

Le analisi sulla situazione del mondo come di una singola regione di globo non può prescindere dal prendere in considerazione l'impatto della pandemia di Sar-CoV-2, dalla capacità di ridurlo, così come le previsioni sui prossimi decenni sono sotto il vincolo del progredire del cambiamento climatico. Le tensioni geopolitiche accompagnano il processo di ristrutturazione complessivo dei rapporti sociali di produzione. Le tecnologie del digitale che costituiscono una componente necessaria di qualsiasi processo di innovazione, in base a questo dato dovrebbero costituire un elemento costitutivo di qualsiasi analisi, laddove questa scavi nel profondo delle trasformazioni in corso; si potrebbe dire che proprio per questo lo si dà per scontato, tuttavia vale la pena riprendere alcuni aspetti del quadro generale – per questo vale la pena prendere a riferimento gli ultimi due articoli di Alessandro Scassellati¹ – aggiornato agli ultimi sviluppi.

Gran parte dell'umanità vive agganciata alla rete digitale, agli estremi i cittadini dei paesi più avanzati, la cui vita è attaccata in mille modi alla rete, generano una mole crescente di dati riferiti alla propria vita e vivono di fatto in un regime di continua sorveglianza più o meno istituzionalizzata o regolata; all'estremo opposto i migranti che attraversano mari e deserti, con le vite affidate a telefoni cellulari e satellitari. I social network sono all'origine dei più clamorosi accumuli di ricchezze, il luogo dove le potenzialità di cooperazione sociale e condivisione della conoscenza, ideali della prima ora di chi ha costruito la rete, dell'etica hacker, si è tramutato in un dispositivo di messa a valore delle relazioni a tutti i livelli e di inasprimento delle disuguaglianze; certo gli ideali della prima ora non sono stati del tutto disattesi, ma, a fronte del movimento per la condivisione di dati e conoscenza nella ricerca e nelle pubbliche amministrazioni, la rete è diventato il luogo delle peggiori patologie nella formazione delle opinioni, delle visioni del mondo, nella crescita della violenza nei confronti di ogni soggetto considerato diverso da sé. I movimenti globali dal Social Forum Mondiale ai Fridays For Future si sono diffusi e organizzati grazie all'uso della rete ovvero del sistema complessivo dei media che si sono evoluti e ridefiniti nelle tecnologie veicolate dalla rete.

La guerra ibrida, la rappresentazione digitale del mondo come un grande campo di battaglia

Nel contempo il digitale contribuisce a ridefinire radicalmente le strategie, i dispositivi e le dottrine militari; il campo di battaglia, i dispositivi militari costituiscono uno spazio digitalizzato, mentre la penetrazione e la destrutturazione delle reti digitali, che sorreggono il funzionamento delle società, costituisce un fondamento delle strategie militari²; una pratica che viene ampiamente esercitata in tempo di pace, in modalità in cui i confini tra una pura attività criminale ed un esercizio di tecniche militari sono spesso sfumati e confusi. La strategia degli Usa 'Defending forward' prevede di stare in costante contatto con gli avversari³ ovvero di essere all'interno dello spazio degli avversari.

Le manovre militari -così possiamo definirle almeno per ora- che si svolgono attorno

all'Ucraina costituiscono anche una occasione per sperimentare la digitalizzazione del cosiddetto warfare⁴ che permette di integrare con dispositivi digitali, di coordinare e centralizzare le più diverse tecniche militari, attivando la cosiddetta guerra ibrida, dove tutti i livelli di intervento sono integrati, compreso quello finanziario. Si va oltre il concetto della 'guerra asimmetrica' a cui siamo stati abituati nel quale le forze di guerriglia si confrontavano con truppe regolari. Gli USA sviluppano il concetto di Integrated Deterrence⁵. Appare evidente come integrare tutte le modalità, i livelli ed i teatri conflitto entro una rappresentazione multidimensionale dello spazio conflittuale globale, richieda l'analisi di una mole di dati, informazioni e parametri di riferimento di una straordinaria complessità che può essere realizzata tramite un apparato digitale di analoga complessità con al centro gli algoritmi dell'Intelligenza Artificiale e del Machine Learning; questo apparato, che opera integrando numerosi sottosistemi, ovviamente diventa a sua volta oggetto di attacco da parte degli avversari, la logica è quella di penetrare nel sistema nervoso centrale e periferico dell'avversario.

Se la condivisione della conoscenza è un obiettivo fondamentale di qualsiasi movimento di liberazione, vedi la lotta contro i brevetti che 'proteggono' i vaccini, contro il monopolio delle conoscenze che è alla base del sistema di sfruttamento e dei rapporti di forza nel sistema capitalistico nella competizione geostrategica al contrario la protezione dei brevetti, delle basi conoscenza che sono alla base di qualsiasi filiera produttiva, è un obiettivo primario di qualsiasi governo e sistema di potere. Esempio è il ruolo negli USA della struttura di Cybercom⁶ nella realizzazione delle strategie difensive nella cyber -guerra e nella difesa della 'proprietà intellettuale' del sistema economico statunitense.

Nel contesto dello sviluppo del cosiddetto *Decision-Centric Warfare* in Cina, vale a dire nell'Esercito di Liberazione Popolare, si parla del System Destruction Warfare, mentre nel caso della Russia il termine di riferimento è New Generation Warfare, come riferiscono gli analisti statunitensi⁷.

Per operare sul campo di battaglia digitalizzato la Defense Advanced Research Projects Agency's (DARPA) ha sviluppato un modello, il Mosaic Warfare concept, nel quale i centri di comando potenziati dall'Intelligenza Artificiale guidano unità disaggregate sia composte che soldati in carne ed ossa che autonome; un sistema quindi caratterizzato da una estrema complessità -almeno apparente- e adattabilità⁸.

Diritti digitali tra appropriazione privata e sorveglianza di stato.

Se, come abbiamo indicato, la competizione geostrategica si svolge su tutti i piani, su tutte le articolazioni di ogni formazione sociale, se c'è uno spettro quasi continuo in cui si collocano le diverse forme tra competizione e conflitto aperto, tutte le articolazioni della vista sociale, politica, economica e culturale sono 'campi di battaglia' che in quanto tali

richiedono un'opera di *sorveglianza continua* che varia a seconda del regime del paese, diventando un fattore caratterizzando dello stesso regime politico del paese, parte integrante del modo di riproduzione sociale.

I diritti digitali dei cittadini sono soggetti quindi sia all'aggressione da parte di società -che sui dati relativi alle persone ed alle collettività fondano i propri profitti, dal Big tech ai piccoli broker di informazioni- che dalla sorveglianza di Stato.

Il governo cinese ha sviluppato un ennesimo e pervasivo dispositivo di sorveglianza attorno al certificato sanitario utilizzato per controllare il contagio⁹; niente a che vedere con il green pass europeo che si limita a registrare i dati della vaccinazione. Il certificato cinese, contiene una serie di dati, come la localizzazione, lo stato di salute, la registrazione degli spostamenti e soprattutto corrisponde a dati conservati centralmente che come tali dal centro possono essere manipolati ed è ciò che l'articolo citato racconta. Il suo uso è rafforzato da una legione di pubblici ufficiali che hanno il potere di limitare i movimenti dei cittadini e metterli in quarantena. Il sistema di sorveglianza messo in atto contro la pandemia, centrato sul certificato ed una serie di app, richiede comunque l'intervento di un gran numero di addetti al tracciamento. Un sistema che perfezionato in pandemia è destinato a crescere anche quando la pandemia sarà diventata un ricordo.

Gli strumenti utilizzati vanno dalle telecamere usate per controllare l'uso delle mascherine, al controllo sul consumo di energia elettrica indice della presenza delle persone in quarantena nella propria dimora, sino a sensori sulle porte per verificare se vengono aperte.

In generale il sistema oltre ad esercitare un controllo pervasivo viene poi utilizzato per raccogliere lamentele e richieste dei cittadini, come nella città di Hangzhou attraverso il "City Brain" center. Il modello implementato è quello del tutto il potere al centro esattamente il contrario di un modello di partecipazione. La Cina ha mobilitato 4,5 milioni dei cosiddetti 'grid workers', uno ogni 250 cittadini, per combattere la pandemia. Il fondamento delle tecnologie e delle procedure che costruiscono un reticolo di sorveglianza e classificazione sul territorio sono le tecnologie di geolocalizzazione¹⁰, questo in Cina come negli USA, ma la Cina ha realizzato un dispositivo particolarmente efficiente -salvo quando la rete tecnologica salta e la vita quotidiana dei cittadini incontra blocchi inaspettati- integrando tecnologia e forza lavoro, in uno sforzo straordinario di disciplinamento della popolazione.

Per capire l'intreccio tra sviluppo tecnologico, dispositivi di sorveglianza e conduzione della guerra ibrida vale l'esempio della CIA che ha creato nel 2015 il 'Directorate for Digital Innovation' incaricato di coordinare e stimolare gli sforzi interni all'agenzia per l'innovazione tecnologica; inoltre ha costituito al proprio interno dei veri e propri laboratori

di ricerca i CIA Labs, arrivando a riconoscere a chi ha contribuito a realizzare brevetti un 15% dei profitti sino a 150.000 dollari all'anno¹¹. I brevetti in possesso della CIA appartengono alle aree di punta dell'innovazione tecnologica.

Alla base delle tecniche di sorveglianza e della raccolta di informazioni di qualità sta la precisa individuazione dei soggetti che usufruiscono dei servizi in rete. Il passaggio cruciale è l'uso da parte delle persone, degli utenti, del proprio nome, il che permette ovviamente di integrare tutte le fonti informative, sia dal punto di vista della profilazione da parte dei social networks che da parte delle agenzie di controllo governative: è il cosiddetto Real Name System. Come sempre la Cina è all'avanguardia¹² gran parte dei servizi in rete sono obbligati alla registrazione con nomi reali dei propri utenti per legge dal 2012. Questa politica procede tra non poche difficoltà a causa di diverse forme di resistenza, mentre in generale lo Stato cinese cerca di rendere sempre più stringente il proprio controllo sulla rete; non solo il governo cinese ma anche le maggiori società che erogano servizi sulla rete hanno espresso un interesse analogo ad avere le esatte generalità dei propri utenti per rendere più efficace la profilazione, per quanto l'incrocio dei dati permetta la costruzione di profili utili e la personalizzazione dei servizi, con la conseguente nascita di molteplici controversie sulla privacy, spinte e contropunte sulle norme destinate a definire i diritti digitali.

La commissione propone una dichiarazione sui diritti e principi digitali per il decennio digitale¹³ dove ritroviamo il principio generale del 'mettere al centro le persone' che ricorre in tutti i documenti proposti dalla commissione compresi quelli relativi all'Intelligenza Artificiale. Il diritto alla connessione viene legato al concetto di 'prezzi accessibili' il che lo esclude dall'essere un diritto fondamentale garantito dal pubblico ad ogni cittadino. Altro punto cruciale è la trasparenza degli algoritmi di Intelligenza Artificiale, di cui ha trattato il Digital Service Act che è ben lungi dall'essere raggiunta trattandosi del cuore dei processi che generano profitto e vantaggio competitivo nel controllo e nella analisi dei flussi di dati. La definizione di uno spazio pubblico è del tutto generico pur trattandosi di una semplice raccomandazione e non già di una norma regolativa. Il riferimento privilegiato al mercato delle norme europee definisce i confini entro cui forzatamente le norme debbono muoversi.

La definizione di una identità digitale, punto cruciale sia per il diritto all'accesso quanto per la difesa della privacy, è già stata affrontata dal REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO che modifica il regolamento (UE) n. 910/2014¹⁴ per quanto riguarda l'istituzione di un quadro di riferimento per un'identità digitale europea, proposto sempre dalla commissione il 3 giugno del 2021, a conclusione di una consultazione pubblica avviata il 24 luglio 2020 e conclusa il 2 ottobre 2020. Per capirsi dal regolamento 910/2014 deriva l'istituzione dello SPID.

Della produzione normativa sul digitale da parte della UE a partire dalle proposte della

Commissione al Consiglio e al Parlamento abbiamo già parlato e giocoforza continueremo a discutere, di volta in volta andiamo ad incappare sui principi neoliberali fondanti l'Unione ed espressi nei suoi trattati. Nel frattempo l'Europa continua ad essere un punto caldo del confronto geostrategico che ha ritrovato in Ucraina un punto di altissima tensione.

L'abbandono dell'Afghanistan da parte degli Usa ha riproposto il tema della difesa europea sia pure nel contesto dell'Alleanza Atlantica, per quanto detto sulla forma dei conflitti, sulla centralità della guerra ibrida, la strutturazione di una Difesa Europea richiede quell'integrazione di tutti i livelli del confronto geostrategico da quello puramente militare, sia pure radicalmente innovato secondo la metodologia Warfare Centric, in termini generali dei diversi piani economico, politico, diplomatico e militare, sino all'uso dei flussi migratori che sono diventati arma comunemente usata dal mediterraneo al Medio Oriente all'Est Europa. L'Integrazione dei diversi piani richiede una effettiva integrazione di funzioni, istituzioni, sottosistemi ed apparati e quindi una centralizzazione, la costruzione di un luogo a cui imputare questo compito. Se questo è vero, oggi l'Unione Europea è totalmente incapace di assolvere a questo compito, sembra molto lontana dal costituirsi come un polo imperialista autonomo -questione su cui da alcuni molto si insiste- e appare subordinata agli interessi strategici degli Stati Uniti.

Ad aggravare questo quadro sembra essere il funzionamento non proprio ottimale dell'agire strategico degli USA sotto l'amministrazione Biden a partire dalle modalità di uscita dal teatro afgano. Su questo, proprio in base alle considerazioni sin qui fatte vale la pena ritornare ed approfondire, come in parte si sta già facendo in alcuni articoli della nostra rivista, approfondendo l'analisi anche in vista delle prossime mosse della FED e dello stato di crisi di diversi paesi in giro per il mondo dalla Turchia all'Argentina.

D'altra parte mentre i governi del mondo non riescono trovarne un accordo efficace impattare il riscaldamento globale, le proiezioni strategiche tengono realisticamente conto delle conseguenze del cambiamento climatico. Esse diventano parte del quadro strategico. La competizione per le risorse naturali che il cambiamento climatico rende scarse, vedi il Land Grabbing, di cui la Cina è protagonista nella corsa per accaparrarsi terreno fertile in giro per il mondo, rende la competizione geo-strategica una gara per la vita di intere popolazioni. I conflitti nelle diverse regioni del globo influenzano di volta in volta l'andamento dei prezzi delle materie prime energetiche o alimentari, delle terre rare o del litio, entrando nel grande gioco dell'inflazione, ma il gioco è molto più grande e riguarda le condizioni minime di sopravvivenza a breve termine di larghe fette dell'umanità.

La guerra ibrida che incorpora sempre di più i processi di questa crisi complessa appare sempre di più come una danza sul ponte del Titanic. Se non si tiene conto di questo, si compie certo un esercizio di esegesi dell'andamento dei conflitti regionali in cui si articola il confronto globale, ma non si coglie la posta in gioco reale. Certo poi il precipitare di situazioni metastabili può essere scatenato da singoli episodi come fu l'attentato di

Sarajevo, ma si tratta sempre di una illusione ottica se non si tiene conto del processo complessivo. L'orizzonte catastrofico di cui oggi si ragiona non è più l'olocausto nucleare - per quanto non lo si possa escludere del tutto - ma è la catastrofe climatica a cui ci si sta appropinquando lungo un percorso costellato da crisi sociali, economiche ed ecologiche, pur tuttavia vale sempre quella logica secondo cui in caso di conflitto nucleare andavano salvati gli stati maggiori, i governi la testa e le risorse strategiche, una sorta di presunto codice genetico delle società. La stessa logica domina oggi l'agire strategico il cui scopo è quello di garantire la sopravvivenza della testa, delle risorse che permettono di riprodurre la formazione sociale in caso di catastrofe, a fronte della evidente incapacità di salvare il complesso della società, l'umanità tutta entro il complesso delle relazioni ecologiche esistenti.

Per questo motivo sono necessari movimenti che riescano ad assumere questo punto di vista, partendo dalla radicalità di fondo della crisi e dei suoi orizzonti catastrofici, ricollegando a questo via via tutti i termini particolari del suo procedere, i conflitti, la rivendicazione, le forme di lotta e le organizzazioni. Quando si parla dell'obiettivo e della pratica della condivisione della conoscenza a questo ci si deve riferire altrimenti si rischia di produrre enunciazioni e proclami senz'altro fondati e coerenti, ma privi di una reale spinta, dove l'attributo della globalità l'uso dell'aggettivo 'mondiale' si traduce in un uro esercizio retorico, privo delle sue reali motivazioni e quindi disgiunto da un percorso concreto che la situazione reale ci dice essere molto, ma molto difficile al limite dell'impossibilità.

di Roberto Rosso

1. <https://transform-italia.it/russia-ucraina-nato-e-unione-europea-tra-minacce-di-guerra-e-diplomazia/> e <https://transform-italia.it/russia-ucraina-nato-e-unione-europea-tra-minacce-di-guerra-e-diplomazia/> [↔]
2. <https://www.defense.gov/News/News-Stories/Article/Article/2840284/persistent-engagement-strategy-paying-dividends-cybercom-general-says/> [↔]
3. Idem *"Defending forward, he said, is getting into the space of our adversaries, so that we can better defend the United States and our allies as well as our interests."* [↔]
4. <https://www.hudson.org/research/16729-implementing-decision-centric-warfare-elevating-command-and-control-to-gain-an-optionality-advantage>
<https://www.hudson.org/research/17507-russia-is-teaching-a-master-class-in-decision-centric-warfare>
<https://www.defenseone.com/ideas/2022/01/russia-teaching-master-class-decision-centric-warfare/361310/> *"The Putin regime's effort to bring Ukraine back into Russia's fold is an excellent case study in what we call "decision-centric warfare." By generating more options for Russian aggression compared to those available to Ukraine and its supporters, the Kremlin is imposing a series of dilemmas on its opponents. For example, If Western military support makes an incursion into the Donbass more fraught, Russia can pursue a decapitating attack on Kyiv with its Belarussian ally. If U.S. and European governments cut Russia off from the global financial system in the wake of an invasion in Ukraine' east or south, Moscow can throttle undersea communications that carry trillions in Western transactions per day. Or if U.S. and allied negotiators attempt protracted negotiations to deny Russia a pretext for war, Moscow can empower its paramilitaries and proxies to resume their gray-zone offensive."* [↔]
5. <https://www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/> *In terms of integrated ... we mean, integrated across domains, so conventional,*

nuclear, cyber, space, informational,” he said. “[It is also] integrated across theaters of competition and potential conflict [and] integrated across the spectrum of conflict from high intensity warfare to the gray zone.” [↔]

6. <https://www.defense.gov/News/News-Stories/Article/Article/2840284/persistent-engagement-strategy-paying-dividends-cybercom-general-says/> *“Therefore, Cybercom is working with the defense industrial base to protect intellectual property and stop them from being able to gain advantages, he said.”[↔]*
7. <https://www.hudson.org/research/16729-implementing-decision-centric-warfare-elevating-command-and-control-to-gain-an-optionality-advantage> *The People’s Liberation Army (PLA) concept of System Destruction Warfare and the Russian military’s New Generation Warfare are representative of the new approaches being employed against the United States and its allies. Although they are very different in their theory of victory and methodology, both concepts share a focus on information and decision-making as the main battlegrounds for future conflict. They direct attacks on an opponent’s battle network electronically and physically to degrade its ability to obtain accurate information while introducing false information that erodes the opponent’s ability to orient. Simultaneously, military and paramilitary forces would present dilemmas to the opponent by isolating or attacking targets in a manner that neutralized their combat potential and controlled the escalation of a conflict.[↔]*
8. *An example of decision-centric warfare is Defense Advanced Research Projects Agency’s (DARPA) Mosaic Warfare concept. Mosaic Warfare’s central idea is that disaggregated manned and autonomous units guided by human command with AI-enabled machine control could use their adaptability and apparent complexity to delay or prevent adversaries from achieving objectives while disrupting enemy centers of gravity to preclude further aggression.[↔]*
9. <https://www.nytimes.com/2022/01/30/world/asia/covid-restrictions-china-lockdown.html> [↔]
10. <https://chinachange.org/2013/08/08/the-urban-grid-management-and-police-state-in-china-a-brief-overview/> [↔]
11. <https://fedtechmagazine.com/article/2020/10/cia-unveils-lab-focus-house-technology-innovation>[↔]
12. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2719384 [↔]
13. <https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles> [↔]
14. <https://www.agid.gov.it/it/piattaforme/eidas> [↔]