Premessa

Innanzitutto desidero esprimere un vivo ringraziamento al Presidente e tutti i membri della Commissione Difesa della Camera per avermi invitato in audizione per discutere un Decreto Legge che riveste una particolare urgenza nonché una importanza cruciale per il nostro paese, per l'Europa e per il contributo che l'Italia può offrire alla comunità internazionale.

Vorrei sottolineare che la materia (sicurezza cibernetica e delle reti) che il Decreto si propone di disciplinare non riveste soltanto una particolare urgenza in questa delicata fase degli equilibri geopolitici mondiali; essa è altresì destinata ad incidere profondamente sul futuro delle nuove generazioni e sulla stessa tutela della sovranità, dello Stato di diritto, dei valori fondanti della nostra Costituzione e delle democrazie nel prossimo decennio.

Le mie riflessioni ed i miei suggerimenti nascono dall'esperienza pratica ed accademica maturata nell'ultimo decennio:

Consigliere per la Cybersecurity del Ministro dell'Interno, docente di "Cyber International Politics" al PHD della Scuola Superiore Sant'Anna di Pisa e di "Cyberspace" al Master di Cyber Defence promosso dallo SMD alla Scuola di Telecomunicazioni FFAA di Chiavari, nonché delle mie recenti attività di insegnamento alla Luiss "Guido Carli e alla Link Campus University, ateneo in cui dal 2015 dirigo il noto Master di Intelligence e Sicurezza giunto alla sua XIV edizione. A partire dal 2012 ho, inoltre, avviato interessanti scambi didattici con docenti e ricercatori del Dipartimento di Scienze Politiche e di Computer Science del MIT di Cambridge (MS/US), con il Centro dei Cybersecurity dell'Università di Tel Aviv con il Centro di ricerca per il contrasto al terrorismo islamista a Parigi, Science PO.

Sono infine particolarmente lieto di invitare nei prossimi mesi il Presidente ed i componenti della Commissione ad intervenire ai seminari e alle tavole rotonde che insieme ai miei colleghi organizzeremo nell'anno accademico 2019/2020 in materia di Cybersecurity e Difesa. Speriamo così offrire cosi un piccolo contributo ad un fruttuoso e più intenso interscambio tra Università e Istituzioni Democratiche.

Suggerimenti relativi al Decreto Legge in oggetto

Prima di esaminare i singoli articoli ed illustrare eventuali ipotesi di modifica desidero sottolineare quattro aspetti:

a) La rivoluzione tecnologica non si è limitata a creare soltanto il V Dominio sulla cui analisi da quasi un ventennio si concentra l'attenzione della Dottrina militare e delle Scienze Strategiche. A seguito di una acuta intuizione del Gen. Dempsey

all'epoca (2011) Chief of Staff delle Forze Armate degli Stati Uniti si è colta con sempre maggiore lucidità la grande trasversalità e pervasività della rivoluzione digitale che investe la società nel suo complesso: dalla vita quotidiana alla sanità, dai processi industriali alla pubblica sicurezza, dal traffico aereo all'auto a guida autonoma, dalla Sicurezza Nazionale alla Difesa.

b) In conseguenza di ciò i rischi e le minacce connesse al cosiddetto "lato oscuro" (Isaac Ben Israel 2013) della rivoluzione tecnologica in area ITC interseca in modo trasversale l'insieme dei domini, rendendo più labili e confusi tre confini tradizionali: politica interna ed estera, ambito civile e militare, pubblico e privato (i.e. Infrastrutture critiche);

c) Le importazioni di reti prodotti, componenti e servizi da imprese provenienti da paesi extracomunitari dove è assente lo Stato di diritto costituisce di per sé un forte di rischio che il legislatore deve prendere in considerazione. Non mi riferisco soltanto alle interferenze, all'azioni di influenza o agli attacchi rivolti a "rubare" (o meglio copiare) importanti scoperte e conquiste appartenenti al patrimonio scientifico, tecnico, militare e industriale pregiato e sensibile del nostro Paese.

d) Nei regimi politici dove non opera lo Stato di diritto e caratterizzati da gravi opacità nella *governance* è molto più probabile il rischio di manipolazioni, intrusioni, penetrazioni e azioni criminali di vario tipo con enormi difficoltà di attribuzione. Per quanto ci riguarda le ingerenze esterne extra UE e i meccanismi intrinseci alla rivoluzione digitale potrebbero in un futuro non lontano rendere di di difficile attuazione alcune disposizioni della nostra Costituzione. In queste settimane la ricerca che sto conducendo si sofferma (sia pur in forma ancora preliminare) su una decina di articoli della Carta: 6, 9, 14,15, 33, 36, 37,41,42, 47, 48.

Da queste sommarie considerazioni derivano i seguenti suggerimenti:

1) La sovranità digitale - persino nel caso del Firewall cosidetto "Muraglia Cinese" per essere veramente tale necessità di una cooperazione internazionale mirata di paesi confinanti e/o alleati. Pertanto il Decreto Legge dovrebbe fare esplicito e vincolante riferimento alle disposizioni di Cyber Security e Cyber Defence adottate (o in sede di adozione) in ambito UE e NATO. La Commissione conosce assai meglio del sottoscritto la collaborazione NATO/UE che in campo Cyber se non erro sta procedendo positivamente e rapidamente a livello tecnico.

2) L'impatto trasversale e pervasivo della rivoluzione digitale è tale che non ha senso affidare i meccanismi relativi alla sicurezza cibernetica nazionale ad un singolo Ministero e tanto meno al MISE che non ha competenze primarie in materia di Sicurezza, ma ha viceversa la funzione fondamentale di stimolare la crescita, l'innovazione, le start up (come ben sapete sempre più spesso usate come cavallo di troia per le intrusioni), l'occupazione, la ricerca e lo sviluppo. Viceversa le finalità del Decreto Legge in oggetto sono essenzialmente rivolte alle materie della Sicurezza Nazionale, della Pubblica Sicurezza e della Difesa con connessioni alle normative di sicurezza a livello Europea e Atlantico (ruolo MAECI);
3) A mio modesto avviso anche a seguito del recentissimo Decreto di istituzione del Dipartimento Digitale della PdC gli strumenti della Sicurezza Nazionale Cibernetica non possono che fare riferimento (compresa ovviamente la vigilanza) alla Presidenza del Consiglio, d'intesa (e con il più ampio) coinvolgimento dei Ministeri della Difesa, degli Interni nonché per le sue competenze specifiche del Ministro degli Esteri e degli Affari Europei;
4) Occorre ripensare l'approccio alle misure di sicurezza rivolte alle imprese private e/o partecipate o controllate dal pubblico siano esse fornitrici della Pubblica Amministrazione e/o delle Infrastrutture critiche o del nuovo elenco previsto dal Decreto. Interventi expost e test in corso di bandi e gare aperte pongono delicati problemi di legittimità e in ogni caso le iniziative che si inseriscono nei processi hanno generalmente scarso successo, salvo semmai ispezioni e controlli tecnici a sorpresa non di routine. L'autorità pubblica ha viceversa il compito di indicare ex ante le direttive, gli standard, gli obblighi di notitificazione degli incidenti e i divieti sulla base di informazioni tecniche elaborate in Italia, a livello UE e NATO (ed anche da Stati membri e alleati). Se la Francia per ipotesi scopre una vulnerabilità non è che l'Italia deve ripartire da zero.
5) Per quanto riguarda lo strumento occorre dare uno sguardo anche a quanto realizzato o in corso di realizzazione negli altri paesi. Da una rapida rassegna possiamo ipotizzare che nell'ordinamento italiano lo strumento più adatto (per la sua snellezza operativa e per il suo carattere essenzialmente tecnico) ed anche come agile raccordo con il punto unico di contatto previsto dalla NIS sia l'istituzione di una Agenzia di Valutazione ai sensi della legislazione 1999 e seg. In pratica Il CVCN si trasformerebbe utilmente in AVCN presso la PdC, titolare della Sicurezza Cibernetica Nazionale e connesse funzioni di vigilanza sulla Agenzia .
6) L'assunzione del personale cosi come e' prevista dal Decreto con i vincoli previsti sia per il reclutamento esterno che sia per il reclutamento interno (utilizzo di personale civile e militare) è in palese contraddizione con gli obiettivi del

provvedimento in sede di conversione. A queste condizioni l'insuccesso è assai probabile. Lo Stato deve assumere o reclutare al proprio interno chi gli serve con (funzionari e dirigenti) e offrire retribuzioni non troppo lontane dalle competenze e dalle esperienze professionali necessarie per i difficili compiti assegnati.

7) Una ultima considerazione di carattere terminologico. L'espressione Perimetro è fuorviante e fonte di incomprensione. So bene che l'uso è metaforico, ma nel linguaggio comune e sui media può a mio avviso portare ad una notevole incomprensione. L'universo digitale è pluridimensionale senza considerare le molteplici ed ibride vulnerabilità interne alle organizzazioni. Pertanto sarebbe a mio avviso più chiara una espressione tipo dominio di Sicurezza Cibernetica Nazionale o comunque un termine giuridico più pertinente

Vi ringrazio davvero molto dell'attenzione sottolineando senza una strumentazione davvero adeguata stessa normativa sul Golden Power rischia di essere adottata prevalentemente su alert esterni (peraltro ad oggi assolutamente giustificati).

Prof. Marco Mayer

Direttore Master Intelligence e Sicurezza Link Campus University;

Adjunt Prof. Conflict and Peace Buiding, Luiss Guido Carli;

Il