la connessione tra gli utenti in tutto il mondo.

---

https://www.theguardian.com/technology/2015/nov/26/anonymous-swaps-isis-propaganda-site-for-prozac-ad-in-trolling-fight

[6] Cohen, Jared. "Waging a Digital Counterinsurgency". Foreign Affairs, November/December 2015 Issue. Ultima modifica 18 Giugno 2016. https://www.foreignaffairs.com/articles/middle-east/digital-counterinsurgency

La maggior parte del traffico di internet passa attraverso cavi sottomarini, nello specifico circa il 95-99% [7], che collegano tutti i continenti. Uno degli snodi più importanti è quello del Mar Mediterraneo, che permette la connessione con l'Europa, con il Nord Africa, Medio Oriente e paesi dell'Oceano Indiano, attraverso il Canale di Suez. La costruzione di cavi è di conseguenza diventata un importante business e un modo per modificare gli equilibri connettivi tra i paesi e la loro governance.

Un caso interessante in questo senso è stato lo scandalo Datagate. Infatti, inseguito alla fuga di notizie del 2013 provocata da Edward Snowden, è stato dimostrato come gli Stati Uniti, attraverso l'agenzia NSA, controllassero a livello globale le informazioni e spiassero i leader degli altri paesi. La vulnerabilità di questi cavi è data da diversi fattori: infatti essi sono esposti non solo a danni involontari, come può essere il morso di uno squalo o lo scontro con una nave in passaggio, ma da veri è propri atti di sabotaggio da parte di altri governi o cellule terroristiche.

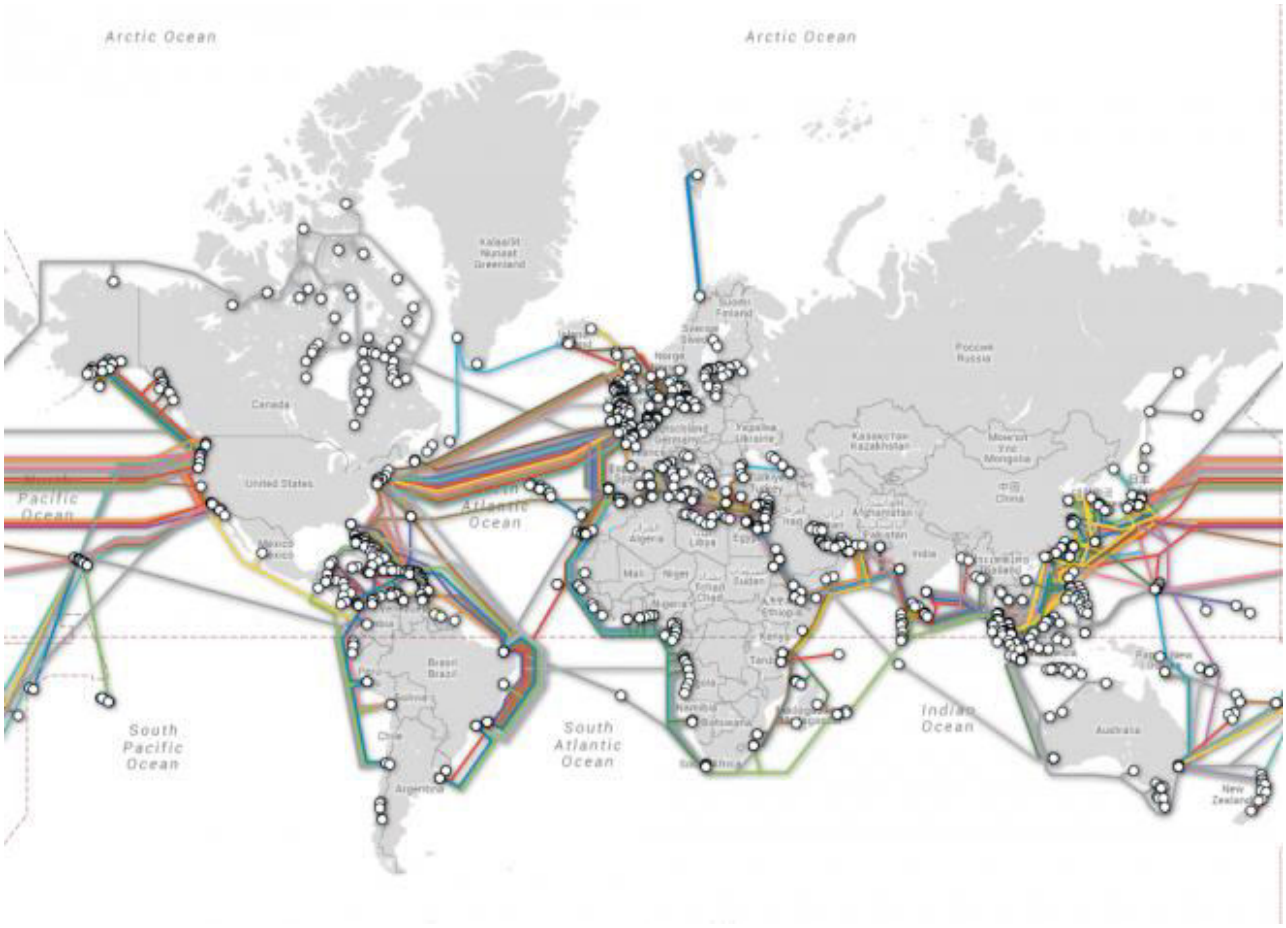


Figura 1 Mappa della rete mondiale di cavi sottomarini Fonte: Submarine Cable

[7] Frediani, Carola. "Ecco l'internet dei cavi sottomarini. Tra geopolitica e velocità della rete". L'Espresso, 29 Agosto 2014. Ultima modifica 2 Agosto 2016. http://espresso.repubblica.it/visioni/tecnologia/2014/08/29/news/ecco-l-internet-dei-cavi-sottomarini-tra-geopolitica-e-velocita-della-rete-1.178225

Capitolo II

Cyber terrorismo: realtà o finzione

Il terrorismo non è sicuramente un fenomeno nuovo; quello che è cambiato tuttavia è il modo in cui i terroristi comunicano e coordinano i propri attacchi, grazie all'utilizzo di internet. Una delle minacce considerate più pericolose è il cyber terrorismo o "Pearl Harbor digitale", attraverso il quale i terroristi possono distruggere le infrastrutture di altri stati con virus o trojan horse, utilizzando un semplice computer. Le opzioni a disposizione dei cyberterroristi sono descritte da Barry L. Collins nello scritto del 1997 "The Future of the CyberTerrorism: Where the Physical and Virtual Words Converge"[8]. Potrebbe trattarsi di un attacco al sistema che controlla il traffico aereo, provocando delle collisioni, fino alla manipolazione di una centrale che produce cereali per immettere più ferro in essi, in modo da incidere sulla dieta delle persone negativamente e provocare malattie e decessi.

Tra gli attacchi che Thomas Rid annovera tra i più importanti c'è quello ad una conduttura siberiana, che serviva il mercato europeo, passando prima per il Kazakistan e la Russia. Nel giugno del 1982, un satellite americano captò una fortissima esplosione. La causa sarebbe stata il cattivo funzionamento di un software di controllo, chiamato SCADA (Supervisory Control And Data Acquisition), rubato dal KGB in Canada. Quello di cui i sovietici non erano a conoscenza era che il software era stato modificato dalla CIA, in modo da produrre una pressione interna ben maggiore di quanto le condutture potessero sopportare. Il risultato fu la più imponente esplosione non nucleare mai vista dallo spazio, come ci dice nel libro "At the Abyss" Thomas Reed, un ufficiale del National Security Council al tempo. Tuttavia nessun media confermò questa esplosione, negata sia dall'Unione Sovietica che dalla CIA, che declassò l'avvenimento nel Farewell Dossier. Nell'eventualità che sia realmente accaduto, non si sa nemmeno se ci siano stati dei morti. Le prove sull'evento sono infatti così poche e dubbie che non si può certamente parlare di cyber terrorismo.

Un altro esempio spesso citato è l'attacco che ha colpito l'Estonia nell'Aprile 2007. All'epoca l'Estonia era uno dei paesi più connessi al mondo e quindi relativamente vulnerabile a questo tipo di attacchi. Il tutto cominciò circa due settimane prima del 9 maggio, il giorno della celebrazione della vittoria contro la Germania nazista in Russia. Nello stesso periodo, le autorità di Tallin decisero di spostare un memoriale russo al milite ignoto risalente alla seconda guerra mondiale dal centro alla

[8] Collins, Barry L. "The Future of the CyberTerrorism: Where the Physical and Virtual Words Converge". Istitute for Security and Intelligence, 1997. Ultima modifica 20 Agosto 2016. http://www.crime-research.org/library/Cyberter.htm

periferia della città. Ciò provocò l'indignazione della Russia e dei cittadini di lingua russa, che scesero in piazza tra il 26 e il 27 aprile, dando luogo a scontri violenti.
Tali sommosse furono accompagnate anche da attacchi cyber, che si servirono inizialmente di metodi poco articolati, come attacchi ping flood o Dos, per divenire successivamente più sofisticati. A partire dal 30 aprile, aumentò il volume di DDos, dando luogo al più vasto attacco mai visto, che si protrasse per tre settimane. L'operazione raggiunse l'apice il giorno della succitata ricorrenza: 58 siti furono oscurati in una volta, compreso quello della più grande banca estone, la Hansapank.
Tuttavia, tale protesta non ebbe effetti considerabili sul commercio, il governo o la società. La principale conseguenza a lungo termine fu che il governo estone ottenne dalla NATO l'istituzione di un'agenzia permanete a Tallin, il Cooperative Cyber Defence Centre of Excellence.
Rimangono sconosciuti i mandanti degli attacchi. Il governo estone puntò il dito contro il Cremlino ma né gli esperti dell'Alleanza Atlantica né la Commissione Europea trovarono prove del coinvolgimento della Russia nella protesta.
Anche questo attacco non può quindi considerarsi cyber-terrorismo, in quanto si configura più come un atto di protesta non violento.
Nel 2006, sotto l'amministrazione di Bush Junior e poi Obama, grazie alla collaborazione tra intelligence americana e israeliana, venne alla luce la prima arma cibernetica, la già citata Stuxnet. Lo scopo era quello di danneggiare o almeno ritardare lo sviluppo degli impianti nucleari in Iran. L'intervento ha quindi portato a due risultati, ovvero disinnescare la minaccia atomica del regime di Ahmadinejad e disincentivare Israele dall'attaccare l'Iran. Infatti, il virus non si limitava solo a rubare dati o a bloccare i software ma intaccava anche il lavoro delle turbine, che erano costrette a girare sempre più velocemente, senza che il sistema segnalasse alcuna anomalia. Per il contagio vennero utilizzate chiavette USB. Tuttavia, Tel Aviv potenziò il virus e lo rese capace di propagarsi più facilmente. A questo punto, esso dilagò anche al di fuori della centrale di Natanz, provocando dissesti su altre reti, che non erano obiettivi dell'operazione. A novembre 2013, il malware era ancora operativo. Infatti, secondo la compagnia di sicurezza informatica Kaspersky, il virus avrebbe attaccato delle centrali atomiche russe. Non si tratta, tuttavia, di un episodio di cyber terrorismo, dal momento che l'obbiettivo dell'operazione non era quello di incutere terrore ma di comunicare all'Iran che il suo programma di arricchimento dell'uranio non sarebbe stato tollerato.
Una delle minacce più recenti è sicuramente quella del gruppo terroristico dello Stato Islamico, che si è dimostrato piuttosto abile con le nuove tecnologie. Questo non ha fatto altro che aumentare i dubbi sull'eventualità di un attacco cyber da parte loro. Attacchi che non si sono mai verificati, date le scarse risorse e capacità di hacking dei militanti. Basti pensare che gli hacker cinesi, che sono stati accusati di aver attaccato le imprese degli Stati Uniti, hanno bisogno del sostegno delle autorità

cinesi per effettuare le proprie operazioni. "You need some resources. You need access to certain kinds of technology. You need to have hardcore programmers" ha dichiarato Jim Lewis del Centro per Studi Strategici e Internazionali. "ISIS doesn't have those capabilities."[9]

A dimostrazione di questa tesi, un paio di anni fa, durante un attacco violento tra Gaza e Israele, gli hacker di entrambe le parti sono riusciti a lanciare solo attacchi Distributed Denial of Service (DDoS), che comportano l'utilizzo di più server per sovraccaricare un sito web e disattivarlo per un breve periodo.

Cyber spionaggio

Nonostante sia dubbio che si siano effettivamente verificati episodi di cyber terrorismo, è importante notare che anche altre sono le vie per farsi strada nel web e minare la tranquillità degli stati. Internet può essere infatti utilizzato come strumento offensivo da parte dei così detti hacktivisti o sfruttato dai terroristi per reclutare sostenitori, finanziarsi e fare propaganda. Una minaccia è sicuramente costituita dal cyber spionaggio. Una definizione è quella del Financial Times, secondo cui "cyber espionage describes the stealing of secrets stored in digital formats or on computers and IT networks."

I suoi fautori sono in genere agenti del governo altamente addestrati o hacker che agiscono di propria iniziativa o in nome di una causa più grande. Gli autori rimangono in genere anonimi, come nel caso di "Titan Rain", una serie di attacchi che colpirono i sistemi governativi e militari americani nel 2003 e che si protrassero per cinque anni. Nonostante l'operazione fosse partita da computer cinesi, non è chiaro se le agenzie di sicurezza di Pechino fossero effettivamente dietro gli attacchi. Il Pentagono stimò che gli hacker avessero sottratto tra i dieci e i venti terabyte di dati dai network del Dipartimento di Stato.

Un altro esempio è "Ghost Net", un'operazione di spionaggio internazionale, probabilmente di origini cinesi, scoperta da Ron Delbert e il suo team dell'Università di Toronto nel marzo 2009. Gli hacker avevano infettato 1.295 computer tra ministeri degli affari esteri, ambasciate, organizzazioni internazionali, agenzie di comunicazione e organizzazioni non-governative in 103 paesi, prendendone il pieno controllo.

Solo raramente i governi rivelano informazioni sulle operazioni andate buon fine o lo fanno con molta parsimonia. Inoltre, non sempre i ricercatori sono in grado di gettare luce su questi fenomeni. Gli episodi di cyber spionaggio, nonostante i cospicui investimenti statali nell'ambito della difesa, crescono rapidamente, contro entità sia pubbliche che private.

---

[9] Frizzell, Sam, "Experts Doubt ISIS Could Launch Major Cyberattack Against the U.S.". Time, 19 Settembre 2012. Ultima modifica 12 Settembre 2016. http://time.com/3403769/isis-cyberattack/

Propaganda terroristica

Per quanto riguarda la propaganda, il professor Anthony Pratkanis osservava già nel 1999: "what you're seeing now is just the first round of what will become an important, highly sophisticated tool in the age-old tradition of war- time propaganda […] The war strategists should be worried about it, if they aren't yet."[10]

La presenza dei terroristi su internet e sui social network, infatti, è notevolmente aumentata negli ultimi anni. In particolare, notiamo come i gruppi jihadisti abbiano mostrato grande abilità nell'uso di questi strumenti: lanciano campagne ben organizzate, reclutano, promuovono e glorificano i propri atti di terrorismo.

Come ci spiega il report dell'Europol del 2016, negli ultimi due anni le organizzazioni terroristiche pare abbiano cambiato la propria strategia comunicativa, adattandosi all'offerta delle piattaforme social e cercando di aggirare le autorità, che provano a contenere il fenomeno, grazie anche alla collaborazione con i colossi della rete. Tale cambiamento è riscontrabile anche nel confronto tra al-Quaeda di Bin Laden e l'ISIS di Al-Baghdadi. Il primo amava fare ampi discorsi in cui spiegava i rapporti causa-effetto tra gli attacchi terroristici che si abbattevano sull'occidente e ciò che avveniva in Medio-oriente, in cui gli Stati Uniti erano la causa e al-Quaeda l'effetto. Più semplicemente, il secondo intermezza le parole con immagini violente, persone che muoiono bruciate vive e militanti che tagliano teste, in modo da catturare l'attenzione anche di chi non è interessato alla politica internazionale.

Difatti, la propaganda dell'ISIS ha avuto un grande successo nel reclutamento, grazie alla sua campagna mediatica basata su forza e capacità diffusiva. Come riporta il the Guardian[11], i responsabili della propaganda dell'ISIS sfruttano gli hashtag più popolari (come ad esempio quello sul referendum scozzese) e i forum per assicurarsi un'ampia distribuzione dei loro contenuti su Twitter e YouTube. I gruppi jihadisti hanno inoltre capito che devono rapidamente raggiungere un certo livello di diffusione, per evitare i controlli di questi ultimi, passando prima per justpaste.it, un sito che permette di pubblicare testi anonimamente.

Questi video hanno, inoltre, una qualità sorprendentemente alta: sono infatti girati in HD e hanno un proprio logo, ovvero quello di Al Hayat Media Center[12], la principale casa produttrice dell'organizzazione terroristica e sono in lingua inglese. Al Hayat Media è infatti rivolto a chi non parla arabo e soprattutto agli spettatori giovani.

---

[10] Citato in Rick Montgomery, "Enemy in Site—It's Time to Join the Cyberwar," *Daily Telegraph* (Australia), April 19, 1999, p. 19.

[11] Malik, Laville, Cresci e Gani. "Isis in duel with Twitter and YouTube to spread extremist propaganda". The Guardian, 24 Settembre 2014. Ultima modifica 22 Agosto 2016. https://www.theguardian.com/world/2014/sep/24/isis-twitter-youtube-message-social-media-jihadi

[12] Al Hayat Media Center. https://alhayatmedia.wordpress.com/ Ultima mofifica 15 Agosto 2016.

Nel video intitolato “There is no Life without Jihad”[13], primo video ad essere messo in rete dalla casa produttrice, vediamo dei giovani tra le palme che, con atteggiamento calmo, rassicurano il pubblico sul fatto che comprendono quanto sia difficile essere mussulmani in un paese occidentale e li esortano ad aderire al gruppo terroristico e a vendicare le morti causate dal coinvolgimento militare occidentale in Medio Oriente.

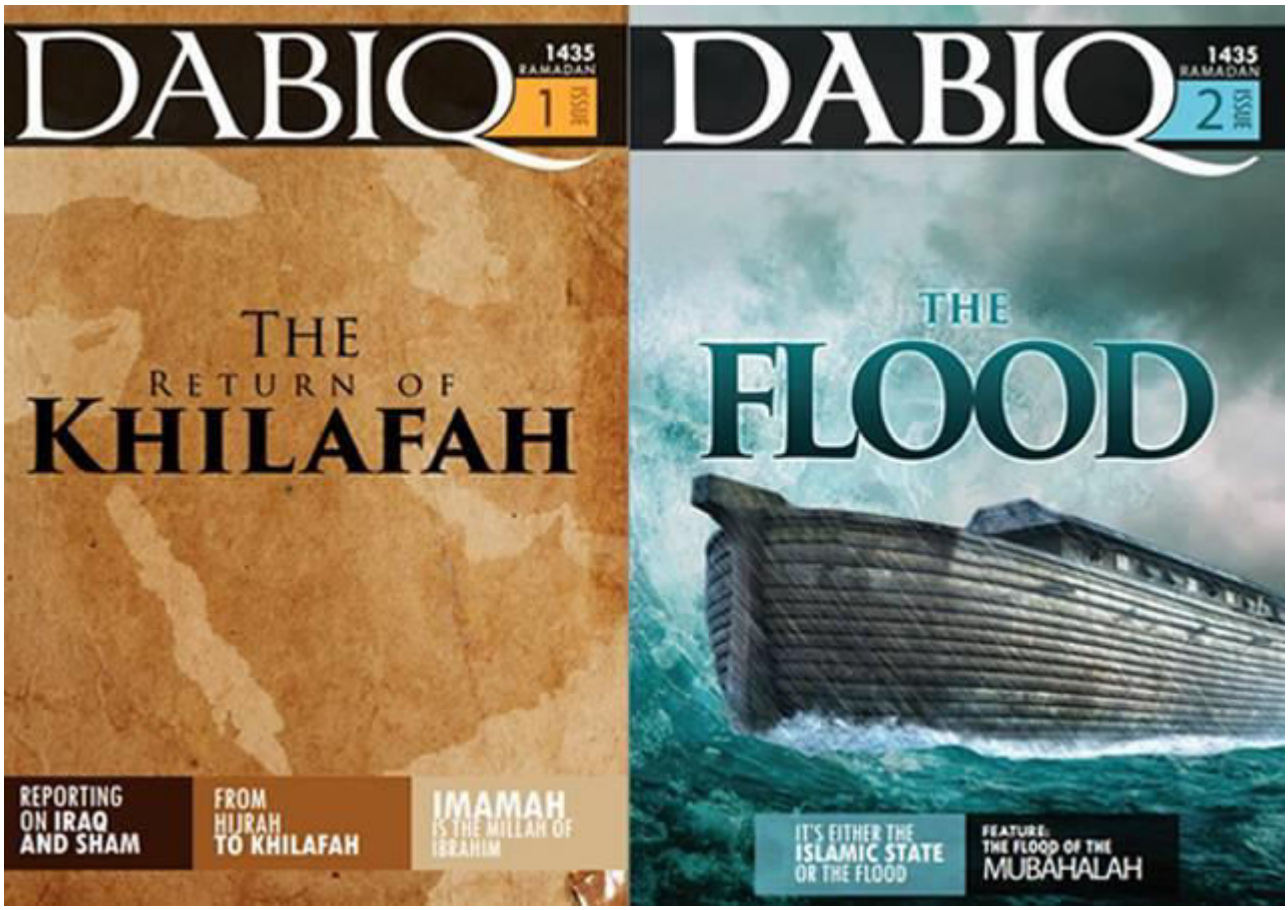
I loro programmi sono variegati. “Eid Greetings from the Land of Khilafah”, per esempio, filmato nella città occupata di Raqqa in Siria, si svolge come un documentario di viaggio. I combattenti dell'ISIS, provenienti da Finlandia, Indonesia, Belgio, UK e altri paesi, parlano di come sia bello essere lì. “I don’t think there’s anything better than living in the land of khilafah,” dice Abu Abdullah al-Habashi, dalla Gran Bretagna. “We don’t need any democracy, we don’t need any communism or anything like that, all we need is sharia.” Le interviste sono intervallate da scene vivaci, che raccontano la vita di strada e di bambini alle fiere. Il tutto si conclude con lo slogan: “I wish you were here.”

Allo stesso tempo, non hanno alcuno scrupolo nel mostrare, come già detto, vere e proprie esplosioni, scontri a fuoco, esecuzioni e cadaveri. I colori sono saturi e fanno risplendere i combattenti. Le detonazioni vengono mostrate in slow motion e l’apposita colonna sonora compare in stile karaoke. Nei primi quattro mesi del 2015 lo Stato islamico ha pubblicato video che ritraggono l'esecuzione di "spie russe" da parte di un bambino, massacri di cristiani copti e etiopi, orribili torture e la morte di un pilota giordano, bruciato vivo

La stessa rivista online, “Dabiq”, dal nome di una città siriana legata al mito dell’apocalisse, ha lo scopo di reclutare jihadisti e educare le menti dei giovani mussulmani ad un nuovo modo di guardare e pensare il mondo. Notiamo un uso strategico delle immagini, che raffigurano decapitazioni, moschee sciite distrutte e bambini dilaniati dalle bombe americane. Inoltre, gli articoli sono scritti in varie lingue, incluso l’inglese, al fine di raccogliere un pubblico sempre più vasto. Le diverse sezioni sono colorate in base al tipo di contenuto (articoli, rapporti ecc..); questo a dimostrazione dello studio accurato che c’è dietro. Nella prima uscita troviamo le dichiarazioni generali del califfato (*khilafah*), nel secondo si cerca di stupire e invogliare i mussulmani a unirsi allo stato islamico e si provano a spegnere le voci di dissenso fra i suoi sostenitori, e così via con gli altri numeri.

[13] Wall Street Journal, 20 Giugno 2014. “New ISIS recruitment Video Aimed At Western Muslims” Ultima modifica 20 Agosto 2016. http://www.wsj.com/video/new-isis-recruitment-video-aimed-at-western-muslims/749B2C6E-A554-4522-A1A4-CF5CAAADD984.html

In sostanza, "avere un'immagine di successo è il modo migliore per attirare nuovi militanti. Ecco perché l'ISIS fa un uso maniacale della propaganda: vuole diffondere un'idea vincente di sé"[14].



Dentro la macchina della propaganda ISIS

L'innovazione più significativa apportata dallo Stato Islamico riguarda la comunicazione, che vede team dall'Africa occidentale all'Afghanistan lavorare senza sosta per diffondere il "brand" del califfato. Le sue strategie comunicative sono state approfonditamente analizzate dal report del ricercatore della Quillam Foundation, Charlie Winter. Secondo lo studio, il califfato rilascia in media 38 slot di propaganda al giorno, tra foto, audio, video e testi, rendendo vane misure repressive come la censura. Anche il tentativo di trovare una contro-narrativa per esautorare il brand del gruppo è fuori luogo, in quanto dovrebbe piuttosto essere elaborata una narrativa

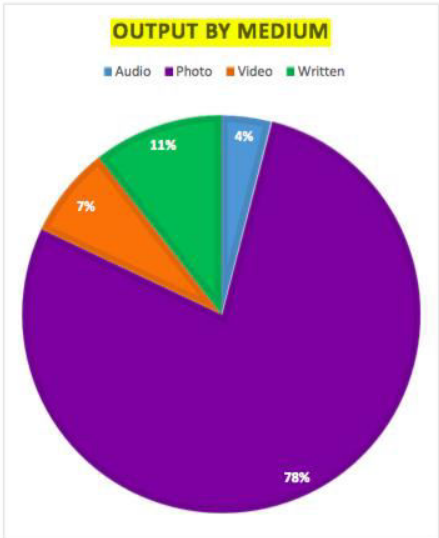


Figura 1: Fonte:Documenting the virtual "Caliphate"

[14] Orsini, Alessandro. "ISIS: I terroristi più fortunati del mondo e tutto ciò che è stato fatto per favorirli". (Milano: Rizzoli, 2016), 20

alternativa.

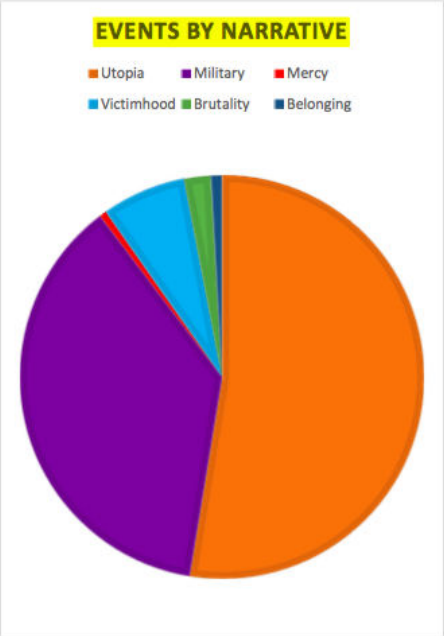


Figura 3: Fonte:Documenting the virtual "Caliphate"

É fondamentale sottolineare che, a dispetto di quanto riportato dai giornali e politici occidentali, la violenza non è l'unico contenuto della produzione mediatica dello stato islamico. I temi principali classificati dallo studio sono pietà, appartenenza, brutalità, vittimismo, guerra e utopia, anche se gli ultimi tre sono prevalenti. Più della metà dei contenuti si focalizza sulla vita dei civili nei territori occupati dall'ISIS, descrivendo uno scenario fatto di attività economiche, eventi sociali, ordine pubblico e fervore religioso. In questo modo, il gruppo attrae sostenitori sia dal punto di vista ideologico che politico. Allo stesso tempo, la propaganda insiste molto sul tema della guerra e delle operazioni militari, arrivando a mettere in scena dei falsi attacchi per perpetuare l'idea che lo stato Islamico sia costantemente sull'offensiva. Il pubblico a cui esso si rivolge, tuttavia, è più regionale rispetto al passato, con l'obbiettivo di scoraggiare il dissenso e gli atti di ribellione nei territori controllati dal califfato.

In quanto ai mezzi di diffusione, in passato i gruppi jihadisti tendevano a prediligere i forum in lingua araba protetti da una password per comunicare e scambiarsi idee. Tali forum sono ancora attivi ma hanno assunto un ruolo secondario rispetto ai social media open source e peer to peer, grazie ai quali il gruppo ha registrato un successo senza precedenti nel recruitment. Dati i problemi etici e legislativi causati dall'uso delle loro piattaforme, le grandi corporation hanno reagito con forza. Facebook, per esempio, ha introdotto una stretta regolamentazione che ha permesso di espellere la propaganda jihadista dalla piattaforma. Lo stesso non si può dire di Twitter, che fatica ancora a raggiungere questo obbiettivo.

A partire dall'estate 2014, lo stato islamico ha smesso di utilizzare account ufficiali, perché più facili da individuare e sospendere, operando soprattutto attraverso gli hashtag. Questi ultimi non possono essere né bloccati né sospesi da Twitter e consentono di raggiungere in poco tempo una vastissima diffusione.

Soluzioni per il contrasto alla propaganda terroristica online

Il primo luglio 2015, l'Europol ha lanciato l'unità Internet Referral per combattere la propaganda terroristica su Internet. Essa si propone i seguenti obiettivi:

- coordinare e condividere i compiti di identificazione e segnalazione dei contenuti di matrice terroristica;
- effettuare e supportare, in modo efficiente ed efficace, i rinvii;
- sostenere le autorità competenti, fornendo analisi strategiche e operative;
- agire come Centro europeo di eccellenza per i compiti sopra elencati[15].

Questa unità si avvale di rapporti fiduciari con le autorità di polizia in tutta l'UE. Inoltre, si rifà a canali di comunicazione e database altamente sicuri. Dimitris Avramopoulos, Commissario per la migrazione, gli affari interni e la cittadinanza, ha dichiarato:

> The recent terrorist attacks in France, Tunisia and Kuwait have shown once again how important it is to combat terrorist threats with determination. The establishment of the EU Internet Referral Unit is one of the first deliverables of the European Agenda on Security. It will provide operational support to Member States on how to tackle more effectively the challenges of detecting and removing the increasing volume of terrorist material on the internet and in social media. The launch of this important initiative is the result of our common efforts. The success of this initiative will depend on the continued good cooperation and contributions from all stakeholders[16].

Secondo il report dell'anno scorso del Homeland Security Commitee, l'ISIS, grazie all'uso sofisticato di internet, alla sua presenza sui social media e allo sfruttamento della guerra civile in Siria, è stata in grado di attirare più di 25.000 foreign fighters per unirsi alle sue fila in Iraq e Siria. Oltre 4.500 sono di nazionalità occidentale, di cui 250 cittadini statunitensi. A gennaio 2016, l'amministrazione Obama ha rivisto la sua strategia per combattere la propaganda online dell'ISIS, dato che gli sforzi fatti in precedenza sono risultati inefficaci. È stata quindi creata una task force antiterrorismo, che si trova presso il dipartimento di Sicurezza Nazionale statunitense e che dovrebbe coinvolgere decine di altre agenzie. È stato inoltre rilanciato il piano precedente migliorandolo, allo scopo di erodere il fascino che lo Stato Islamico suscita con la sua propaganda e di aiutare gli alleati a localizzare e fermare la produzione di video e altro materiale in inglese. Obama, dopo aver annunciato i piani alla Casa Bianca, si è recato in California per avere sostegno anche dalle aziende della Silicon Valley, come Apple, Facebook ecc… "The idea is to come out

[15] http://data.consilium.europa.eu/doc/document/ST-7266-2015-INIT/en/pdf
[16] Europol. "Internet ReferralUnit Combat Terrorist and ViolentExtremist Propaganda". Ultima modifica 26 Agosto 2016. https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda

with a work plan," ha detto un funzionario dell'amministrazione. "Nobody wants to have their platforms co-opted by terrorists."[17] L'FBI ha fatto pressioni per modificare i sistemi di codifica di smartphones e altri dispositivi, come è accaduto per il caso di San Berardino. Tuttavia, sono state fatte delle resistenze da parte delle aziende.

Secondo il direttore di Google Ideas, Jared Cohen, sarebbe necessario confinare i gruppi terroristici, come l'ISIS, nel Dark Web, dove la loro propaganda non avrà la stessa facilità diffusiva. Inoltre, propone di cancellare immediatamente i loro account, così che le persone non possano entrarvi in contatto. La UK internet Counter Terrorism Unit fa sapere, infatti, che rimuove da Internet 1.000 articoli, i cui contenuti violano la legislazione sul terrorismo, ogni settimana, di cui 800 hanno a che fare con la Siria e l'Iraq[18].

A scendere in campo contro l'Isis non sono solo le istituzioni ma troviamo anche gli hacker, come ad esempio Anonymous. Le campagna più attiva, che ha più che altro lo scopo di informare, è #opIceIsis, che gira intorno a due account Twitter: @TheAnonMessage e @OpIceIsis. Infatti, in un'intervista a France24[19], un membro del gruppo ha spiegato le motivazioni dietro questa campagna, ovvero sottolineare la responsabilità degli USA nella nascita dell'ISIS, ribadire che la religione islamica non è quella di cui si fa interprete lo Stato Islamico e mostrare ciò che accade in Iraq[20]. Troviamo anche The Jester, un gruppo di hacker filo-americani e filo-governativi, da sempre nemici di Anonymous, che sono riusciti a far chiudere numerosi profili di militanti o simpatizzanti ISIS. Un esempio è anche il gruppo turco RedHack di ispirazione marxista-leninista, molto vicino ad Anonymous e ai curdi, quindi profondamente anti-ISIS.

Armi cibernetiche

Secondo alcune stime del Market info Group LLC, nel decennio 2014/2024, il mercato mondiale delle cosiddette cyber weapons supererà i 3000 miliardi di euro. Le cause di tale fenomeno sono molteplici:

- numero crescente delle minacce alle infrastrutture e alle industrie critiche;

[17]Miller e De Young. "Obama administration plans shake-up in propaganda war against ISIS". The Washington Post, 8 Gennaio 2016. Ultima modifica 29 Agosto 2016. https://www.washingtonpost.com/world/national-security/obama-administration-plans-shake-up-in-propaganda-war-against-the-islamic-state/2016/01/08/d482255c-b585-11e5-a842-0feb51d1d124_story.html

[18]Gov.uk. "Radicalization". Ultima modifica 1 Settembre 2016. https://www.gov.uk/government/publications/online-radicalisation/online-radicalisation#question-time-live-with-detective-chief-superintendent-sue-southern-from-west-midlands-police

[19] Borges, Anelise. "Anonymous 'declare cyber war' on IS militants". France24, 23 Settembre 2014. Ultima modifica 5 Settembre 2016. http://www.france24.com/en/20140920-tech24-Anonymous-VS-ISIS-online-war-against-terrorism/

- aumento delle spese per la difesa;
- aumento delle iniziative aziendali;
- crescita della preferenza da parte dei governi delle armi cibernetiche negli scontri bellici.

I paesi all'avanguardia in questo settore sono sicuramente Stati Uniti, Cina, Russia, Corea del nord, Corea del Sud e Iran. Dei paesi appena citati, la Cina pare sia quello che si svilupperà di più in quanto, dati alla mano, gli utenti sono 400 milioni, 1/3 della popolazione mondiale, con un aumento di 50 milioni all'anno rispetto ai 250 milioni americani. Se saliamo di livello, ovvero quello globale, su una popolazione stimata nel 2020 di 7.5 miliardi, si ipotizza che gli utenti di internet saranno 4,8 miliardi. Grazie a questi dati, è facile intuire che in futuro ci sarà un nuovo e grande tipo di conflitto, ovvero su chi deciderà le regole del cyberspazio, avendo in mano la rete e quindi il "mondo".

Quindi, si farà sempre più ricorso alle armi cibernetiche, perché meno costose rispetto a quelle cinetiche. Infatti, basti pensare che un caccia costa tra gli 80 e i 120 milioni di dollari, mentre si valuta che un'arma cibernetica parte dai 300 fino ai 50 mila dollari. Inoltre, questo non è l'unico vantaggio: esse sono più precise, efficaci, lanciabili da qualunque parte del mondo, per lo più anonime e personalizzabili (tailored of the target). Tuttavia, esse possono essere definite "one-shot", perché quando vengono rivelate non possono più essere utilizzate, dato che non porterebbero allo stesso effetto sorpresa della prima volta, vanificando o indebolendo così l'attacco.

Questo tipo di armi offensive sono di tre tipi: semplici, moderatamente complesse e complesse. Nel primo caso si sfrutta la mancanza di autenticazione, nel secondo si individua il processo di controllo e nel terzo viene alterato il processo in modo che il bersaglio non si accorga del pericolo. Tuttavia, non tutte le strutture sono collegate ad internet, per questo si usano altri strumenti per intaccarle come la chiavetta USB. Un esempio è certamente il caso Sunxet, che vide coinvolta una centrale nucleare in Iran. Per quanto riguarda le cyber weapons difensive, esse sono più costose.

Se invece volessimo dare una definizione di arma cibernetica, cominciamo con il dire che non ve n'è ancora una accettata a livello internazionale. Una definizione molto elementare è quella di Umberto Gori, riportata nel 2014 su Cyber Warfare: "uno strumento informatico costituisce una cyber weapons se, e soltanto se, ha una valenza almeno potenzialmente letale, e cioè distruttiva di cose o persone". Secondo la definizione di Stefano Mele, si tratta invece di "un'apparecchiatura, un dispositivo, ovvero qualsiasi insieme di istruzioni informatiche dirette a danneggiare illecitamente un sistema informatico o telematico avente carattere di infrastruttura critica, le sue informazioni, i suoi dati o i suoi programmi, in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione totale o parziale, o l'alterazione del suo funzionamento". Dunque, come già affermato, il fatto che non ci sia una definizione concordata a livello internazionale non permette di stabilire un quadro

giuridico capace di valutare in maniera oggettiva la gravità della minaccia e la responsabilità di chi ha commesso il fatto, lasciando così allo stato ampia discrezionalità al riguardo.
Un tentativo, però, è stato fatto con il Tallin Manual on the International Law Applicable to Warfare, scritto da un gruppo indipendente di esperti, che individua tre principi importanti: riservatezza, integrità e disponibilità.
In ordine di pericolosità riconosciamo:

- Attacchi Denial of Service (Dos) e vandalismo web, in cui lo scopo è di sovraccaricare i siti internet. Questo attacco mira a mettere fuori uso temporaneamente i sistemi colpiti, senza avere conseguenze di lungo termine.
- Attività di raccolta di dati sensibili, ci si impadronisce di password, documenti, progetti. Da qui parte l'attività di spionaggio che può portare anche alla cancellazione dei dati del nemico che dovrà poi riscrivere tutto.
- Attacco alle apparecchiature, dove si mira a distruggere le apparecchiature militari, i satelliti e i sistemi di comunicazione.
- Attacchi diretti alle infrastrutture, andando a colpire quelle strutture che rogano servizi essenziali come energia, acqua ecc.

Sulla base di questi attacchi, un sistema di difesa all'altezza dovrebbe essere basato su:

- controllo delle reti;
- rivelazione e classificazione dell'attacco;
- decidere appropriate contromisure.

Attivismo e Hactivism

Internet rappresenta lo strumento ideale per esprimere la propria opinione e quindi anche il proprio dissenso. Gli attivisti, ovvero militanti impegnati politicamente e socialmente, utilizzano il web per informare su questioni rilevanti e su come sostenere la propria causa e le loro manifestazioni di piazza possono sfociare anche in atteggiamenti violenti. L'hacktivism è invece definito dalla Prof. Dorothy Denning "the marriage of hacking and activism". Il modus operandi degli hacktivist è più sottile, perché non prevede manifestazioni di piazza ma agisce completamente sul web. Le azioni tipiche sono sit-in elettronici, email a raffica, virus, worm e spoofing dei siti web. La nascita dell'hacktivism si fa risalire al settembre del 1999, quando un gruppo chiamato Electronic Disturbance Theater (EDT) organizzò una serie di sit-in virtuali contro il presidente messicano Zedillo, la Casa Bianca, il Pentagono e altre istituzioni. Durante uno di questi sit-in elettronici, i siti di tali istituzioni vennero colpiti da un attacco Denial of Service (DoS), che porta ad un sovraccarico delle reti e del server, causando la paralisi e l'oscuramento del sito in questione. Questo tipo di

attacchi non sono però innocui come potrebbero sembrare. Un esempio è l'assalto del febbraio del 2000 verso alcuni siti di e-commerce, tra cui eBay, Amazon.com, Yahoo!, ecc… Gli esperti sostennero che dietro questo attacco si celavano settimane, se non mesi, di preparazione. Infatti, il software responsabile dell'operazione fu caricato su centinaia di computer in tutto il mondo, che divennero, all'insaputa dei proprietari, ingranaggi di questa potente macchina[21], causando notevoli danni economici. A marzo dello stesso anno anche un altro gruppo, The Electrohippies, ha tentato di bloccare con lo stesso tipo di attacco il sito della Banca Mondiale e del Fondo Monetario Internazionale. Tuttavia, non tutti i gruppi utilizzano metodi non violenti per promuovere i propri ideali. Alcuni siti, ad esempio, forniscono informazioni su dottori e cliniche che offrono servizi di aborto, incitando all'uso della violenza contro di loro. Diversi governi hanno cominciato a vedere l'hacktivism come una potenziale minaccia e sono state per questo approvate delle leggi, come quella nel Regno Unito del 2000.

[21] Richtel e Brinkley. "Spread of Attacks on Web Sites Is Slowing Traffic on the Internet". Th New York Times, 10 Febbraio 2000. Ultima modifica 21 Settembre 2016. "Spread of Attacks on Web Sites Is Slowing Traffic on the Internet".

Capitolo III

Sfida alle libertà civili

Il concetto di "conflitto tra libertà e autorità" descritto da Mill si riferisce alla tensione tra diritti individuali e regole imposte dall'autorità pubblica, che esercita il proprio potere sulla società civile. Con la rivoluzione informatica e la pervasiva diffusione di informazioni e tecniche di comunicazione, le società contemporanee stanno attraversando una nuova fase di tale conflitto, che si sposta nella cyber-sfera e riguarda il bilanciamento tra libertà individuali e misure di cyber-security.

Negli ultimi due decenni, la governance e la sicurezza della cyber-sfera sono passati nelle mani dell'autorità pubblica. Ciò ha comportato un inasprimento di tale conflitto, dovuto anche alla natura stessa della cyber-sfera. I dati che la compongono, infatti, sono per natura malleabili: possono essere immagazzinati, elaborati, modificati da parti terze e possono rivelare informazioni personali sensibili, facilitando misure di controllo e sorveglianza. Diventa quindi possibile per i fautori di tali misure minacciare il diritto alla privacy e all'anonimato degli utenti. Allo stesso tempo, dal momento che la cyber-sfera è ormai divenuta una parte costitutiva delle società contemporanee, si averte sempre più l'esigenza di difenderla da possibili minacce e attacchi cyber. Tale necessità è spesso invocata a giustificazione della sorveglianza pervasiva a cui siamo sottoposti e delle violazioni dei diritti individuali.

Lo scandalo NSA (National Security Agency) del 2013 offre un esempio tangibile di come il potere statale possa declassare tali diritti. Esso ha inoltre portato alla luce la necessità di riequilibrare il rapporto tra cyber-security e diritti individuali nella cyber-sfera. Con le parole di Obama: "we have to strike the *right balance* between protecting our security and preserving our freedoms ... But given the history of abuse by governments, it's right to ask questions about surveillance – particularly as technology is reshaping every aspect of our lives"[22].

Il caso Datagate

Come ha dichiarato al The Guardian, quando Edward Snowden, esperto informatico e impiegato nella società di consulenza Booz Allen Hamilton, lasciò il proprio paese il 20 maggio 2013 per

[22] The White House. "Remarks by the President in a Press Conference". Ultima modifica 25 Settembre 2016. https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference

recarsi ad Hong Kong, sapeva che non vi avrebbe più fatto ritorno. Il ventinovenne aveva cominciato a raccogliere informazioni sui massicci programmi di sorveglianza della National Security Agency americana nel 2012, con l'intenzione di svelare all'opinione pubblica mondiale un sistema in grado di spiare le comunicazioni dei cittadini indiscriminatamente e in qualunque momento[23].

Il primo articolo fu pubblicato il 6 giugno 2013 da Glenn Greenwald sul succitato giornale inglese, rendendo di dominio pubblico l'esistenza del programma "PRISM", che permetteva di immagazzinare le comunicazioni digitali degli utenti americani dirette verso l'estero. Esso vedeva il coinvolgimento di colossi del web come Apple, Facebook, Microsoft, Skype e Yahoo, che si affrettarono a negare qualunque coinvolgimento. Lo stesso Mark Zuckerberg dichiarò che "Facebook non fa e non ha mai fatto parte di un programma che consegni un accesso diretto ai nostri server al governo degli Stati Uniti o a qualsiasi altro governo"[24].

Lo scandalo raggiunse ben presto dimensioni mondiali, alimentato dalle informazioni pubblicate giornalmente dal The Guardian e dal Washington Post, mentre negli USA cominciava la caccia alla talpa. Snowden ammise poco dopo le proprie responsabilità nella fuga di informazioni, lasciando poi la Cina per recarsi a Mosca. Pare che il suo intento iniziale fosse quello di stabilirsi a Cuba o in America Latina ma non poté lasciare l'aeroporto per settimane, a causa dell'annullamento del passaporto da parte delle autorità statunitensi. Il primo agosto ottenne, infine, un anno di asilo in Russia.

Lo stesso mese, il The Guardian rese nota l'esistenza del più ampio programma di sorveglianza diretto dall'NSA, XKeyscore, che permetteva di accedere alle email, chat online, metadati e cronologia di milioni di utenti in tutto il mondo. Riempiendo un semplice form, era addirittura possibile accedere all'attività online dei cittadini in tempo reale, senza il bisogno di alcun mandato o autorizzazione da parte dell'NSA. "Seduto alla mia scrivania", ha dichiarato Snowden, "potrei intercettare chiunque, voi giornalisti o il vostro commercialista, un giudice federale o anche il presidente, basta avere una mail personale"[25].

---

[23] Lütticke, Markus. "A chronology of the NSA surveillance scandal". Deutsche Welle, 31 Ottobre 2013. Ultima modifica 25 Settembre 2016. http://www.dw.com/en/a-chronology-of-the-nsa-surveillance-scandal/a-17197740

[24] Il Post, 8 Giugno 2013. "La risposta di Zuckerberg sul caso PRISM". Ultima modifica 25 Settembre 2016. http://www.ilpost.it/2013/06/08/la-risposta-di-zuckerberg-sul-caso-prism/

[25] Greenwald, Glenn. "XKeyscore: NSA tool collects 'nearly everything a user does on the internet". The Guardian, 31 Luglio 2013. Ultima modifica 25 Settembre 2016. https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

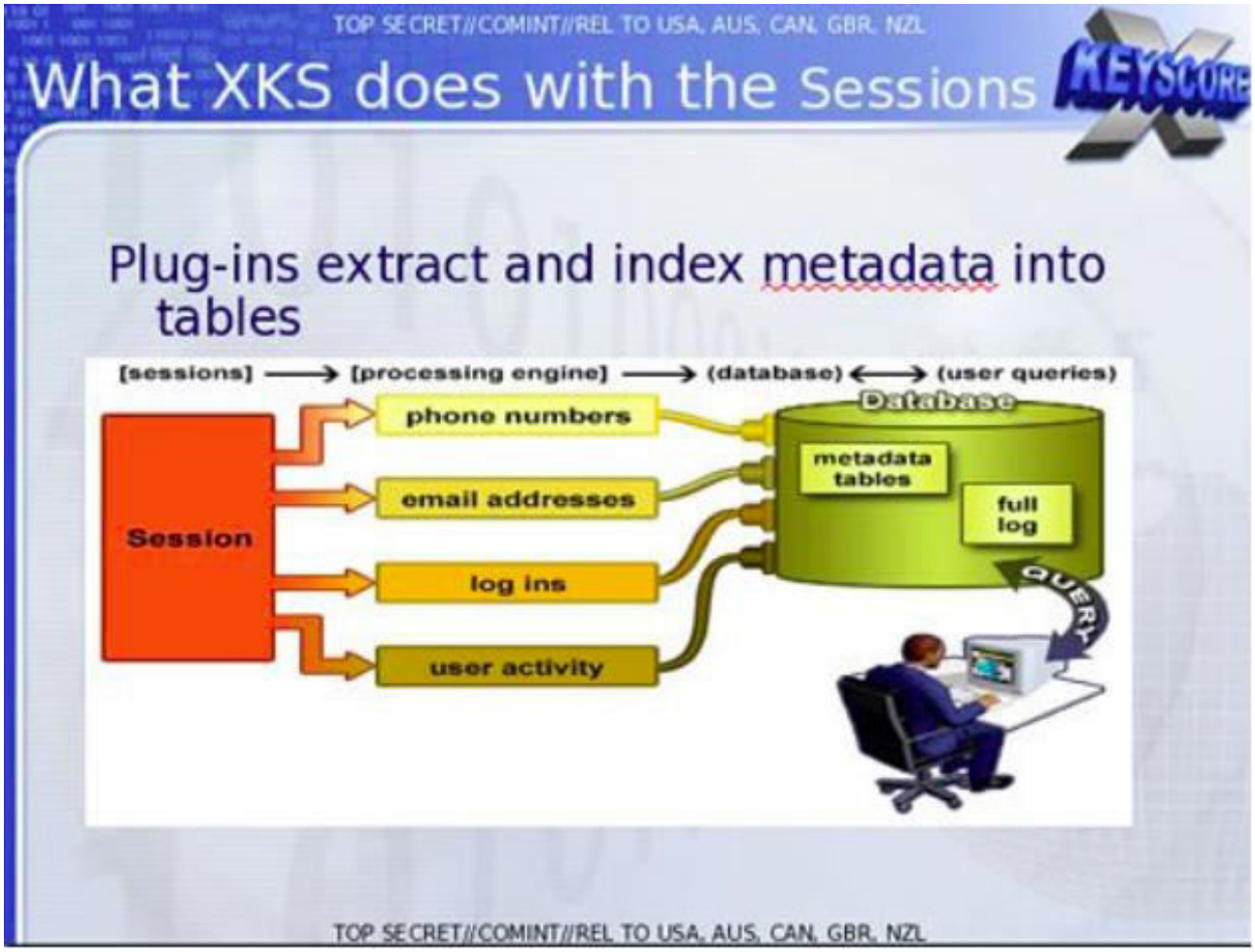


Figura 4 Fonte: The Guardian

Una battuta di arresto significativa si è avuta nel giugno 2015, con l'approvazione del Freedom Act, che limita per la prima volta lo strapotere dell'NSA. I cambiamenti più significativi riguardano i metadati, che saranno raccolti esclusivamente dalle compagnie telefoniche e rilasciati solo a fronte di un'esplicita richiesta del governo, approvata dal Tribunale di sorveglianza dell'intelligence straniera. L'agenzia aveva già sospeso la raccolta dei dati pochi giorni prima, in seguito al mancato rinnovo della sezione 215 del Patriot Act, che l'autorizzava ad immagazzinare i tabulati telefonici dei cittadini americani, anche qualora non fossero indagati, e ad ottenere dati finanziari e libri contabili delle compagnie del web[26].

[26] Repubblica, 2 Giugno 2015. "Usa, approvato il Freedom Act. Limitata l'attività della Nsa. Finisce era del Datagate". Ultima modifica 25 Settembre 2016. http://www.repubblica.it/tecnologia/sicurezza/2015/06/02/news/usa_approvato_il_freedom_act_limitata_l_attivita_della_nsa-115906794/

La sorveglianza dopo Snowden

A distanza di circa due anni dallo scandalo Datagate, gli americani sembrano nutrire sentimenti contrastanti per quanto riguarda la tutela della privacy. Infatti, nonostante la maggioranza di essi sia contraria all'idea che il governo li sorvegli, solo una ridotta percentuale ha preso precauzioni per proteggere i propri dati dai programmi dell'NSA.

Lo riferisce un recente sondaggio condotto dal Pew Research Center sulle strategie per la tutela della privacy dopo il caso Datagate. Poco più della metà dei 475 intervistati ha dichiarato di essere molto o piuttosto allarmata dalla sorveglianza esercitata sui dati e le comunicazioni digitali degli americani, mentre il 46% si è detto non molto o per nulla preoccupato.

Tra i soggetti rientranti nella prima categoria, meno della metà ha dichiarato di aver cambiato le proprie abitudini nel modo di comunicare online e telefonicamente. Poco più di un terzo degli intervistati a conoscenza dei programmi di sorveglianza ha detto di aver preso almeno qualche precauzione per proteggere i propri dati dal governo, come cambiare le impostazioni della privacy o disinstallare un'app. La percentuale scende al 25% per quanto riguarda cambiamenti nell'uso del proprio account email, motore di ricerca e cellulare.

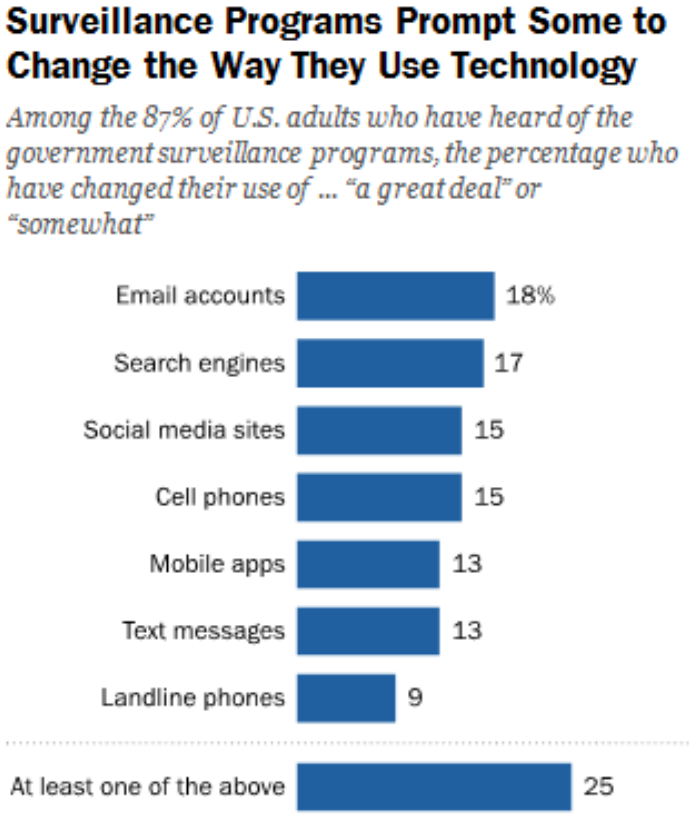


Figura 5 Fonte: Pew Research Center

I motivi dell'inerzia dei cittadini sono molteplici. Innanzitutto, gli intervistati sembravano meno allarmati per il monitoraggio delle proprie attività online di quanto non siano per il programma nel suo insieme. Mentre il 57% delle persone a conoscenza del programma di sorveglianza dell'NSA lo ha definito "inaccettabile", poco meno del 40% si è dichiarato molto o piuttosto preoccupato dalla sorveglianza in prima persona. Uno degli intervistati ha infatti dichiarato che non stesse facendo nulla di male e che avrebbero quindi potuto monitorarlo a loro piacimento.

Si tratta anche di una questione di conoscenza. Infatti, la maggioranza delle persone crede che sia molto o piuttosto difficile trovare strumenti che possano proteggere efficacemente la loro privacy online e al telefono. Per quanto riguarda strumenti più specifici, come programmi di cifratura delle

email e plug-in che incrementino la sicurezza del proprio browser, tra il 70% e l'80% degli intervistati non ha adottato o non era al corrente di queste soluzioni.

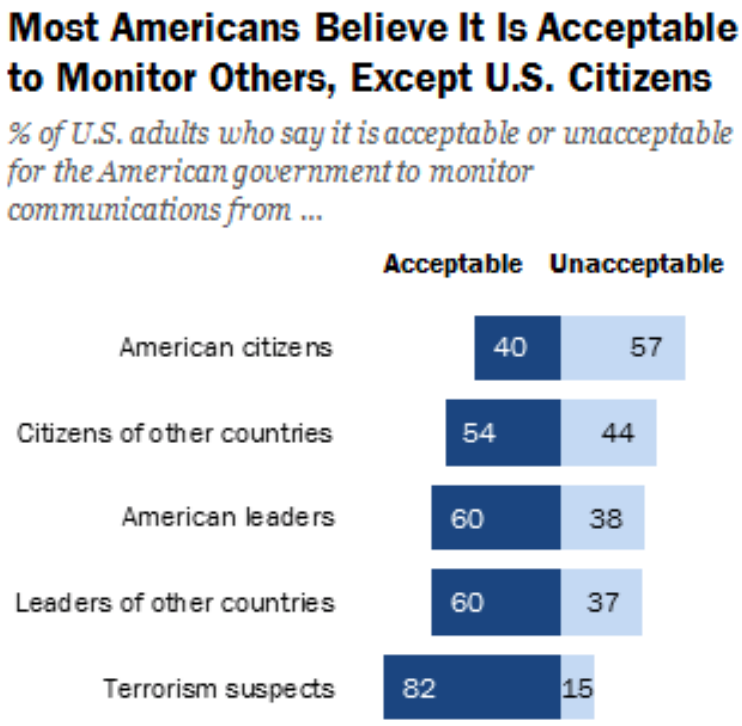


Figura 6 Fonte: Pew Research Center

Curiosamente, lo scetticismo riguardo ai programmi di sorveglianza del governo non ha colore politico. Democratici e Repubblicani hanno la stessa probabilità di cambiare le proprie abitudini online e hanno dato risposte simili riguardo ai soggetti che sarebbe accettabile sorvegliare. La maggioranza degli intervistati si è detto a favore della sorveglianza per i sospetti terroristi e il 60% del monitoraggio dei leader americani e stranieri, mentre la maggior parte delle persone ha dichiarato di essere in disaccordo con ila sorveglianza dei cittadini americani.

L'unica differenza è emersa in relazione al fatto che i programmi di sorveglianza servissero o meno l'interesse pubblico. I Repubblicani si sono dichiarati il 15% in più delle volte meno fiduciosi nell'operato del governo, forse per via dell'attuale amministrazione democratica. Infatti, nel 2013 uno studio del Pew aveva messo in evidenza come circa due terzi dei Democratici si fossero opposti ad un programma di sorveglianza simile sotto la presidenza Bush, mentre la stessa percentuale aveva supportato l'operato dell'NSA sotto Obama. Il trend opposto è stato riscontrato per i democratici.

La sentenza Safe Harbor

Con l'espressione "Safe Harbor" si fa riferimento ad un accordo che permetteva alle aziende statunitensi, come Micrsoft, Google e Facebook di trasferire i dati dei propri utenti europei oltreoceano. L'accordo attuava la direttiva Ue 95/46, entrata in vigore nell'ottobre 1998, sulla protezione dei dati personali ma è stato dichiarato invalido dalla Corte di Giustizia dell'Unione Europea nel 2015, grazie a Max Schrems.

Lo studente e attivista austriaco aveva notato come all'atto di iscrizione a Facebook fosse necessario sottoscrivere un contratto con Facebook Ireland, che permetteva il trasferimento dei propri dati nei

server situati in California. Si era dunque rivolto all'Autorità per la protezione dei dati Irlandese, sostenendo che, alla luce dello scandalo Datagate, il diritto statunitense non fosse adatto a proteggere i dati degli utenti europei.

Dopo un primo respingimento da parte dell'Autorità Irlandese, Schrems aveva portato il caso all'attenzione della Corte di Giustizia dell'Unione Europea, che accolse le sue istanze. Conseguentemente, l'accordo potrà essere sospeso a discrezione dei singoli stati membri, nel caso in cui non sia garantito un "livello adeguato" di protezione delle informazioni.

"Questa decisione è un colpo alla sorveglianza di massa operata dagli Stati Uniti che si poggia principalmente su partner privati", ha dichiarato in un comunicato stampa Max Schrems. Quest'ultimo ha ricevuto il sostegno, seppur virtuale, dello stesso Snowden, che ha twittato "Complimenti, @MxScrems. Hai cambiato il mondo in meglio".

Conclusione

Questa tesi ha avuto come obbiettivo quello di fare una paronimica delle emergenti minacce informatiche, provando a sfatare il mito del cyber terrorismo e riconoscendo la presenza di ulteriori rischi cibernetici con cui lo stato deve fare i conti. L'importanza di tutto ciò deriva dal fatto che gli individui, vivendo in una società dell'informazione come la nostra, spendono una considerevole quantità della loro vita nel cyber-sfera, portando le interazioni on-line e la vita nel mondo fisico ad intrecciarsi sempre di più.

Dal punto di vista teorico, a fronteggiarsi sono due gruppi: chi sostiene che il cyber terrorismo sia una minaccia imminente e chi invece lo considera un nulla di fatto, data la scarsità di attacchi che possano propriamente definirsi tali. Data la coesistenza di queste due concezioni opposte, è persino difficile pervenire ad una definizione condivisa sul piano internazionale. La complessità del dibattito è acuita anche dalla necessità di bilanciare sicurezza e libertà individuali.

Questi due elementi sembrano infatti essere antitetici, perché un maggiore godimento della prima comporta una minor fruizione dei secondi. Appare, quindi, necessario ricercare un criterio che permetta un giusto equilibro tra i due. Va comunque sottolineato che le misure di sicurezza informatica contribuiscono al benessere individuale, in quanto sono il mezzo attraverso il quale le autorità pubbliche rispondono all'esigenza di creare un ambiente sicuro per i propri cittadini. In tal modo, esse corrono tuttavia il rischio di violarne i diritti individuali ma ciò è giustificabile solo quando si tratti di una violazione minima e momentanea.

Infatti, i diritti di cui usufruiamo nel cyber spazio dovrebbero godere di pari dignità rispetto a quelli che esercitiamo nel mondo fisico. Ne consegue che essi non possono essere invasi in misura indefinita e senza una chiara giustificazione, ogni volta che la sicurezza sia presumibilmente a rischio, come è accaduto con lo scandalo PRISM. Infatti, il diritto alla sicurezza ha lo scopo di proteggere la capacità degli individuali di raggiungere il proprio benessere.

Riassunto in inglese

The term cyber terrorism was invented in the 80s by Barry Collins, in order to explain the use of cyber-space for terrorist purposes. At first, this concept included activities such as campaigning and espionage but, after the Estonian DoS (Denial of Service) attacks of 2007, it became more focused on the concrete implications of the phenomenon. A shared definition could be the one by Akhgar, Staniforth and Bosco:

> The use, making preparations for, or threat of action designed to cause a social order change, to create a climate of fear or intimidation amongst (part of) the general public, or to influence political decision-making by the government or an international governmental organisation; made for the purposes of advancing a political, religious, racial or ideological cause; by affecting the integrity, confidentiality, and/or availability of information, information systems and networks, or by unauthorised actions affecting information and communication technology based control of real-world physical processes.

First of all, it is important to stress out that cyber terrorism takes place in cyber space, i.e. "the notional environment in which communication over computer networks occurs", as defined by the Oxford Dictionary. Even though we often imagine it as a virtual space, the latter cannot exist without several physical infrastructures. They range from portable devices, such as mobile phones or computers, to servers, data centres, Network Operations Centres and, above all, fiber-optic cables. The most important hub is the Mediterranean one, that allows the connection between Europe, North Africa, Middle East and India.

Secondly, this phenomenon may arise in various ways, as described by Collins in his book "The Future of the Cyber Terrorism": from attacking the air traffic control systems, leading to the collision of civilian aircrafts, to accessing the control systems of a cereal manufacturer, changing the levels of iron supplement and causing disease and death.

However, the existence of documented episodes of cyber terrorism is in doubt. An important case described by Collins is the aforementioned cyber attack that hit Estonia in 2007. It was the largest DDos (Distributed Denial of Service) Attack the world had ever seen, causing the shutdown of 58 websites all at once. However, the incident cannot be properly classified as cyber terrorism, since its purpose was to protest against the government decision to move the Russian memorial of unknown soldier to the outskirt of the capital.

Nonetheless, the Internet is increasingly used by terrorist organization in order to rise funds, campaign and recruit fighters. These activities often take place in the most remote and obscure areas of the cyber-sphere, Deep and Dark Web. The former includes the so called "hidden sites", that cannot be found through common

search engines if you do not know the url. The latter can only be accessed through specific softwares such as TOR (The OnionRouter) and I2P, whose purpose is to hide the user's IP address. The main benefits are the anonymity, cost-effectiveness and omnipresence of communications, that allow terrorists to colonize the cyber-space.

The Islamic State, in particular, has demonstrated remarkable skill in using the Internet for propaganda purposes. At first, jihadists were primarily using password- protected forums in the Deep Web but, recently, the latter have been replaced by open-source and peer-to-peer social media. In particular, as reported by The Guardian, ISIS takes advantage of the most popular hashtags in order to disseminate its contents as widely as possible on Twitter and YouTube.

According to a report presented by the Quillam Foundation ISIS releases about 38 batches of propaganda per day (including pictures, videos, articles and audio programmes). In spite of the image portrayed by western media, violence is not the only subject of its contents. The main themes are mercy, belonging, brutality, victimhood, military and utopia, even though the last three are prevalent. More than half of the material focusses on the everyday lives of civilians in the areas occupied by the caliphate, describing economic activities, social and religious events. In this way, the Islamic States "attracts supporters based on ideological and political appeal". On the other hand, a recurring theme is war, so that attacks are often faked in order to convey the idea that the Islamic State is constantly on the offensive.

The same themes appear in the ISIS online publication, Dabiq, named after a Syrian city linked to the myth of apocalypse. The journal aims to recruit fighters and to educate young Muslims to a new way of thinking and it is written in various languages, English included, in order to gather a wide audience.

According to the 2015 report of the Homeland Security Committee, thanks to its pervasive propaganda and expert use of social media, ISIS attracted more than 25.000 foreign fighters, of which 250 American citizens. As a result, the U.S. government created a task force that is part of the National Security Department and will involve all the major Silicon Valley companies, such as Apple, Facebook and Twitter.

Regarding the European Union, the Europol established an Internet Referral Unit in 2015, that will work jointly with the police force of all the member states. As stated by Dimitris Avramopoulos, the European Commissioner for Migration, Home Affairs and Citizenship:

> The recent terrorist attacks in France, Tunisia and Kuwait have shown once again how important it is to combat terrorist threats with determination. The establishment of the EU Internet Referral Unit is one of the first deliverables of the European Agenda on Security. It will provide operational support to

> Member States on how to tackle more effectively the challenges of detecting and removing the increasing volume of terrorist material on the internet and in social media. The launch of this important initiative is the result of our common efforts. The success of this initiative will depend on the continued good cooperation and contributions from all stakeholders.

The spreading of jihadist contents on the Internet has been hindered also by various groups of hackers, such as Anonymous. The latter started a campaign called #opIceIsis, in order to underline the U.S. government's rensponsabilities in the rise of ISIS and to stress the difference between the Islamic religion and jihadist extremism.

However, cyber terrorism is not the only threat that the state must counter in the cyber-sphere. In fact, the Internet is an important tool also for the so called "hacktivists". Hacktivism is defined by Prof. Dorothy Dennings as "the marriage of hacking and activism and it consists of electronic sit-ins, email floods, viruses, worms and website spoofing.

The origin of this phenomenon dates back to 1999, when a group called Electronic Disturbance Theatre (EDT) organized virtual sit-ins to protest against the Mexican president Zedillo, the White House, the Pentagon and other institutions, that were hit by DoS attacks. However, not all hacktivist groups use non-violent methods in order to advance their cause. Some websites, for example, incite to violence towards non-objector gynaecologists, sharing their personal data on the Internet.

It is important to underline that the web can be a powerful weapon for states themselves, through which they can steal information and threaten their enemies. According to the Market info Group LLC, in 2024 the market of cyber weapons will exceed EUR 3 billion. The most developed countries in this sector are United States, China, Russia, North Korea, South Korea and Iran, often as a result of their large amount of Internet users.

Cyber weapons offer a number of advantages: they are less expensive, precise, effective, anonymous and tailored to the target. However, they can be defined as "one-shot", since they cannot be used more than once in order to avoid loosing the element of surprise. A good example is Stuxnet, a virus allegedly created by the Bush administration in agreement with Israel in order to sabotage Iran's nuclear program. It was introduced to the Natanz nuclear power station via a USB flash drive and targeted its the remote control system, causing the centrifuges to destroy themselves.

Another important phenomenon is cyber espionage, i.e. "the stealing of secrets stored in digital formats or on computers and IT networks". It generally involves highly trained government agents and hackers, that act on their own initiative or for a greater cause. Most of the time, the instigators of the attacks remain anonymous.

A case in point is “Titan Rain”, a series of attacks that affected the American military and government systems in 2003, lasting for five years. Even though the attacks came from Chinese computers, it is unclear if the National Security Agencies in Beijing were effectively behind the operation. The Pentagon estimated that between ten and twenty terabytes of data were stolen from the Department of State networks.

However, the increasing state intervention into the cyber-space can lead to a conflict between individual rights and public authority, exacerbated by the nature of the cyber-sphere itself. In fact, the data of which it is composed are malleable: they can be processed, stored, modified and, more importantly, they can reveal personal information, facilitating control and surveillance measures. On the other hand, the latter are necessary in order to protect the cyber-space, that is now an irreplaceable part of contemporary societies, from possible threats.

The NSA (National Security Agency) scandal of 2013 brought to light the violations of the right to privacy and anonymity committed by the American government and the necessity to strike a balance between cyber-security and individual rights in the cyber-sphere. Thanks to the efforts of Edward Snowden, computer specialist and employee of the consulting firm Booz Allen Hamilton, the existence of programmes such as PRISM and XKeyscore got into the public eye.

The former allowed the U.S. government to store digital communications from the major internet companies, such as Facebook, Skype, Microsoft, Apple and Yahoo. The latter, on the other hand, enabled the NSA analysts to even visualize the internet activity of a given subject in real-time. "I, sitting at my desk," claimed Snowden, could "wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email".

The scandal, however, has had a significant impact on the American legal system, since the power of the aforementioned agency has been severely limited by the approval of the Freedom Act on June 2015. From now on, the metadata will be collected exclusively by telephone companies and released only after an explicit request of the government.

Unfortunately, that cannot be said of American citizens. In fact, according to a survey conducted by the Pew Research Centre, even though the majority of people is worried about the government surveillance programs, just a small fraction of them took precautions in order to protect their privacy. The reason behind this conflicting behaviour is primarily the fact that U.S. citizens seem to be more concerned about the programs themselves than about the hypothesis of being monitored first-hand. Moreover, they are often poorly informed about the tools invented for the purpose of protecting privacy.

The consequences of the Datagate scandal have been felt also in Europe, where the so called Safe Harbour Privacy Principles, that allowed the transfer of the European users’ data to other countries,

have been declared invalid by the Court of Justice of the European Union. This important change has been made possible by the Austrian student and activist Max Schrems.

The latter denounced the violation of the EU privacy laws committed by Facebook, because of its involvement in the PRISM program, getting the support of Snowden himself, that tweeted: “Congratulations, @MaxSchrems. You've changed the world for the better”. From now on, the agreement could be suspended at the discretion of each member state, if they are not provided with an appropriate level of privacy.

This case is the ultimate proof that, even though cyber security contributes to the wellbeing and safety of citizens, its impact on individual rights is justifiable only when it is minimal and temporary. In fact, the rights we enjoy in the cyber-sphere should be accorded the same dignity as the one we have in the physical world. Thus, they cannot be violated at will and without a clear justification, every time that national security is at risk, as for the NSA scandal.

Bibliografia

Akhgar, Staniforth e Bosco. Cyber Crime and Cyber Terrorism Investigator's Handbook (Waltham: Syngress, 2014)

Al Hayat Media Center. https://alhayatmedia.wordpress.com/ Ultima mofifica 15 Agosto 2016.

Borges, Anelise. "Anonymous 'declare cyber war' on IS militants". France24, 23 Settembre 2014. Ultima modifica 5 Settembre 2016. http://www.france24.com/en/20140920-tech24-Anonymous-VS-ISIS-online-war-against-terrorism/

Carl Van Clausewitz. On War (Berlin: Ullstein 1832, 1980)

Cohen, Jared. "Waging a Digital Counterinsurgency". Foreign Affairs, November/December 2015 Issue. Ultima modifica 18 Giugno 2016. https://www.foreignaffairs.com/articles/middle-east/digital-counterinsurgency

Collins, Barry L. "The Future of the CyberTerrorism: Where the Physical and Virtual Words Converge". Istitute for Security and Intelligence, 1997. Ultima modifica 20 Agosto 2016. http://www.crime-research.org/library/Cyberter.htm

Europol. "Internet ReferralUnit Combat Terrorist and ViolentExtremist Propaganda". Ultima modifica 26 Agosto 2016. https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda

Frediani, Carola. "Ecco l'internet dei cavi sottomarini. Tra geopolitica e velocità della rete". L'Espresso, 29 Agosto 2014. Ultima modifica 2 Agosto 2016. http://espresso.repubblica.it/visioni/tecnologia/2014/08/29/news/ecco-l-internet-dei-cavi-sottomarini-tra-geopolitica-e-velocita-della-rete-1.178225

Frizzell, Sam, "Experts Doubt ISIS Could Launch Major Cyberattack Against the U.S.". Time, 19 Settembre 2012. Ultima modifica 12 Settembre 2016. http://time.com/3403769/isis-cyberattack/

Gibbs, Samuel. "Anonymous swaps Isis propaganda site for Prozac ad in trolling fight". The Guardian, 26 Novembre 2015. Ultima modifica 27 Luglio 2016. https://www.theguardian.com/technology/2015/nov/26/anonymous-swaps-isis-propaganda-site-for-prozac-ad-in-trolling-fight

Gov.uk. "Radicalization". Ultima modifica 1 Settembre 2016. https://www.gov.uk/government/publications/online-radicalisation/online-radicalisation#question-time-live-with-detective-chief-superintendent-sue-southern-from-west-midlands-police

Greenwald, Glenn. "XKeyscore: NSA tool collects 'nearly everything a user does on the internet". The Guardian, 31 Luglio 2013. Ultima modifica 25 Settembre 2016. https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

https://www.theguardian.com/world/2014/sep/24/isis-twitter-youtube-message-social-media-jihadi

Il Post, 8 Giugno 2013. “La risposta di Zuckerberg sul caso PRISM”. Ultima modifica 25 Settembre 2016. http://www.ilpost.it/2013/06/08/la-risposta-di-zuckerberg-sul-caso-prism/

Lütticke, Markus. “A chronology of the NSA surveillance scandal”. Deutsche Welle, 31 Ottobre 2013. Ultima modifica 25 Settembre 2016. http://www.dw.com/en/a-chronology-of-the-nsa-surveillance-scandal/a-17197740

Malik, Laville, Cresci e Gani. “Isis in duel with Twitter and YouTube to spread extremist propaganda”. The Guardian, 24 Settembre 2014. Ultima modifica 22 Agosto 2016.

Miller e De Young. “Obama administration plans shake-up in propaganda war against ISIS”. The Washington Post, 8 Gennaio 2016. Ultima modifica 29 Agosto 2016. https://www.washingtonpost.com/world/national-security/obama-administration-plans-shake-up-in-propaganda-war-against-the-islamic-state/2016/01/08/d482255c-b585-11e5-a842-0feb51d1d124_story.html

National Research Council. Computers at Risk: Safe Computing in the Information Age (Washington: National Academy Press, 1991)

Orsini, Alessandro. “ISIS: I terroristi più fortunati del mondo e tutto ciò che è stato fatto per favorirli”. (Milano: Rizzoli, 2016)

Oxford Dictionaries. “Cyberspace”. Ultima modifica 8 Agosto 2016. http://www.oxforddictionaries.com/it/definizione/inglese/cyberspace

Repubblica, 2 Giugno 2015. “Usa, approvato il Freedom Act. Limitata l'attività della Nsa. Finisce era del Datagate”. Ultima modifica 25 Settembre 2016. http://www.repubblica.it/tecnologia/sicurezza/2015/06/02/news/usa_approvato_il_freedom_act_limitata_l_attivita_della_nsa-115906794/

Richtel e Brinkley. “Spread of Attacks on Web Sites Is Slowing Traffic on the Internet”. Th New York Times, 10 Febbraio 2000. Ultima modifica 21 Settembre 2016. “Spread of Attacks on Web Sites Is Slowing Traffic on the Internet”.

The White House. “Remarks by the President in a Press Conference”. Ultima modifica 25 Settembre 2016. https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference

Wall Street Journal, 20 Giugno 2014. “New ISIS recruitment Video Aimed At Western Muslims” Ultima modifica 20 Agosto 2016. http://www.wsj.com/video/new-isis-recruitment-video-aimed-at-western-muslims/749B2C6E-A554-4522-A1A4-CF5CAAADD984.html