Danilo Ceccarelli Morolli

APPUNTI DI GEOPOLITICA

Valore Italiano™

APPUNTI DI GEOPOLITICA

Danilo Ceccarelli Morolli

Valore Italiano™

Danilo Ceccarelli Morolli

APPUNTI DI GEOPOLITICA

Collana Culture & Progresso | Geopolitica

Codice ISBN 978-88-97789-60-4

©2018-2019 Valore Italiano™ - Tutti i diritti riservati

WWW.VALOREITALIANOBOOKSTORE.COM
Facebook.com/valoreitalianoeditore

Riproduzione vietata ai sensi di legge (art.171 della legge 22 aprile 1941, n. 633)

Indice

Abbreviazioni 7

Prefazione di G. Lertora 9

Premessa 13

Ringraziamenti 15

Capitolo Primo. Che cosa è la geopolitica 17

§1. La geopolitica tra storia e definizioni possibili 17

§2. Geopolitica e cartografia: un binomio imprescindibile 28

§3. Cenni di metodologia della geopolitica 32

Capitolo Secondo. Geopolitica o geopolitiche? 41

§1. Nota introduttiva 41

§2. Geopolitica dell'*Intelligence* 41

§2.1. *Cyber-War* e *Cyber Security* 52

§2.2. *Info-War* e geopolitica delle comunicazioni 56

§2.3. *Il Deep Web,* ovvero le incognite di internet 61

§2.4. Geopolitica della sicurezza 64

§3. Geostrategia 69

§3.1. Guerra psicologica 74

§3.2. Alcuni "effetti" delle guerre 75

§4. Geoeconomia e Geofinanza 78

§4.1. Geopolitica del capitalismo 85

§4.2. Le cripto-valute: chimere o realtà? 89

§4.3. I *Big-Data,* ovvero l'oro del XXI secolo 91
§4.4. L'*Intelligence* economica: una nuova frontiera 94
§4.5. Industria 4.0: una rivoluzione in corso 98
§4.6. Geopolitica del lavoro 102
§5. Geopolitica delle risorse ambientali ed energetiche..... 108
§5.1. Risorse energetiche 108
§5.2. Risorse idriche e alimentari 118
§5.3. Lo sviluppo sostenibile: una sfida globale..... 125
§6. Geopolitica del mare 131
§7. Geopolitica dei fenomeni migratori 137
§8. Geopolitica dell'*Outer Space* 145
§9. Geopolitica del diritto 149
§10. Geopolitica della democrazia 155
§11. Geopolitica dell'istruzione, ovvero dell'università 164
§12. Geopolitica dello sport 170
§13. Geopolitica delle religioni 172
§14. Geopolitica della Chiesa cattolica: cenni 177
§14.1. Cenni sulla diplomazia pontificia 184
§14.2. Cenni sulla geopolitica delle Chiese orientali (cattoliche) 188
§14.3. "*Cyber-Theology*": una nuova frontiera 197
§15. La diplomazia parallela 199
§16. Geopolitica e psicologia, ovvero: geopsicologia 203

Capitolo Terzo. Geopolitica "liquida" 209
§1. Nota introduttiva 209
§2. L'Europa: una "espressione geografica"? 210
§3. Gli U.S.A: declino di un "impero"? 217
§4. L'Oriente Slavo: *Renaissance* della Russia? 224

§5. Il Vicino Oriente: figli di Sykes e Picot? 237
§6. La Cina e l'India: solo economia? 260
§7. L'Artico: una nuova "Guerra Fredda" tra i ghiacci? 274
§8. "Nuovo Ordine Mondiale"? 277

Conclusioni 285
Postfazione di R. Chiarelli 287
Alcuni vocaboli della geopolitica 291
Alcuni riferimenti bibliografici 297

ABBREVIAZIONI

AE	*Atlante dell'energia*, Novara 2015.
AG	ISTITUTO DELL'ENCICLOPEDIA ITALIANA "TRECCANI", *Atlante Geopolitico*, Roma 2017.
DG	O'LOUGHLIN J. (a cura di), *Dizionario di geopolitica*, Trieste 2000.
DSG	CORDELLIER S. (a cura di), *Dizionario di storia e geopolitica del XX secolo*, Milano 2001.
EDEC	FARRUGIA E. G. (ed.), *Encyclopedic Dictionary of the Christian East*, Rome 2015.
Gnosis	*Rivista Italiana di Intelligence* – http://gnosis.aisi.gov.it
Limes	*Limes – Rivista Italiana di Geopolitica*
JEAN	JEAN C., *Geopolitica del mondo contemporaneo*, Roma-Bari 2012.
KISSINGER	KISSINGER H., *Ordine mondiale*, Milano 2015.
LS	FRANCESCO, Enciclica *Laudato sì* del 24 maggio 2015.
MARSHALL	MARSHALL T., *Le 10 mappe che spiegano il mondo*, Milano 2017.
MARIZZA	MARIZZA G. (a cura di), *Come orientarsi fra geopolitica, strategia e dintorni*, «Mappamondi» 8, Roma 2013.
Oriente Cattolico	CONGREGAZIONE PER LE CHIESE ORIENTALI – RIGOTTI G. (a cura di), *Oriente Cattolico*, 3 tomi, Roma 2017.
Scritti in onore Lizza	MARCONI M. – SELLARI P. (a cura di), *Verso un nuovo paradigma geopolitico. Raccolta di scritti in onore di Gianfranco Lizza*, 2 tomi, Roma 2015.

§2.1. Cyber War e Cyber Security

Dal momento che l'"informazione è potere", si è sviluppata la così detta *Cyber War*[38]. Questa nuova frontiera di conflitto è caratterizzata dall'uso di tecnologie (elettroniche, informatiche, telecomunicazioni) e rappresenta attualmente una delle punte più avanzate della guerra contemporanea. Non vi sono più eserciti o flotte contrapposte, bensì il controllo del cyber-spazio. In sostanza gli Stati si contrappongono nello spazio, etereo, dell'informatica. Ne consegue che non vi sia più un preciso "tempo" per la guerra, poiché un attacco informatico può avvenire in qualunque momento. Le finalità di un *Cyber Attack* possono essere molteplici e tutto sommato sono di non facile elencazione: dal reperimento di dati sensibili riguardo la strategia militare o l'economia oppure la paralisi delle strutture informatiche oppure ancora il lancio di notizie fuorvianti. La tattica di base è quella della saturazione delle reti dell'avversario (*Denial of Service*), ma si può anche interferire per esempio nelle elezioni, allorquando sia presente una modalità di voto elettronico, oppure ancora il blocco e quindi il collasso di un sistema finanziario. L'effetto di un *Cyber Attack* è quello di indebolire le strutture informatiche e la rete di uno Stato, con conseguente generazione del caos sociale. Oggi ai computer è demandata la gestione di una serie di molteplici attività civili: dalle transazioni economiche alla rete di trasporti, dagli impianti energetici a quelli delle comunicazioni[39]. Ogni Stato possiede tale complessa rete informatica che qualora attaccata ne soffrirebbe di danni incalcolabili; se azzerata farebbe sprofondare quella determinata nazione, nel giro di poche ora, nell'età della pietra.

Un attacco informatico può articolarsi in diverse modalità. Si va dal reperimento di dati sensibili a fini di spionaggio, per esempio entrare in una banca dati di un ente statale (come potrebbe essere il ministero della difesa) oppure un attacco, più devastante, come quello a infrastrutture dette

---

[38] Sul tema, tra i molti, cfr. JEAN C. – SAVONA P., *Intelligence economica. Il ciclo dell'informazione nell'era della globalizzazione*, Soveria Mannelli, Catanzaro, 2011, pp. 63-74.

[39] La questione poi si complica se si pensa alla "domotica", ossia al fatto che oggi le abitazioni domestiche posseggono quasi tutte – almeno nel mondo occidentale – una connessione internet. Questo amplifica a dismisura le possibilità di obiettivi di un attacco informatico, in quanto i privati possono essere target scarsamente protetti. Alcuni attacchi informatici sfruttano infatti i "nodi" delle reti private per interrogare un *Host* e creare il *Tango Down* (cioè mandarlo giù).

"critiche" come ad esempio i servizi dei trasporti o delle comunicazioni o quelli energetici. Oppure vi è la possibilità di *Equipment Disruption*, cioè attaccare i computer e i satelliti militari al fine di spezzare la linea di comando degli ordini. Come si comprende il panorama è complesso e questo è il regno indiscusso degli hacker[40] che vengono ingaggiati dagli stessi Stati. Ad esempio il programma nucleare iraniano sarebbe stato messo fuori uso per diverso tempo proprio grazie ad un virus informatico realizzato da tecnici israeliani[41].

Ulteriore caratteristica degli attacchi cibernetici o elettronici è che questi possono essere posti in essere in qualunque parte del globo e da chiunque abbia le competenze informatiche necessarie. Quindi non sempre sono gli Stati che procedono ad attaccare un sistema-paese avversario, ma possono essere anche dei singoli hacker. Uno degli effetti, ancora poco valutati, di un *Cyber-Attack* può essere anche a scopo "dimostrativo", cioè quello di screditare la sicurezza di una nazione e quindi della sua classe dirigente agli occhi dei cittadini.

Come si può comprendere gli scenari degli effetti di una *Cyber War* sono inquietanti. Per questo gli Stati cercano costantemente – tramite anche i servizi di *Intelligence* informatica – di impedire tali attacchi, creando schermature e meccanismi di difesa e controllo di tutto ciò che è "sensibile" ovvero "critico", al fine di non avere danni. Dalle notizie ufficiali sappiamo che alcuni tentativi di attacco informatico sono stati posti in essere per esempio contro gli USA (nel 2017), in Georgia (2008), in Estonia (nel 2007). Il problema si complica se si pensa che non solo oggi alcuni Stati sono in grado di sferrare attacchi informatici, ma anche gruppi – isolati o aggregati – di hacker i quali compiono tali imprese per motivi ideologici propri, come ad esempio *Anonymous*[42].

---

[40] Per la cronaca esistono ormai dei veri e propri manuali di *Hacking*; tra i molti cfr. MITNICK K. D. – SIMON W. L., *L'arte dell'Hacking*, Milano 2014.

[41] Secondo quanto sostengono W. J. BROAD, J. MARKOFF e D. E. SANGER, cfr.: www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1

[42] *Anonymous* esprime una vera e propria filosofia di alcuni hacker ed è espressione di proteste mirate ma non coordinate. Si parla in questo caso di *Hacktivism* ovvero di azioni di esperti informatici che utilizzano in modo creativo reti e computer al fine di criticare l'operato di alcuni governi o multinazionali. *Anonymous* organizza così petizioni online, virus benevoli, siti web di controinformazione al fine di "liberalizzare" la comunicazione dei cittadini e con essa diffondere la "verità". Sul tema, tra i molti, cfr. COLEMAN C. – PARRELLA B. – PALAZZOLO M., *I mille volti di Anonymous. La vera storia del gruppo hacker più provocatorio al mondo*, 2016; OLSON P., *We Are Anonymous*, New York 2013.

Sul piano, non solo concettuale, ma "tattico", un *Cyber-Attack* comporta una deterritorializzazione della guerra; ciò a sua volta implica degli enormi problemi per il diritto internazionale, che ancora non è giunto a maturazione riguardo tale spinoso problema, ossia non ha individuato una piattaforma di regole. In questa guerra silenziosa di informazioni e tecnologia, i servizi di *Intelligence* occupano un primo piano di rilievo. I loro successi non sono noti in genere, ma i loro insuccessi sono invece conosciuti, perché accadono quando qualcosa va storto. Ciò dimostra quanto dicevo prima, ossia che l'*Intelligence* è indispensabile ma non onnipotente.

Una tematica intimamente connessa al problema del *Cyber War* è rappresentato dalla *Cyber Security*, ovvero la sicurezza delle reti presenti in una nazione. Anche questa è una nuova frontiera, non solo del sapere, ma anche dell'azione, in cui elementi civili e militari si fondono. Infatti la *Cyber Security* è l'altra faccia della *Cyber War.* La rete è non solo spazio di scambio di informazioni ma anche mezzo o porta per poter entrare nei sistemi "critici" di una nazione. Da qui la necessità di schermare il sistema informatico da un lato, e dall'altro quanto più velocemente sia possibile intercettare, ovvero comprendere, che si sia sotto *Cyber Attack*. Se la *Cyber War* è un'azione militare, ossia gestita da ambienti militari, un attacco informatico per esempio ad una grande azienda può esserlo anche da parte di hacker civili che operano a danno di quest'ultima.

Al di là delle varie tipologie di hacker e della "filosofia" dell'hacheraggio, in alcuni casi si è di fronte a veri e propri crimini, che rientrano oggi nella categoria dei *Cyber Crimes*, i cui autori o mandanti sono spesso di difficile individuazione. La *Cyber Security* diventa un settore strategico che fa la differenza per un "sistema" Stato. Le forme di attacco sono molteplici: si va dall'introduzione di un maleware ad una vera e propria manipolazione di apparati. Che il risultato sia l'estrazione di dati utili oppure il blocco di un apparato gestito elettronicamente, l'effetto prodotto sarà sempre un danno, spesso anche di difficile quantificazione economica. Qui entra in gioco la geopolitica e con essa la geostrategia (cfr. *infra*). Tali azioni accadono nei computer presenti in un determinato territorio che è nello Stato ma il danno, anche quando sia solo "aziendale", ha una ricaduta su tutta la comunità che quello Stato incarna e rappresenta. Un esempio di storia contemporanea ci aiuta. La centrale elettrica di Hadera (Israele) fornisce energia a gran parte di Israele (Palestina inclusa); questa centrale subisce, per vari motivi, numerosi attacchi informatici. Israele ha così pensato di creare una struttura di propri hacker (ne ha scelti mille da tutto il mondo) per

proteggersi. Come? La struttura detta "Hyver" ("alveare")[43] riceve dal "cliente" il mandato a testare i propri sistemi di sicurezza informatica. Gli hacker dell'"Hyver" si mettono all'opera e vince – cioè è retribuito – chi riesce e penetrare nel sistema del cliente, il quale a sua volta potrà così comprendere quali siano le falle nel proprio sistema. L'esperimento "Alveare" – che è ormai una realtà consolidata in Israele – ha consentito di potenziare la *Cyber Security* del piccolo ma agguerrito Stato d'Israele, che si mostra essere all'avanguardia anche sul settore della sicurezza informatica.

Sulla scia di Israele, diversi Stati si sono posti il problema tra cui l'Italia, che ha affrontato la cosa istituendo presso il Ministero della Difesa il *Comando Interforze Operazioni Cibernetiche* (in sigla CIOC) che monitorizza la rete evidenziando gli attacchi informatici e neutralizzandoli.

Come si comprende informatica e geopolitica sono ormai legate insieme, grazie a internet e all'elettronica. La Repubblica Estone è attualmente considerata come uno dei paesi più informatizzati d'Europa. A Tallin è stato sviluppato addirittura un sistema ancora sicuro di voto elettronico. Le implicazioni di tale sistema – che si fonda su crittografia incrociata nella quale le password vengono distrutte un mese dopo le elezioni – rappresenta un modello di come si possa realizzare parte della *E-Democracy*.

Le tematiche inerenti la *Cyber Security* investono gli Stati, generando una geopolitica in cui si delinea la necessità di una maggiore comunicazione e condivisione di dati e di problemi tra gli stessi. Qualunque cosa sia connessa è infatti possibile oggetto di hackeraggio, con le conseguenze che ben si possono immaginare. Un esempio: i moderni aeroplani civili sono strutture ingegneristiche altamente complesse e integrate in un sistema elettronico e informatico, altrettanto sofisticato. Se un terrorista fosse in grado di inserirsi nel computer di un *Boeing* o di un *Airbus* il risultato sarebbe devastante e l'autore dell'attacco sarebbe di difficile individuazione. Come si osserva dall'esempio, la *Cyber Security* crea una sfumatura veramente sottilissima per non dire inesistente tra ambito civile e quello militare. Ciò induce anche a ripensare alla geopolitica di internet. Va detto che oscurare completamente la rete è impossibile. Alcuni Stati (ad esempio la Cina o l'Iran) intervengono pesantemente in essa all'interno dei propri confini nazionali, attuando una vigilanza o meglio una

[43] http://mytech.panorama.it/sicurezza/i-commando-israeliani-della-cyber-guerra/

sorveglianza della rete e delle strutture informatiche. Chiaramente la competizione si innalza, anche da un punto di vista tecnologico, perché nonostante gli sforzi dei governi nel "bannare" siti e controllare programmi, alcuni applicativi permettono ugualmente le conversazioni; ad esempio è il caso dell'uso di *WeChat* che è largamente diffuso in Cina e che consente comunicazioni col mondo esterno. Al momento si sta studiando la possibilità di implementare il sistema di *Blockchain*, ma ancora siamo agli esordi e sulla questione mi riprometto di trattarne, seppur brevemente, nel paragrafo dedicato all'economia e alla finanza. Negli ambienti dell'*Intelligence* si parla sempre di più di *Cyber Intelligence*[44] che rappresenta certamente una sfida attuale ma anche futura di incredibile importanza.

Gli Stati avrebbero desiderio di controllare il *Cyber-Spazio*, che è diventato così una sorta di "quinto potere". Così ad esempio la Cina, nel 2005, ha creato un proprio spazio internet, includente una serie di regole proprie per i provider cinesi e una contestuale riduzione dei IEP (nodi di scambio); in buona sostanza la Repubblica Popolare Cinese controlla il *Cyber Spazio*. Dunque l'era di internet libera e senza confini sta tramontando? Difficile rispondere. Il tentativo riuscito, di una super potenza emergente come la Cina, sembrerebbe offrire una risposta parzialmente affermativa in tal senso.

§2.2. Info War e geopolitica delle comunicazioni

Connessi ai concetti sopra accennati vi è quello della *Info War*, letteralmente la "guerra delle informazioni". Se la *Cyber War* ha come oggetto l'attacco delle reti informatiche e dei sistemi informatici, l'*Info War* ha come scopo quello di cercare di orientare la pubblica opinione. Il problema della pubblica opinione e dell'impatto sulla classe dirigente è stato da sempre avvertito da tutti i poteri. I Nazisti fecero della propaganda uno strumento teso alla manipolazione sociale di cui Joseph P. GOEBBLES (1897-1945, ministro della propaganda hitleriana dal 1933 al 1945) può considerarsi come una sorta di fautore. Ai tempi del nazismo si riteneva che la massa fosse un soggetto passivo; al contrario la "scuola" italiana della tecnica sociale dell'informazione, propugnata da Francesco FATTORELLO

[44] Cfr. MORI M., *Servizi e segreti. Introduzione allo studio dell'Intelligence*, Roma 2015, pp. 239-241.

(1902-1985)[45] – poi brillantemente proseguita da Giuseppe RAGNETTI – ha chiarito come anche la pubblica opinione sia composta da soggetti opinanti[46], sfatando così la chimera della dominazione mentale della massa.

In realtà l'*Info War* è sempre esistita, poiché propaganda e informazione sono le facce della medesima medaglia e inevitabilmente interagiscono fra di loro. Lo sforzo delle informazioni pubbliche, atte non solo a informare ma, in certi casi, anche a orientare la pubblica opinione non è solo e sempre governativo, ma può essere anche indotto da soggetti esterni che riescono a propagandare notizie fuorvianti. In sostanza si verifica che alcuni elementi esterni allo Stato – gruppi di pressione oppure anche altri Stati – pongano in essere azioni di influenza della pubblica opinione al fine di cercare di orientare il ciclo decisionale della leadership. Un esempio storico, ancora attuale, ci è fornito da alcuni movimenti così detti "pacifisti". All'origine della filosofia pacifista vi è il rifiuto della violenza e della guerra. Tuttavia alcuni di questi movimenti sono stati spesso uno strumento – consapevole o inconsapevole – nelle mani del nemico. Uno dei tanti esempi storici è il così detto *Appello di Stoccolma* (del 1950) sul disarmo atomico, che fu strumentalizzato dall'URSS in chiave anti-americana; eravamo in piena "Guerra Fredda": l'*Appello* era improntato al pacifismo, ma in realtà andava in ausilio all'URSS che, come noto, non era poi così "pacifica" come super-potenza.

Oggi l'*Info War*, attingente al concetto di *Soft Power*[47], è un'arma sia nelle mani della leadership che degli oppositori. Il far circolare delle notizie fuorvianti ma apparentemente vere, il voler screditare una classe politica o un partito e così via sono aspetti che rientrano in questa grande e complessa categoria di scontro geopolitico. La storia d'Italia repubblicana rappresenta una sorta di "teatro anatomico" ovvero di esempio di come l'*Info War* sia stata attuata sia internamente che esternamente, soprattutto durante la Guerra Fredda in cui gli interessi degli USA e dell'URSS erano puntati proprio sulla penisola italiana per ovvie ragioni strategiche. Oggi gli strumenti di comunicazione sociale, da

---

[45] Cfr. http://www.treccani.it/enciclopedia/francesco-fattorello_(Dizionario-Biografico)/

[46] Cfr. RAGNETTI G. (a cura di), *Francesco Fattorello – Teoria della tecnica sociale dell'informazione*, Urbino 2005.

[47] Per *Soft Power* si intende una forma più sottile e pacifica di potere fondata sulla influenza persuasiva realizzata mediante la diplomazia, la cultura, l'ideologia e l'eventuale propaganda.

internet ai Social, rappresentano un'occasione ghiotta per chi voglia cimentarsi in tale antica materia.

Occorre dire anche che l'*Info War* contemporanea ha portato come risultato, indiretto e forse inconsapevole, quello di evidenziare il ruolo dell'informazione pubblica intesa ora anche come un fattore della produttività di una nazione. Infatti il grado di sviluppo dei servizi di pubblica informazione sono un indice dell'evoluzione tecnologica di uno Stato e quindi del benessere economico[48].

Connessi ai temi sopra accennati una menzione merita il concetto di *Proxy War*. L'espressione letteralmente significa "guerra per procura"; questa sta a indicare un conflitto tra due parti – non necessariamente Stati – che si concretizza non già mediante una contrapposizione frontale bensì mediante "spazi" intermedi oppure per mezzo di soggetti terzi. La storia offre numerosi esempi di *Proxy War*, uno tra i tanti è l'occupazione sovietica in Afghanistan (1979-1989), durante la quale USA e URSS si fronteggiarono per mezzo dei *mujahidin* afghani che erano aiutati dagli USA e dai loro alleati.

Come si può ben comprendere lo "spazio" informativo, così come quello dei mass-media e dei Social, è un territorio in cui la geopolitica interviene attivamente. Questo sia perché gli Stati hanno ovvio interesse a ciò che accade all'interno ma anche ciò che avviene all'esterno, soprattutto in quei paesi verso cui siano presenti degli interessi. Parimenti gli aspetti cartografici non sono esenti dallo spazio informativo, anzi sono spesso oggetto di ciò; pertanto, anche per tale ragione, la geopolitica rientra in questo settore che oggi è in espansione sia concettuale che applicativa[49]. In sostanza la geopolitica oggi occupa anche lo spazio comunicativo e non potrebbe essere diversamente. Chi ha il controllo di tale "territorio" ne consegue, ovviamente, un grande vantaggio, né potrebbe essere diversamente.

Il ruolo della competizione nello spazio mediatico e delle comunicazioni è certamente pertinenza della geopolitica contemporanea. Per esempio internet ai primi anni novanta del XX secolo non era diffuso in modo capillare come oggi nel mondo[50]. Attualmente l'88% del Nord America ha una connessione internet, mentre il 43% nell'America Centrale

---

[48] *Ibid.*, p. 149.
[49] BETTONI G. – TAMPONI I., *Geopolitica e comunicazione*, Milano 2012.
[50] Fonte: *AG*, p. 1098.

e il 56% nell'America del Sud. Si evidenzia una grande crescita di internet nel Sud America; mentre solo il 26% delle persone ha una connessione internet in Africa e il 19% in Asia Meridionale. In Vicino Oriente il 36% ha una connessione, mentre più florida è la situazione dell'81% in Europa Occidentale; in Europa orientale la percentuale scende al 58%, mentre – andando verso Est – la percentuale scende al 38%, per poi salire di molto nell'emisfero australe con il 69%. Internet è oggi collegato agli smartphone; i primi quindici paesi al mondo per possessori di smartphone sono (in ordine)[51]: Corea del Sud (88%), Australia (77%), Israele (74%), USA (72%), Spagna (71%), Nuova Zelanda (70%), UK (68%), Canada (67%), Cile (65%), Malaysia (65%). Ciò implica da un lato la crescita economica dei produttori di smartphone e dell'altra l'utilizzo sempre più massiccio di internet anche tramite cellulare. Ne è venuta fuori la statistica dei primi dieci paesi al mondo per percentuale di mail lette dallo smartphone sul totale[52], come segue: Giappone (88%), Italia (74%), Svezia (72%), USA (72%), Spagna (69%), UK (69%), Australia (68%), Francia (68%), Germania (62%). Chiaramente ad internet e agli smartphone è connessa la tematica dei Social: la parte del leone la fanno *Facebook*, *WhatsApp* e *Facebook Messenger*. Tutto ciò porta a delle considerazioni che esulano forse dalla geopolitica in senso classico, ma di cui i vari governanti non possono esimersi dal sapere. Il tempo che gli utenti passano con il cellulare in relazione all'uso dei Social o di applicativi (come per es. *WhatsApp*), è quanto mai notevole. Vi sono poi delle persone, alquanto creative, che al lancio di una notizia iniziano ad inviare ai loro contatti vignette satiriche o piccoli filmati, da loro stessi creati, che poi finiscono per diventare "virali". Ancora un esempio: *Facebook* è diventato un luogo di aggregazione e un mezzo per conoscere nuove persone. I giovani si sentono menomati se non posseggono uno smartphone, e i modelli più costosi giungono facilmente a superare il migliaio di euro o di dollari. Sembra che *WhatsApp*, *Facebook* o *Twitter* si siano impossessati quasi delle vite delle persone e questa "febbre" dei Social contagia anche gli Stati poveri. Ad esempio nelle Filippine le persone trascorrono in media 3.7 ore al giorno, mentre in Argentina, in Messico e in Brasile ben 3.2[53]. Non è un caso che paesi tendenzialmente meno ricchi abbiano avuto un così grande boom dei Social. Qui rientra un aspetto geopolitico. Infatti Filippine, Argentina, Messico, Brasile sono Stati caratterizzati da una forte

[51] Fonte: *AG*, p. 1099.
[52] Fonte: *AG*, p. 1099.
[53] Fonte: *AG*, p. 1100.

migrazione e quindi i Social consentono ai parenti che vivono lontani di contattare i loro familiari in patria. Così insieme alle rimesse dall'estero questi paesi vedono un incremento di internet indotto dai loro connazionali che vivono all'estero. Infine vi è anche un problema di "dipendenza psicologica" da queste forme di connessione sociale. Certamente quando Antonio MEUCCI (1808-1889) inventò il telefono non pensava che questo strumento avrebbe avuto un così grande successo fino a diventare qualcosa di diverso da un semplice dispositivo di comunicazione vocale; il "passo" successivo fu realizzato da Guglielmo MARCONI (1874-1937) che ideò il wireless, le cui applicazioni appaiono di incredibile portata. Infatti oggi non possiamo fare a meno del telefonino; se giriamo in una città che non conosciamo e ci accorgiamo che abbiamo dimenticato lo smartphone in albergo, si avvertono delle sensazioni di "disagio" fino anche quella di avere ridotta la propria sicurezza personale. Questo processo è avvenuto così velocemente a partire dall'inizio del millennio che non ce ne siamo nemmeno accorti ma con esso abbiamo sviluppato una dipendenza psicologica. In alcuni Stati l'uso degli SMS avverte la cittadinanza di un imminente pericolo (per es. un terremoto o un tornado); oggi numerose aziende private usano *WhatsApp* per inviare messaggi a tutto il personale o a parte di esso. Attualmente si stima che più di un miliardo e duecento milioni di persone usa *WhatsApp* e che questo sia presente in ben 180 nazioni; ma *WhatsApp* è nato solo nel 2009 (e nel 2014 è stato incorporato da *Facebook*) ed oggi appare uno strumento essenziale per la comunicazione cellulare, tanto che stanno decadendo gli SMS (*Short Message Service*). Viene da chiedersi: prima del 2009 il mondo come era? Molti se lo ricordano ovviamente, ma le nuove generazioni non potranno far altro che andare a sfogliare i libri di storia.

In conclusione lo spazio delle comunicazioni non è più rinunciabile e si genera una lotta per la conquista dello stesso. La considerazione geopolitica è che chi detiene parti dello spazio delle comunicazioni ovviamente fa la differenza ed è capace anche di dare informazioni, perfino fuorvianti. Oggi il Presidente degli Stati Uniti possiede un account di *Twitter*[54] e "dialoga" con il popolo; tuttavia non vi è nulla di nuovo sotto il sole: l'imperatore di Costantinopoli sedeva nell'Ippodromo e quello era il momento in cui i sudditi potevano vedere e "dialogare" con il *basileus*. In sintesi: il potere ha sempre usato i mezzi di

[54] Per la cronaca anche il Romano Pontefice usa un account *Twitter*.

comunicazione e continuerà a farlo nei secoli successivi al nostro; ciò che cambia sono le tecnologie, ma la sostanza sembra restare la stessa e con essa la competizione per garantirsi lo "spazio" comunicativo.

§2.3. Il Deep Web, ovvero le incognite di internet

Tornando per un istante ad internet, occorre spendere qualche ulteriore parola. La "filosofia" di internet è ancora – almeno a livello ideale – ispirata al principio di libertà e ciò anche perché esiste il *Deep Web* ("web profondo" ovvero "sommerso"). A questo spazio virtuale si accede con appositi strumenti, principalmente mediante specifici browser[55]. Tale spazio è profondo, come dice il termine stesso, e possiede vari livelli. Questo è il regno indiscusso degli hacker esperti. Infatti il *Deep Web* è uno spazio altamente pericoloso, in quanto una volta entrati lì è facile essere preda degli hacker. Inoltre è anche la zona ove si possono consumare veri e propri crimini (come ad esempio la falsificazione di identità, la pedo-pornografia, il traffico di armi e ogni altra sorta di illecito). Le forze di polizia – che perseguono i *Cyber Crimes* – e quelle di *Intelligence* – cui sta a cuore la sicurezza dei cittadini e dello Stato – navigano regolarmente in queste "acque oscure" al fine di intercettare il crimine o minacce alla sicurezza. Si profila, per le forze dello Stato, una sorta di guerra sottomarina particolarmente difficoltosa, che richiede una preparazione tecnica e professionale di alto livello; sembra un gioco ma non lo è affatto.

La domanda che molti si pongono è quanti livelli di profondità possiede il *Deep Web*? In realtà non vi è una risposta univoca, ma – al momento – solo delle teorie e quindi delle ipotesi. In generale si può dire che esiste un primo livello del web che è detto di "superficie"; questo è quello accessibile a tutti. In questo primo livello – in realtà articolabile in vari sotto-livelli – vi sono i siti di pubblico dominio, quelli con accesso libero e anche quelli che richiedono una registrazione (per es. un sito che vende libri o un Social). Un gradino più in basso, vi sono i servizi detti *Cloud*, ossia le "nuvole", nelle quali occorre però registrarsi per collocare i vari dati. In questa parte del web vi sono anche le "reti" (per esempio la rete di una scuola oppure quella di una società che produce materie plastiche, ecc.). Scendendo più in profondità – ma siamo sempre nel *Web Surface* – vi è la così detta *Bergie Web.* Questa zona è costituita da tutti

[55] Ad esempio, vi è il browser denominato TOR (acronimo che sta per *The Onion Router*).

La verità attraversa sempre tre fasi,
dapprima viene ridicolizzata.
poi viene volutamente contrastata.
Infine accettata come una cosa ovvia.

Arthur SCHOPENHAUER (1788-1860)

CONCLUSIONI… APERTE

In base a quanto ho cercato di tratteggiare nelle pagine precedenti appare chiaro che ogni Stato o potenza proceda attuando il proprio "grande gioco"; ossia tutti competono, in un modo o nell'altro, per raggiungere obiettivi e conquistare spazi – sia materiali che immateriali – procedendo in una ideale linea che assomiglia ad una retta che dunque appare infinita. Ne consegue che in geopolitica non esistano "dogmi" bensì interessi che possono essere di varia tipologia come si è potuto accennare nei precedenti capitoli. Pertanto la geopolitica fornisce delle risposte più spesso in forma di ipotesi, alcune delle quali prendono poi il nome di "teorie" – più o meno organiche – che tuttavia per loro natura non potranno essere mai definitive.

Dunque, essendo la geopolitica una disciplina che possiede carattere di grande praticità, ritengo molto più utile, pratico e perfino saggio affidare le conclusioni dei presenti *Appunti* al Lettore, dichiarandomi fiducioso che queste potranno essere – con buona probabilità – decisamente migliori di quelle che avrei potuto scrivere io come autore.

Valore Italiano™ Editore

Via Mario Menichini, 54
00135 Roma, Italia

www.valoreitalianobookstore.com
Facebook.com/valoreitalianoeditore

Contatti: *info@valoreitaliano.com*

Per la copertina di questo volume la geopolitica è un pane rovente, simbolo di necessità e attrazione.

L'Ammiraglio Giuseppe Lertora, autore della Prefazione, scrive che ci troviamo davanti ad un: "... *libro composito, accessibile anche a neofiti, tanto più adatto ai cultori della materia; senza retorica né melina...*" e che Danilo Ceccarelli Morolli : "... *snoda i vari intercalari con trattazioni di alto profilo concettuale, con appropriate dissertazioni, esempi concreti ed inediti, considerazioni e dotti richiami storici.*"

Per canto suo l'Autore dichiara in premessa che: "... *il presente scritto è volutamente intitolato* Appunti *poiché desidera possedere uno scopo eminentemente introduttivo e didattico; in esso vi è la chiara volontà di offrire agli studenti o al lettore alcune nozioni generali e di base riguardo una disciplina che per la vastità di argomenti, richiede sempre più elevate e specifiche competenze e conoscenze.*"

Euro 26,00

ISBN 978-88-97789-60-4

9 788897 789604

CULTURE & PROGRESSO GEOPOLITICA