ApertaContrada
RIFLESSIONI SU SOCIETÀ, DIRITTO, ECONOMIA

di **Giuseppe Tropea**
pubblicato il 28/01/2025

LA CIBERSICUREZZA COME NUOVA FUNZIONE DELL'AMMINISTRAZIONE [1]

1. Premessa: cybersicurezza in senso ampio e in senso stretto

Un aspetto importante da mettere innanzi tutto in luce è che nello spazio cibernetico dell'*onlife*-world non vi è più differenza fra online e offline[2]; inoltre, a causa dell'espansione inusitata della sorveglianza e della prevenzione, non esiste neanche netta divisione tra pubblico e privato né tra sfera militare e civile[3].
L'espansione della digitalizzazione dello Stato e delle imprese aumenta il campo dei potenziali attacchi cibernetici, ma soprattutto incide in maniera sempre più radicale sui diritti e pone, pertanto, sfide nuove che attengono al nucleo funzionale stesso del costituzionalismo. Inoltre, la nascente funzione pubblica della cybersicurezza inizia a porsi come garanzia essenziale per la continuità nell'erogazione dei servizi pubblici, specie di quelli essenziali.
In Cisgiordania, al fine di identificare i palestinesi prima che accedano a determinati luoghi di lavoro o di svago, i coloni ebrei utilizza(va)no l'applicazione di riconoscimento facciale *White Wolf*. Nella città di Hebron, l'esercito israeliano ha provveduto a istallare delle telecamere per identificare i palestinesi: una rete di telecamere a circuito chiuso, nota come *Hebron Smart City*, monitora(va) in tempo reale la popolazione, a volte rendendo possibile vedere persino all'interno delle case private.
L'attenuazione dei confini pubblico/privato e sfera militare/civile, secondo il vettore che vede in vari Stati anche diversi dal nostro (ad es. in Germania)[4] la progressiva rilevanza della rinnovata funzione di prevenzione, si ha soprattutto proprio nell'ambito della cybersicurezza. Emergono nel contesto che

---

*CONCLUSIONI AL WEBINAR SU "LA CIBERSICUREZZA COME NUOVA FUNZIONE DELL'AMMINISTRAZIONE", 2 dicembre 2024. Nel corso dell'evento, che ha visto le relazioni di Riccardo Ursi, Marcos Almeida Cerreda, Elena Buoso, Giovanni Cocozza, Fulvio Costantino, Pierpaolo Forte, è stato discusso il volume di Stefano ROSSA, *Cybersicurezza e pubblica amministrazione*, Editoriale Scientifica, Napoli, 2023.

[2] L. FLORIDI (Editor), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer Open, 2015, 7, in particolare: «i. the blurring of the distinction between reality and virtuality; ii. the blurring of the distinctions between human, machine and nature; iii. the reversal from information scarcity to information abundance; and iv. the shift from the primacy of entities to the primacy of interactions».

[3] A. COLOMBO, *Il governo mondiale dell'emergenza*, Milano, 2022. Da ultimo, sostenendo la persistenza del fenomeno della globalizzazione, S. CASSESE, *Stato e globalizzazione: chi vince e chi perde?*, in *Riv. trim. dir. pubbl.*, 2024, 529 ss.

[4] E. BUOSO, *Potere amministrativo e sicurezza nazionale cibernetica*, Milano, 2023.

stiamo considerando nuovi rischi per la sicurezza. Si pensi a internet: da un lato spazio connotato da anonimato e assenza di confini, dall'altro, e proprio per questo, soggetto a numerosi pericoli per l'economia nazionale e la sicurezza degli Stati[5].

Sul punto si è distinto fra un concetto di sicurezza cibernetica in senso ampio e uno in senso stretto.

Quello in senso ampio evocherebbe una riproposizione della nozione di ordine pubblico, ma inteso in chiave digitale, e riguarderebbe la protezione in ambiente digitale della pacifica e ordinata convivenza (arg. ex art. 159 d.lgs. n. 112/1998). Si pensi al cyber-bullismo, alle fake news, ai furti di identità. Sul punto si è osservato che in tale settore vi è una crescita di regolazione soft a livello ultra-statale, specie nei riguardi delle *Big tech*, e che la prevenzione legata ad alcuni dei rischi sopra indicati si è concentrata prevalentemente sulla riservatezza dei dati. Restiamo dunque nella dimensione che vede al centro la *privacy* e la sua tutela a livello preventivo ex Reg. UE 679/2016.

Diverso il concetto di sicurezza cibernetica in senso stretto. Qui ad essere coinvolte e minacciate sono le infrastrutture tecnologiche materiali e immateriali in sé, e in questa particolare accezione la sicurezza cibernetica potrebbe configurarsi come funzione pubblica[6].

In genere si registrano tre scopi devoluti al contrasto alle minacce: confidenzialità, integrità, utilizzabilità, conosciuti come triade CIA. A questa triade, la direttiva NIS ha aggiunto i concetti di resilienza e di autenticità.

È su questo secondo profilo che può svolgersi qualche altra riflessione, anche richiamando quanto è stato sin qui detto da chi mi ha preceduto.

A livello nazionale, da tempo le Relazioni sulla politica dell'informazione per la sicurezza trasmesse dal Governo (Presidenza del Consiglio dei ministri) al Parlamento ai sensi dell'art. 38 della legge n. 124/2007 pongono particolare attenzione all'accresciuto livello di complessità e sofisticatezza della minaccia cyber e all'eterogeneità del profilo soggettivo dell'attaccante.

Emerge, in proposito, una variegata gamma di attori che si muovono nel *cyber space* con finalità ed obiettivi diversi, tutti di difficile identificazione, che vanno dall'hacker individuale che agisce a scopo di lucro, all'organizzazione criminale, fino all'apparato governativo che persegue obiettivi geopolitici o propagandistici.

Questo versante dei rapporti fra libertà e sicurezza e fra privacy e sicurezza è però diverso rispetto a quello trattato al punto precedente, perché qui la sicurezza (informatica) non si pone in tendenziale

[5] R. URSI, *La sicurezza cibernetica come funzione pubblica*, in *La sicurezza nel cyberspazio*, a cura di R. Ursi, Milano, 2023, 8.
[6] R. URSI, *La sicurezza cibernetica come funzione pubblica*, cit., 13.

contrasto con la privacy, e con altre libertà e diritti, ma tende al contrario a proteggerla[7]. È questo un aspetto peculiare della cd. sovranità digitale, come garanzia verso attori statali o privati di tenuta dei principi costituzionali, dei diritti e delle libertà. Anche in questo caso al costituzionalismo digitale[8] si è opposta la critica di un certo irenismo[9].

Si potrebbe ipotizzare che ciò avviene anche perché in questo caso la tutela della privacy si accompagna, e non avversa, la crescita di nuovi mercati in espansione[10], mentre vedere ciò nel quadro di una univoca tendenza al rafforzamento della sicurezza europea può allo stato apparire ottativo e prematuro. Si vuol dire che, se le funzioni di sicurezza interna ed esterna sono e restano statali (art. 117, co. 2, lett. d) e h), art. 4, par. 2 TUE), il fondamento di competenza europeo è l'art. 114 TFUE (e 11 Cost.), che lega a livello europeo la sopravvivenza del sistema digitale mediante la tutela del mercato, dei consumatori e dei prodotti digitali.

Come la gran parte delle normative del settore, anche la cybersicurezza non poteva che essere regolata da una disciplina essenzialmente di *soft law,* che evoca una sorta di cyber-giusnaturalismo, a iniziare dalla *Strategia in materia di sicurezza informatica* del 2003 dell'Unione Europea (dove ancora la cybersicurezza non era nominata), fino alle rilevanti Comunicazioni della Commissione del 2010, *Un'agenda digitale europea*, e del 2013, la *Strategia dell'Unione europea per la sicurezza cibernetica*. Da ultimo, però, è intervenuta una normativa di hard law, ossia il regolamento europeo (UE) 2019/881 in materia di cybersicurezza (il c.d. Cybersecurity Act).

Come si vede è stata la crisi economico-finanziaria del 2008 ad accelerare politiche pubbliche sulla cybersecurity, incentivata poi dalla pandemia e dai conflitti internazionali degli ultimi anni.

2. L'evoluzione organizzativa in Italia

Si è notato come l'aspetto strutturale della cybersecurity per definizione è eterogeneo, reticolare e multilivello, in quanto si tratta di rapporti e strutture giocoforza influenzati dal livello sovra-nazionale[11].

---

[7] S. ROSSA, *Cybersicurezza e pubblica amministrazione*, Napoli, 2023, 14.
[8] O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?,* Oxford, 2021.
[9] M. BETZU, *I poteri privati nella società digitale: oligopoli e antitrust*, in *Dir. pubbl.*, 2021, 746.
[10] Sulle più recenti politiche pubbliche europee in materia v. F. COSTANTINO, *Cybersicurezza e contratti pubblici. A proposito del volume di Stefano Rossa su Cybersicurezza e pubblica amministrazione*, in www.apertacontrada.it, 23 dicembre 2024.
[11] I. FORGIONE, *Il ruolo strategico dell'Agenzia Nazionale per la Cybersecurity nel contesto del Sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in *La sicurezza nel cyberspazio,* cit., 95 ss.

Dal punto di vista organizzativo il modello è quello ben noto della *governance*[12]. Si è parlato di Stato-catalitico, diverso da quello regolatore e promotore[13]. Come nel processo chimico di catalisi si assiste alla immissione di una sostanza che propizia l'accelerazione di una reazione a fronte dell'invarianza della sostanza immessa, in questo contesto per 'catalisi' si deve intendere l'immissione del ruolo pubblico all'interno di logiche tecniche e private, quali quelle della innovazione digitale e della sicurezza digitale, mantenendo inalterati i profili essenziali della sfera pubblica e del suo ruolo di garanzia ordinamentale, a partire dalla tutela dei diritti fondamentali e della sovranità. Del resto, già con la l. n. 48/2017 (legge "Minniti") si parla di sicurezza integrata. In questo senso, se la sicurezza integrata è declinazione empirica della sussidiarietà, può dirsi che la cybersecurity alla luce degli approdi più recenti sia manifestazione della sussidiarietà digitale (cyber-resilienza) e del decentramento funzionale tipologicamente connaturato alle reti digitali. Esemplare il protocollo siglato nel 2022 tra Garante per la protezione dei dati personali e ACN per stabilire una organica cooperazione tra le due istituzioni al fine di un coerente ed efficace esercizio delle proprie competenze.

Nel nostro Paese il primo modello organizzativo-funzionale in questo ambito venne delineato durante il Governo presieduto da Mario Monti con il DPCM del 24 gennaio 2013, volto a tutelare la sicurezza nazionale attraverso la protezione cibernetica delle infrastrutture critiche materiali e immateriali, con un'organizzazione inserita nell'ambito dei servizi di *intelligence*.

In seguito, anche a fronte di una strategia unionale connotata da un approccio plurisettoriale e integrato, sfociato nella direttiva 2016/1148 (Direttiva NIS, *Network and Information Security*), oltre al suo recepimento con d.lgs. n. 65/2018, nonché nel Regolamento UE 2019/881 (*Cybesecurity Act*), il Consiglio dei ministri, nella seduta del 19 settembre 2019, ha approvato il d.l. n. 105/2019 che introduce disposizioni urgenti in materia di "perimetro" di sicurezza nazionale cibernetica. Quest'ultimo viene definito non direttamente ma teleologicamente, secondo una tecnica tipica della materia della prevenzione. Da ultimo c'è stato il recepimento di NIS 2 in Italia con la legge 28 giugno 2024, n. 9 (e d.lgs. n. 138/2024).

Per quanto riguarda le procedure di segnalazione degli incidenti su reti, sistemi informativi e sistemi digitali rientranti nel perimetro di sicurezza nazionale cibernetica, i relativi soggetti (amministrazioni pubbliche, nonché enti oppure operatori nazionali, pubblici e privati), individuati con d.m. 131/2020 nei

---

[12] L. FLORIDI (Editor), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, cit., 8: « Hierarchical patterns were key models for social order. Political organisations were represented by Westphalian States, exerting sovereign powers within their territory. Within such States, legislative, executive and judiciary powers were deemed to balance each other and protect against the risk of power abuse. By enabling multi-agent systems and opening new possibilities for direct democracy, ICTs destabilize and call for rethinking the worldviews and metaphors underlying modern political structures».

[13] A. VENANZONI, *L'ordine costituzionale della cybersecurity*, in www.formucostituzionale.it, 26 novembre 2024.

"soggetti che esercitano funzioni essenziali e servizi essenziali", devono notificare l'incidente al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT: *Computer Security Incident Response Team - Italia*) italiano. La minaccia deve consistere nel "malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, (da cui…) possa derivare un pregiudizio per la sicurezza nazionale". Il CSIRT procede poi a inoltrare tempestivamente tali notifiche al Dipartimento delle informazioni della sicurezza (DIS: Dipartimento delle informazioni per la sicurezza).

Inoltre, i soggetti "perimetrati" ex art. 7 DPCM n. 131/2020 devono annualmente predisporre e aggiornare i beni ICT, reti, sistemi informativi a disposizione, effettuando un'analisi di rischio.

L'art. 4 del d.l. n. 105/2019, inoltre, modifica il d.l. n. 21/2012 in tema di poteri speciali del Governo nei settori ad alta intensità tecnologica (c.d. *golden power*). L'esame delle modifiche intervenute dimostra l'attenzione del legislatore rispetto ai rischi implicati dalle innovazioni tecnologiche. Difatti, è stato istituito il perimetro di sicurezza nazionale cibernetica ed è stata prevista la possibilità di valutare nuovamente l'incidenza sugli interessi tutelati dal d.l. n. 21/2012, in base ai criteri di nuova previsione, durante i procedimenti - concernenti attivi societari strategici che rientrano in tale perimetro – precedenti all'entrata in vigore della novella. Le modifiche alla normativa sui poteri speciali e la disciplina relativa al perimetro di sicurezza nazionale potrebbero non essere del tutto in grado di difendere l'Italia dai rischi insiti nel 5G, in quanto la verifica governativa avviene su singole operazioni, mentre quella tecnica del Centro di Valutazione e Certificazione Nazionale (CVCN) è ridotta dalla scarsità delle risorse a disposizione, al contrario dei forti investimenti cinesi sul punto. Inoltre, la vicenda TIM-Huawei dimostra un esercizio del golden power molto contenuto rispetto alle possibilità offerte dalla novella del 2019.

Vi sono diversi modelli organizzativi in chiave comparata: a) quello della autorità indipendente; quello dell'amministrazione ministeriale (es. Germania); c) quello che accentra il ruolo del capo del governo (es. Italia).

Con il d.l. n. 82/2021 sono state quindi emanate alcune disposizioni urgenti in materia di Cybersicurezza, tra le quali definizione dell'architettura nazionale di Cybersicurezza e istituzione dell'Agenzia per la Cybersicurezza nazionale. Qui la cybersicurezza viene definita così: "l'insieme delle attività […] necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico".

L'avvenuto distacco dell'Agenzia per la cybersicurezza nazionale dal Sistema nazionale di informazione, peraltro, rende non chiaro il ruolo dell'Agenzia nel settore, poiché essa resta comunque coinvolta negli

aspetti relativi alle informazioni per la sicurezza della Repubblica, avendo il coordinamento delle attività di ricerca informativa su quelle raccolte dalle varie autorità competenti in materia di difesa nazionale.

3. Cybersecurity e smart city

C'è quindi il tema, eminentemente di politica pubblica, del rapporto fra *cybersecurity* e le *smart cities* viste come luoghi di insicurezza per chi fa uso delle nuove tecnologie[14]. Non solo la persona nella sua dimensione individuale, ma il cittadino o spesso l'impresa o l'amministrazione come soggetti che attraverso la privacy (vista come mezzo a un fine, e non kantianamente come fine in sé) tutelano la propria dimensione economica e di governo. L'evoluzione della disciplina europea, infatti, conferma una progressiva attenzione alla garanzia del funzionamento del mercato interno, a fronte dello sviluppo tecnologico e della grande diffusione delle ICT nella società. A ulteriore conferma di tale assetto sta la dimensione non solo "verticale", ma anche "orizzontale" di tale governance, che vede uno spiccato coinvolgimento degli operatori privati, nel rispetto di un sistema preventivo di certificazione e da uno successivo di notificazione, basato sul binomio obbligo/sanzione[15].

Il tema è stato sinora più trascurato, per la priorità nelle agende urbane della questione della sicurezza urbana di tipo "fisico". Tuttavia, ormai è sempre più al centro della scena. Facendo un paragone, si potrebbe azzardare il passaggio dalla centralità tradizione del diritto di accesso e dei suoi problematici rapporti con la privacy, all'attuale centralità, anche nei repertori giurisprudenziali, della difesa del segreto industriale che si cela dietro la riservatezza, e contro la trasparenza.

Gli attacchi informatici alle reti delle *smart cities* possono essere suddivisi in attivi (*active cyberattacks*) e passivi (*passive cyberattacks*), a seconda se essi determino la manomissione dei dati o consistano in sole attività di intelligence. La difesa da queste forme di criminalità informatica richiede un serio ed efficiente sistema di public cybersecurity, inteso come quell'insieme di misure che le istituzioni pubbliche adottano per difendere i propri sistemi e tutelare gli individui che interagiscono nel cyberspazio da eventuali attacchi.

Ad essere vulnerabili sono per prime le *smart connected cities*, fondate su una rete complessa e interdipendente di dispositivi, piattaforme, sistemi e utenti, tale per cui l'infezione di uno solo di essi apre

[14] Sia consentito sul punto il rinvio a G. TROPEA, *Dal panottico alla dashboard della smart city securitaria*, in www.federalismi.it, 25 settembre 2024.
[15] S. ROSSA, *Cybersicurezza e pubblica amministrazione*, cit., 104.

alla possibilità di infettare, con effetto a cascata (*cascading damage*), tutti gli altri, causando un furto diffuso di informazioni provenienti da cittadini, enti pubblici, imprese, forze dell'ordine ecc.[16].

L'aumento del numero, della portata e dell'impatto degli attacchi informatici, anche e soprattutto nelle smart city, necessita di una difesa dinamica, proattiva e adattativa, supportata da valutazioni in tempo reale attraverso il monitoraggio continuo e l'analisi dei dati. Questo tema naturalmente incrocia quello della questione tecnologica, ossia attraverso quali strumenti si esercita la funzione della cybersicurezza, e naturalmente la risposta è in prima battuta l'intelligenza artificiale, con le sue luci ma anche se sue tante ombre e bias[17], tema sul quale non posso qui concentrarmi, vista la sua vastità e delicatezza.

4. Alcune perplessità conclusive

A fronte della tendenziale condivisibilità sul fatto che si sia di fronte a una nuova complessa e variegata funzione amministrativa, per le ragioni sopra indicate, bisogna a questo punto fare alcuni rilievi critici.

1) Prima di tutto, le regole procedurali in ordine all'inserimento di un soggetto nel perimetro di sicurezza nazionale sono connotate da un arretramento di tutela rispetto alla l. 241/90; mentre i criteri sostanziali in ordine all'inserimento di un soggetto nel perimetro di sicurezza nazionale, nonostante la centralità della Presidenza del Consiglio, vengono ritenuti afferire alla categoria della discrezionalità tecnica o mista[18]. Ma quando si tocca il tema del golden power (es. 5G, cloud) mi pare che la discrezionalità si accresca ulteriormente. Emblematico mi pare il recente caso Cedacri[19], in cui la lettura sostanziale e non formale della disciplina da parte del Tar ha evidenziato l'intrinseca politicità della stessa, e un'impostazione dirigista nell'uso del Golden power, con il Tar Lazio che, nel dare ragione al Governo, finisce per suggerire indirettamente come si debba gestire una società proprio in un ambito relativo allo sviluppo di software per la protezione dei dati relativi alla persona, alla negoziazione e allo scambio di dati e prodotti, nonché alla gestione documentale nell'ambito della gestione delle attività finanziari.

2) Il secondo profilo tocca il tema regolatorio: come si è detto, in questo caso la riservatezza del dato è mezzo rispetto al fine, sicché è necessario partire da questo presupposto per intendere come la regolazione in materia debba essere per quanto possibile una regolazione *hard*, non fatta esclusivamente

[16] G. PANATTONI, *Le Smart Connected Cities: i fattori di insicurezza e (s)fiducia dei cittadini*, in *Dir. pubbl.*, 2023, 646.
[17] Sul punto v. da ultimo R. BRIGHI, *Cybersicurezza e Intelligenza Artificiale. Un'analisi critica*, in BioLaw Journal – Rivista di BioDiritto, Special Issue 1/2024, 111 ss.
[18] E. BUOSO, *Potere amministrativo e sicurezza nazionale cibernetica*, cit., 104.
[19] Tar Lazio n. 10275/24.

di *soft law* proveniente da *law firms* legate agli interessi delle Big tech. In questo campo, infatti, la presenza del privato resta fondamentale, specie per la proprietà delle infrastrutture e per le asimmetrie informative del settore, costringendo lo Stato (debole) ad agire sul mercato ICT (quasi) al pari di un privato. Le c.d. legge di Moore e legge di Rock, infatti, mettono in luce che tanto più la tecnologia è evoluta tanto più costa produrla[20].

3) Il terzo profilo tocca infine il tema organizzativo, ma parte dai medesimi presupposti critici di quello regolatorio: l'esercizio di funzioni amministrative tradizionalmente di competenza degli Stati e la partecipazione all'attività di natura politica in materia di cybersicurezza, dovrebbero essere incardinate presso il Governo o il Parlamento, mentre la legittimazione tecnocratica e non democratica di autorità indipendenti non scongiura il rischio che esse possano arrivare a svolgere un potere pubblico non bilanciato e controllato dal Parlamento, di nuovo magari a favore di poteri privati. Sicché nel caso italiano, in cui le funzioni di autorità nazionale competente NIS sono state attribuite dal decreto-legge n. 82 del 2021 all'Agenzia per la cybersicurezza nazionale, se è vero che il Parlamento non è escluso dal controllo, è pur vero che:

a) il Copasir, a causa della particolare riservatezza del proprio operato, non può garantire sul punto un sufficiente livello di trasparenza;

b) l'autorità nazionale competente in materia di cybersicurezza è istituita presso la Presidenza del Consiglio dei ministri e dall'attribuzione del ruolo di vigilanza parlamentare del Governo principalmente al COPASIR deriva una eccessiva concentrazione di potere in capo al vertice del Governo[21]. Peraltro, l'autonomia dell'Agenzia è fortemente attenuata a causa della relazione di direzione-dipendenza nei confronti del Presidente del Consiglio dei ministri, anche a causa del ruolo sempre più cruciale svolto da quest'ultimo nell'ambito dell'architettura dell'intelligence, specie dopo la riforma del 2007.

Di ciò risente pure l'assetto delle relazioni fra pubblico e privato in materia, connotato da un persistente approccio autoritativo più che collaborativo[22], criticabile specialmente a fronte di uno speculare ampliamento degli strumenti di collaborazione fra l'acquirente pubblico e il venditore privato e della trasformazione in materia dello Stato da regolatore a Stato innovatore[23].

---

[20] S. ROSSA, *Cybersicurezza e pubblica amministrazione*, cit., 47.

[21] L. MORONI, *La governance della cybersicurezza a livello interno ed europeo*, in www.federalismi.it, n. 14/2024. Concorda F. COSTANTINO, *Cybersicurezza e contratti pubblici. A proposito del volume di Stefano Rossa su Cybersicurezza e pubblica amministrazione*, cit.

[22] S. ROSSA, *Cybersicurezza e pubblica amministrazione*, cit., 110.

[23] M. MAZZUCATO, *Lo Stato innovatore*, Roma-Bari, 2018.

Questo, peraltro, mi pare il cuore del bel lavoro di Stefano Rossa, che nell'approfondire (soprattutto nei capp. IV e V) il tema poco battuto della disciplina italiana degli appalti pubblici in ambito proprio di cybersecurity, mette al centro un rinnovato concetto di "sovranità digitale", non già come nazionalismo digitale, tecnologicamente anacronistico e contrastante con la logica dei diritti, ma come ambiente fatto di logica collaborativa, sia pubblico/privato in ambito contrattuale, sia fra Stati europei, al fine di raggiungere sul piano geopolitico un peso pari ai colossi privati americani e alla Cina, allo stato di là da venire.